+

Autorità di Sistema Portuale
del Mare Adriatico Orientale
Porti di Trieste e Monfalcone

PROGETTO FENIX
SERVIZIO DI SVILUPPO E MANUTENZIONE APP FINALIZZATA ALLA GESTIONE DEL TRAFFICO VEICOLARE

Sommario

1. INTRODUZIONE

L'Autorità di Sistema Portuale del Mare Adriatico Orientale, di seguito AdSP MAO, all'interno del progetto FENIX "A European Federated Network of Information eXchange in LogistiX" (https://fenix-network.eu/) co-finanziato dal Programma Connecting Europe Facility dell'Unione Europea, al fine di sviluppare un'architettura federata europea per la condivisione dei dati al servizio della comunità logistica europea di caricatori, fornitori di servizi logistici, etc., ha deciso di sviluppare un'applicazione Mobile finalizzata al tracciamento e alla gestione dei flussi veicolari nonché della documentazione relativa agli aspetti logistico/doganali.
Il presente capitolato, integrato delle parte progettuale mira alla definizione delle specifiche relative ad un servizio di sviluppo e gestione dell'App nel suo complesso.

Importo del corrispettivo a base d'asta: euro 200.000 (duecentomila)
(esclusi IVA ed oneri previdenziali).

1.1 Caratteristiche richieste e proprietà intellettuale

In accordo con il comma 1 dell'art. 68 del D. lgs. 7 marzo 2005, n. 82 e s.m.i. (Codice dell'Amministrazione Digitale, in seguito CAD), il presente Capitolato fa riferimento ad un software sviluppato per conto dell'Autorità di Sistema Portuale del Mare Adriatico Orientale.

L'Ente affida lo sviluppo del software all'operatore selezionato e quest'ultimo si impegna a consegnare all'Ente lo sviluppo e manutenzione dei moduli richiesti sulla base dei requisiti definiti dall'AdSP MAO.

Tale servizio, in linea con il comma 1-bis dell'art. 68 del CAD, deve prevedere tra l'altro, l'utilizzo dei seguenti formati:

- Dati aperti: uso di formati pubblici e aperti per la rappresentazione di dati, metadati e documenti;
- Utilizzo di interfacce aperte: uso di interfacce aperte, vale a dire interfacce pubbliche, documentate e liberamente implementabili/estendibili;
- Utilizzo di standard per l'interoperabilità e la cooperazione applicativa: aderenza agli standard di interoperabilità e di cooperazione applicativa.
- Soluzione Modulare: la soluzione proposta deve avere una struttura modulare e implementare le seguenti caratteristiche:
    - Adozione di soluzioni che assicurino l'interoperabilità e la cooperazione applicativa;
    - Scalabilità della soluzione, quindi prevedere la possibilità di poterne estendere le funzionalità;
    - Riusabilità della soluzione.

Si precisa che l'AdSP MAO, in adempimento al comma 2 dell'art. 69 del CAD, mantiene la titolarità esclusiva del software realizzato nonché i diritti di proprietà e, quindi, di utilizzazione, di tutto quanto realizzato e dei relativi materiali e documenti creati, inventati, modificati, predisposti o realizzati dall'operatore o dai suoi dipendenti nell'ambito o in occasione dell'esecuzione del servizio.

Inoltre, la proprietà intellettuale e il diritto di sfruttamento industriale dei moduli realizzati è esclusiva dell'AdSP MAO, la quale potrà, pertanto, senza alcuna restrizione, utilizzare, pubblicare, diffondere, vendere, duplicare o cedere, anche solo parzialmente, i materiali e le opere dell'ingegno oggetto dell'appalto.

Nello svolgimento dell'attività dovrà essere osservata la massima riservatezza su ogni informazione di cui l'operatore, nel corso dello svolgimento dell'incarico, venisse a conoscenza.

L'operatore è espressamente obbligato a fornire all'Amministrazione tutta la documentazione e il materiale necessario all'effettivo sfruttamento di detti diritti di titolarità esclusiva, compreso il codice sorgente completo nella forma utilizzata per lo sviluppo della soluzione.

