

Capitolato Tecnico

CAPITOLATO TECNICO

GARA EUROPEA A PROCEDURA APERTA TELEMATICA PER L'APPALTO DEL SERVIZIO
DI MANUTENZIONE CORRETTIVA ED EVOLUTIVA DEGLI APPLICATIVI
- PORTALE STRUMENTI – PDA – GST
GIÀ IN ESERCIZIO NELL'INFRASTRUTTURA ISMEA, BASATI SU FRAMEWORK LIFERAY E
PERSONALIZZATI IN JAVA ED ALTRI LINGUAGGI - CIG 91886390C8

1. Premessa

Ismea è dotata di una serie di applicativi, già in esercizio nell'infrastruttura, basati su Framework *Liferay* e personalizzati in Java ed altri linguaggi, utilizzati per le proprie attività istituzionali ed in particolare per quelle legate alla gestione dei servizi erogati agli utenti esterni ed interni di Ismea.

Al