In linea con i criteri elencati al comma 1-bis dell'art. 68 del CAD, il fornitore dovrà garantire in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio, tenuto conto della tipologia di software in oggetto.

1.2 Caratteristiche richieste in materia di sicurezza

La presente sezione riporta le richieste specifiche che dovranno essere rispettate dall'aggiudicatario nella realizzazione del servizio oggetto del presente Capitolato e opportunamente documentate.

ID	Ambito	Caratteristica richiesta
PR001	Privacy	Aderire al GDPR, Regolamento UE 2016/679
PR002	Privacy	Garantire la possibilità di estrarre in qualsiasi momento una copia completa di dati, metadati e documenti memorizzati, in formati pubblici e aperti.
SIC01	Sicurezza accessi logici	Garantire l'accesso alle informazioni attraverso un sistema di autenticazione e autorizzazione, che consenta la gestione di profili autorizzativi basati su ruoli
SIC02	Protezione canali scambio dati	Garantire il transito delle informazioni verso l'utenza con l'utilizzo di protocolli e meccanismi di scambio crittografati (es. canale HTTPS)
SIC03	Gestione obsolescenza	Garantire la presenza di componenti tecnologiche aggiornate e conformi agli standard di mercato alla data di consegna.
SIC04	Gestione log	Attivare il controllo delle attività svolte dagli utenti attraverso appositi meccanismi di registrazione e tracciatura dei log.
SIC05	Ciclo di sviluppo sicuro del software	Adottare un modello (specificare quale) di ciclo di sviluppo sicuro del software conforme alle "Linee Guida per l'adozione di un ciclo di sviluppo di software sicuro" di AGID.
SIC06	Sicurezza accessi logici	Indicare se l'accesso alle informazioni è garantito attraverso un meccanismo di autenticazione a più fattori (*strong authentication*).
SIC07	Protezione dei dati	Indicare se i dati a riposo sono memorizzati in forma criptata.
SIC08	Fornitura Software	Indicare se il componente oggetto di fornitura è stato sottoposto a test OWASP con esito positivo. Nel caso fosse stato sottoposto a qualche altro test di sicurezza, si indichi quale.
SIC09	Fornitura Software	Indicare se è possibile utilizzare sistemi di protezione *antimalware* sui sistemi utilizzati per la gestione dei dati.
SIC10	Fornitura documentazione	Fornire il piano di Business Continuity e Disaster Recovery della infrastruttura

1.3 Il progetto e il contesto di riferimento

L'AdSP MAO si è dotata di un sistema informativo "*Port Community System*" (PCS) realizzato per essere al servizio dell'intera comunità portuale, denominato "Sinfomar". Questo sistema è stato progettato per gestire in modo efficiente la specificità legislativa propria del Porto di Trieste, composto dalle aree di Porto Vecchio, Porto Nuovo, Oli Minerali, Scalo Legnami e Zona Industriale, caratterizzate da aree parziali o totali di Punto Franco. Tale aree portuali sono divise anche in aree comuni (in capo all'AdSP MAO) e in aree in concessione (in capo ai terminalisti e operatori privati), ivi incluse le aree afferenti alla più ampia realtà della logistica del sistema portuale, come ad esempio l'Interporto di Trieste sito in località Fernetti.

Il progetto Sinfomar ha coinvolto, fin dall'anno 2014, l'intero mondo marittimo locale e regionale. In particolare, tra gli operatori privati sono stati coinvolti gli Agenti Marittimi, gli Spedizionieri, gli Spedizionieri Doganali e i Terminalisti. In misura minore sono stati coinvolti alcuni trasportatori e le società di Sorveglianza. Per quanto riguarda, invece, gli operatori pubblici, sono stati interessati dal progetto Sinfomar i seguenti attori: l'Agenzia delle Dogane, la Capitaneria di Porto, la Guardia di Finanza, la Motorizzazione Civile, la Sanità Marittima, gli interporti regionali (in primis l'Interporto di Trieste, diventato di fatto il principale terminal intermodale di riferimento) ed alcuni operatori particolari, quali le società Alpe Adria S.p.A. (Multimodal Transport Operator regionale), Rail Cargo Austria (impresa ferroviaria), Adriafer S.r.l. (società di manovra ferroviaria) e l'Università di Trieste (soggetto interessato all'analisi dei dati logistici afferenti il Porto di Trieste).

L'AdSP MAO, inoltre, svolge le attività afferenti alla gestione del traffico veicolare in ingresso ed in uscita dal porto e alle relative aree interconnesse.

In questo contesto, nell'ottica di sviluppo di una rete integrata che consenta una sinergia tra gli aspetti logistici e doganali, nonché con il fine più ampio di supportare un network federato a livello europeo (progetto FENIX), l'AdSP MAO intendente sviluppare una APP che consenta la gestione integrata di tutti gli aspetti sopra menzionati.

Tale APP – oggetto del presente capitolato di gara – diventerà strumento importante nel percorso di digitalizzazione dei processi logistico/doganali, aumentandone efficacia ed efficienza.

2. DEFINIZIONE DEI SERVIZI OGGETTO DELL'APPALTO

2.1 Servizi richiesti

In linea con il modello di sviluppo del software sicuro adottato, saranno richiesti un costante confronto e coordinamento tra il team del fornitore e l'AdSP MAO.

L'oggetto della procedura è rappresentato dal servizio di realizzazione, sviluppo, gestione operativa di una Applicazione Mobile e relativo portale gestionale di backoffice (accessibile via Web), secondo quando stabilito e descritto nell'allegato 1 al presente capitolato, in modalità SaaS.

Si evidenzia che nel servizio sono comprese:

- l'attività di interfacciamento con sistemi terzi ed in particolare con il Port Community System Sinfomar. Tutti gli eventuali oneri necessari, relativi a tale finalità di realizzazione del colloquio tra la app e Sinfomar, sono interamente a carico dell'appaltatore, che dovrà in modo autonomo concordare le modalità tecniche e di costo con il gestore del PCS;
- la messa a disposizione e la relativa gestione di tutto l'hardware (server fisico o virtuale) e software necessario all'implementazione dell'applicazione;
- la gestione delle attività propedeutiche alla pubblicazione del software sviluppato sui principali canali di distribuzione (es. Google Play, Apple Play)
- la realizzazione delle funzionalità come riportato nelle specifiche dell'Allegato 1, considerate parte integrante del presente capitolato.

La soluzione SaaS non dovrà comportare alcun investimento in infrastrutture, hardware e licenze software, sia per la AdSP MAO, sia per le imprese terze coinvolte.

Oltre a quanto previsto nell'Allegato 1, il servizio oggetto dell'appalto si compone, inoltre, delle attività trasversali e ambientali di seguito elencate.

2.1.1. Formazione

In particolare, per quanto concerne l'utilizzo del gestionale, si dovrà prevedere un'adeguata formazione al personale individuato il personale interno all'AdSP MAO, che dovrà essere opportunamente istruito sulla base di un programma condiviso ed approvato dall'Ente.

Il programma di formazione dovrà avere come obiettivo immediata autonomia nell'utilizzo del software del personale che parteciperà ai processi integrati del sistema.

È richiesto un pacchetto di 5 giornate, da erogare in presenza o da remoto.

2.1.2. Requisiti tecnici

Dovranno essere seguite le line guida AgID per lo sviluppo di software sicuro, in particolare l'Allegato 2 e l'Allegato 3.

Nello specifico, dovrà essere impedito, oppure adeguatamente gestito, l'inserimento di caratteri non legali secondo i formati più diffusi di interscambio dati (es: *web services* XML, API – Application Program Interface), onde evitare blocchi nelle relative operazioni di interscambio dei dati stessi. Laddove necessario, e per le informazioni non preventivamente tabellate, dovranno essere previste funzioni di controllo sul data entry; ad esempio, l'uso tassativo delle lettere maiuscole nelle sigle dei contenitori oppure nelle partite IVA, nei codici EORI – *Economic Operator Registration and Identification*, ed altre tipologie di anomalie che verranno di volta in volta gestite da AdSP MAO.

Inoltre, dovranno essere rispettate le seguenti caratteristiche:

- infrastruttura tecnologica stabile, performante e sicura;
- l'utilizzo di standard aperti (es. XML, Json, Javascript, CSS, AJAX, SOAP, REST ecc.);
- l'accesso al "gestionale" mediante una interfaccia full web, che non preveda lo scaricamento in locale sul client di ambienti di runtime esterni. L'accesso dovrà avvenire esclusivamente attraverso il protocollo https e non dovrà essere installato software specifico al funzionamento della soluzione;
- la disponibilità di servizi di import ed export di dati da e per sistemi esterni basati sull'utilizzo del protocollo https (e.g. web-services) eventualmente attivabili su specifiche richieste dell'Ente
- l'app dovrà poter essere installata su dispostivi smartphone di ultima generazione con sistema operativo Android pari o superiore alla versione 12 (livello API 31) e con sistema operativo iOS superiori alla versione 15.

2.1.3. Requisiti di sicurezza dell'Infrastruttura tecnologica

L'appaltatore dovrà fornire una soluzione tecnologica con le seguenti caratteristiche minime e fornire il piano di disaster recovery e business continuity dell'infrastruttura ospitante:

- il server dovrà essere localizzato nella comunità europea e dovrà prevedere un'architettura distribuita sia per evitare sovraccarichi computazioni del server centrale, sia per garantire il servizio nel caso di malfunzionamenti dello stesso.
- il server dovrà essere configurato rispettando tutti i requisiti minimi di sicurezza e utilizzando tutte le restrizioni e le regole (es installazione di Firewall, ecc.) necessarie ad evitare possibili attacchi da parte di personale non autorizzato e/o da bot automatizzati (es. attacchi DDoS - Distributed denial-of-service, ecc.).
- la sicurezza nell'accesso del sistema, da garantire implementando il protocollo Secure Socket Layer (SSL) a cifratura forte (almeno 128 bit);
- backup e archiviazione: i dati dovranno essere archiviati su supporto a lunga conservazione a livello semestrale; giornalmente dovrà essere assicurato il backup del software e dei dati e come previsto dalle 'Misure minime di sicurezza ICT per le pubbliche amministrazioni' (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015). Le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati;
- assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti, ovvero mediante cifratura;
- dati di produzione: i dati di produzione non dovranno essere replicati o usati in altri sistemi a meno di quanto previsto nel requisito back up e archiviazione;
- autorizzazione all'accesso: l'accesso informatico del personale (sia normale, sia privilegiato) a applicazioni, sistemi, reti, data base dovrà essere ristretto e soggetto a procedura di autorizzazione;
- antimalware: dovrà essere presente un presidio antimalware e antivirus che garantisca rispetto alla 'bontà' dei file caricati sul sistema e che questi possano infettare le postazioni degli utenti;
- sicurezza applicativa: le applicazioni messe a disposizione di AdSP MAO dovranno essere progettate in accordo con gli standard e le best practices di sicurezza;
- logging: i log che riportano la registrazione degli accessi dovranno essere raccolti e conservati in conformità con le prescrizioni del codice della privacy;
- crittografia: tutti i dati dovranno essere crittografati quando trasmessi su rete;
- gestione delle chiavi di crittografia: le chiavi di crittografia dovranno essere generate e memorizzate in modo sicuro;

Il fornitore dovrà rispettare il Regolamento UE 2016/679 in materia di privacy e successive evoluzioni: il soggetto fornitore deve garantire e dimostrare di aver fatto tutto quanto necessario al fine di conformarsi al GDPR e alle disposizioni applicabili in materia di protezione dei dati personali e in modo particolare di aver sviluppato le valutazioni del rischio dell'uso dell'applicativo che dovrà essere tassativamente disegnato in maniera conforme al Regolamento UE 2016/679. Il soggetto fornitore deve inoltre assicurare che i principi di "privacy by design" e "privacy by default" sanciti dall'articolo 25 del GDPR sono stati assunti quali fondanti nell'elaborazione dell'applicazione, documentando che le condizioni necessarie per garantire la protezione dei dati fin dalla progettazione e per impostazione predefinita siano già implementate all'interno dell'applicazione stessa. Il soggetto fornitore deve altresì garantire che l'applicazione è conforme alle misure di sicurezza del trattamento dei dati contemplate dall'Articolo 32 del Regolamento UE 679/2016 e produrre adeguata documentazione a supporto di eventuali adesioni a codici di condotta (di cui all'articolo 40 del Regolamento UE 679/2016) o a meccanismi di certificazione approvati (di cui all'articolo 42 del Regolamento UE 679/2016).

2.1.4. Impostazione fisica e logica dei dati

La soluzione dovrà garantire un elevato grado di flessibilità di gestione dei dati, di modellazione delle logiche di elaborazione e dei processi, per consentire il rapido e agevole recepimento delle evoluzioni normative e procedurali;

- Il software dovrà consentire ad un operatore anche non formato agevolezza nella fruizione;
- La soluzione dovrà basarsi su un DBMS – *Database Management System* relazionale fra quelli più diffusi disponibili sul mercato dei sistemi *enterprise* di tipo *open source* e gratuito.

2.1.5. Architettura WEB (gestionale)

La soluzione non deve necessitare dell'installazione di macchine virtuali e/o *plug-in* sulle postazioni di lavoro (PDL).

Inoltre, deve consentire il rispetto dei requisiti massimi di sicurezza previsti per legge e poter operare in protocollo HTTPS con utilizzo del certificato Wildcard già in possesso della Stazione Appaltante.

Il software applicativo dovrà essere in grado di operare sui principali browser presenti sul mercato (Mozilla Firefox, Chrome, Edge) indipendentemente dal sistema operativo utilizzato dall'utente. Il sistema dovrà essere fruibile anche da *smartphone*, *tablet* e smart TV aventi installati i sistemi operativi minimi quali IOS 10.x ed Android 9.x e successive versioni.

2.1.6. Disponibilità di adeguati strumenti di interfacciamento automatico

Al fine di garantire una reale integrazione di tutte le banche dati e le funzionalità applicative trasversali, interne od esterne al sistema, e di minimizzare quindi la quantità di operazioni da parte delle entità periferiche, il software gestionale dovrà prevedere la disponibilità di adeguati strumenti di interfacciamento automatico dei dati e delle funzionalità trasversali gestiti con quelli delle altre applicazioni usate dalla Stazione Appaltante (e.g.: Web Service, processi batch di integrazione, API, possibilità di definire processi CUSTOM specifici per la Stazione Appaltante).

2.1.7. Aggiornamenti

Deve essere garantita la manutenzione adattiva, nel caso vengano rilasciate nuove versioni dei sistemi operativi che potrebbero compromettere il corretto funzionamento delle diverse funzionalità previste nell'app. o nuove versioni dei sistemi operativi che garantiscano livelli di sicurezza superiori.

Deve essere garantita la manutenzione correttiva, nel caso vengano riscontrate delle problematiche o dei malfunzionamenti, o nel caso siano necessari degli aggiornamenti atti a garantire un più elevato livello di sicurezza dell'intero sistema e dell'infrastruttura.

Nell'ottica di servizio SaaS, dovranno essere garantiti tutti gli aggiornamenti di Sistema necessari al corretto funzionamento dell'infrastruttura e dell'interfacciamento con terze parti.

2.1.8. Servizi in fase di transizione in uscita

Alla data di rilascio del prodotto finale, i dati e il codice presenti nella piattaforma dovranno essere resi disponibili ad AdSP MAO secondo le specifiche tecniche che saranno concordate con il fornitore, in base alle indicazioni che saranno fornite da AdSP MAO. Dovrà essere fornito tutto quanto necessario affinché la stazione appaltante possa subentrare nella gestione delle attività mediante altro servizio analogo o una soluzione applicativa appositamente identificata.

L'Affidatario dovrà fornire tutta la documentazione aggiornata relativa a software, basi dati, interfacce.

Una eventuale fase di passaggio ad un nuovo sistema o ad una nuova gestione non dovrà comportare alcuna interruzione di servizio per gli utenti e il fornitore dovrà supportare per la migrazione alla soluzione applicativa subentrante.

2.1.9. Assistenza

E' previsto ed incluso nel presente affidamento il servizio di assistenza per due anni dalla data del rilascio del prodotto finito e testato, a garanzia delle funzionalità della parte gestionale e della disponibilità all'uso della app, tramite un opportuno sistema di ticketing concordato dalle parti, secondo le seguenti specifiche:

- tutti i servizi dovranno essere attivi 365 giorni all'anno, 24 ore su 24 per ogni giorno dell'anno;
- deve essere previsto un servizio di reperibilità che garantisca la continuità dei servizi in caso di malfunzionamenti hardware o software bloccanti.

I tempi di intervento massimi richiesti per la risoluzione delle anomalie sono regolati dalle seguenti SLA:
Per "risoluzione" si intende il ripristino completo delle funzionalità.

Item	Tipologia	Tempo di presa in carico	Tempo di ripristino
1	Problema bloccante	Entro 1 ora lavorativa dalla segnalazione di malfunzionamento da parte dell'Adsp	Entro 4 ore dalla presa in carico
2	Problema non bloccante	Entro 1 ora lavorativa dalla segnalazione di malfunzionamento da parte dell'Adsp	Entro 24 ore dalla presa in carico

2.1.10. Accessibilità

La app dovrà soddisfare i requisiti tecnici per l'accessibilità secondo le Linee Guida sull'accessibilità degli strumenti informatici, così come disposto sall'art.11 della L. n. 4 del 9 gennaio 2004, incluse le validazioni con i software di controllo e la conseguente dichiarazione di accessibilità da riportare all'interno della home della stessa app.

3. FIGURE PROFESSIONALI, TEMPI DELL'APPALTO E DOCUMENTAZIONE

3.1 Figure professionali richieste

Prima dell'inizio della realizzazione l'impresa aggiudicataria dovrà comunicare la composizione del proprio gruppo di lavoro, evidenziando il referente del progetto, il responsabile tecnico e il responsabile del servizio di assistenza, con i relativi riferimenti di contatto.

Il gruppo di lavoro deve garantire l'efficiente esecuzione di quanto previsto dal presente Capitolato.

Il personale impiegato deve possedere adeguate formazione e competenza in merito alle specifiche attività richieste ed è tenuto al rispetto del segreto professionale (art. 622 del C.P.) su fatti e circostanze concernenti l'organizzazione e la documentazione dell'AdSP MAO dei quali abbia avuto notizia durante l'esecuzione dell'appalto.

Verranno convocate riunioni di coordinamento (da remoto o in presenza), concordate o su esplicita richiesta dell'AdSP MAO, riguardo lo stato di avanzamento del progetto, eventuali problematiche insorte o questioni aperte di carattere strategico/metodologico da sottoporre all'attenzione dell'AdSP MAO (es. problematiche relative all'interfacciamento tra sistemi.

3.2 Data conclusiva dell'appalto

La versione finale della app e del gestionale dovranno essere consegnati entro il 28 febbraio 2023, e la app dovrà essere online il 1° marzo 2023.
Il ciclo di vita del software prevede una fase finale di manutenzione e assistenza (definite ai precedenti pti 2.1.8. e 2.1.10) previsti e inclusi nel presente capitolato per i due anni conseguenti il rilascio del prodotto software (app+ gestionale).

3.3 Esecuzione del servizio

Verrà eseguito il controllo di coerenza tra quanto richiesto dal presente Capitolato e quanto realizzato.

3.4 Modalità di pagamento

Il compenso verrà erogato in un'unica soluzione al termine del servizio ed a seguito dell'esito positivo della verifica di esecuzione del servizio con relativa emissione del certificato. I pagamenti sono effettuati nei termini di cui al D.Lgs. 9 ottobre 2001, n. 231.

La fattura dovrà essere accompagnata da una relazione tecnico-descrittiva analitica con il dettaglio delle attività svolte.

3.6 Fornitura documentazione finale

All'atto di chiusura dell'affidamento, l'operatore economico dovrà fornire la documentazione qui di seguito elencata, come da linee guida per la sicurezza nel procurement ICT (AgID). Sarà cura dell'Ente verificare che tale documentazione sia rilasciata dall'aggiudicatario completa e conforme.

- Manuali tecnici relativi all'utilizzo dei diversi moduli dell'App sia Mobile che del Gestionale;
- Report degli *Assessment* di Sicurezza eseguiti con indicazione delle vulnerabilità riscontrate e le azioni di risoluzione/mitigazione apportate;
- Indicazione dei prodotti software utilizzati e loro versione (ad esempio web server, application server, CMS, DBMS), librerie, firmware;
- Indicazioni sul processo di installazione degli aggiornamenti di sicurezza.
- Architettura logica generale dell'APP con descrizione dei moduli costituenti e dei loro collegamenti
- Architettura del database
  Documentazione delle Classi e dei principali Metodi, in particolare quelli utilizzati nelle interfacce

3.6.1 Integrazione ed interfacciamento con altri sistemi

Nella documentazione che dovrà fornire l'affidatario, dovrà essere presente un documento di sintesi che presenti tutte le possibili modalità con cui le informazioni contenute nel sistema possano essere esportate verso sistemi esterni oppure importate da sistemi esterni (es.Web Services SOAP o Rest , esportazione files, formato XML, Json ecc.) al fine di consentire la piena interoperabilità o, in altri casi, il riversamento/importazione di dati con altre componenti dei sistemi informativi aziendali. L'appaltatore dovrà predisporre e mantenere in uso un adeguato sistema di archiviazione e di consultazione elettronica di tutti i documenti, gli atti, i fatti e le manifestazioni di volontà prodotti o generati dall'interazione degli utenti interni ed esterni con il sistema, osservando tutte le disposizioni normative e regolamentari vigenti in materia, mantenendo la documentazione consultabile per tutta la durata contrattuale sia per quel che riguarda la documentazione inerente le procedure di estrazione, sia per quel che riguarda tutta la documentazione inerente gli operatori economici. Dovrà essere assicurato, inoltre, un adeguato livello di back up del software e dei dati, tale da garantire, oltre all'eventuale ripristino in caso di problemi alla base dati, l'efficace e adeguato completamento della fase di transizione in uscita, secondo le modalità ed i livelli di servizio indicati nel paragrafo dedicato all'interno del presente documento.

4. IMPORTO A BASE D'APPALTO

L'importo a base d'appalto è stato calcolato sulla stima delle attività previste nelle due fasi:

- prima fase – consegna del prodotto software completo (app + gestionale)
- seconda fase - manutenzione ed assistenza del prodotto software completo (app + gestionale) prevista per i due anni seguenti il rilascio del software, hosting incluso

sulla base di quanto previsto dal D.M. 17 giugno 2016 del Ministero della Giustizia – "Approvazione delle tabelle dei corrispettivi commisurati al livello qualitativo delle prestazioni di progettazione, adottato ai sensi dell'art. 24, comma 8, del D. lgs. n. 50 del 2016", art. 6, comma 2 lettere a, b e c, con riferimento alle seguenti figure professionali e relativi costi come indicato nella tabella seguente:

Figura professionale	Figura tecnica professionale ICT	Costo giornata
Professionista incaricato	Project Manager/Senior Analyst - Responsabile analisi e coordinamento risorse umane	€ 600,00
Aiuto iscritto	Programmatore/Sviluppatore	€ 400,00
Aiuto iscritto	Data Base Architect	€ 400,00
Aiuto iscritto	Sistemista	€ 400,00
Aiuto di concetto	Help desk	€ 296,00

ottenendo i seguenti importi:

	NOME SERVIZIO	DETTAGLIO SERVIZIO	Importo
1	Sviluppo APP	1.1 Design UI	€ 59.360
		1.2 Comunicazioni e notifiche	
		1.3 Supporto multilingua	
		1.4 Gestione login e registrazione	
2	Sviluppo Gestionale	2.1 Design UI	€ 110.160
		2.2 Data base	
		2.3 Comunicazioni con APP	
		2.4 Comunicazioni con piattaforme di terze parti	
		2.5 Aspetti di sicurezza informatica	
3	Mantenimento, assistenza e formazione	3.1 Hosting modalita SAAS - due anni	€ 30.320
		3.2 Manutenzione ordinaria ed evolutiva ed aspetti di sicurezza informatica	
		3.3 Formazione agli operatori	
		3.4 Help desk	

In base a quanto sopra, l'importo a base di gara, al netto di oneri e dell'I.V.A., è pari ad € 200.000 (duecentomila/00).

Ai sensi dell'art. 26, comma 3-bis del D.lgs. 81/2008, trattandosi di un servizio di natura intellettuale, non sussiste l'obbligo di redazione del DUVRI ed i costi per la sicurezza non soggetti a ribasso sono pari a €. 0 (zero).

L'importo a base di gara è al netto di Iva e/o di altre imposte e contributi di legge.

5. OBBLIGHI DELL'AGGIUDICATARIO

L'aggiudicatario dovrà garantire il corretto svolgimento dei servizi oggetto di incarico ed assumere tutti i necessari accorgimenti per espletare gli stessi nel rispetto delle indicazioni riportate nel presente capitolato tecnico, anche per le attività che richiedono una collaborazione con soggetti terzi, secondo i termini e le modalità contenute nell'offerta presentata e nell'ambito degli indirizzi e delle direttive fissati dalla scrivente Autorità.

È fatto obbligo all'Impresa aggiudicataria di:

- fornire la massima collaborazione agli uffici dell'Ente durante tutto il periodo contrattuale per espletare nel miglior modo possibile l'incarico assegnato;
- comunicare, entro 5 gg. dall'aggiudicazione definitiva, il nominativo del soggetto incaricato della gestione dell'appalto e della fatturazione, nonché il numero fax e l'e-mail al quale inoltrare tutte le comunicazioni relative all'appalto ed il recapito telefonico (anche di cellulare) del referente responsabile della ditta stessa, impegnandosi a comunicare eventuali variazioni alla scrivente Autorità;
- comunicare qualsiasi modifica che possa intervenire nella gestione organizzativa;
- provvedere tempestivamente, qualora la scrivente Autorità, con apposita segnalazione, evidenziasse criticità nell'esecuzione delle attività, all'adozione dei rimedi necessari ed idonei a risolvere le anomalie riscontrate;
- sostenere tutte le spese contrattuali inerenti e conseguenti al servizio aggiudicato;
- comunicare qualsiasi modifica possa intervenire nel sistema di gestione della attività in oggetto, nonché qualsiasi variazione circa il possesso dei requisiti di ordine generale di cui all'art. 80 del D.lgs. 50/2016;
- rispettare la normativa sulla riservatezza. Le notizie comunque venute a conoscenza del personale dell'aggiudicatario, non devono essere comunicate o divulgate a terzi, né possono essere utilizzate da parte della medesima, o da parte di chiunque collabori alla sua attività, per fini diversi da quelli contemplati nel presente atto.

L'aggiudicatario si impegna inoltre a non utilizzare per finalità diverse ed estranee al progetto, né a diffondere, la documentazione elaborata dalla scrivente Autorità e di sua esclusiva proprietà.

Il committente si riserva la possibilità di agire per le vie legali nel caso di notizie di cessione delle informazioni a terzi, attività in palese violazione con la protezione dei dati concessi dagli operatori della comunità portuale.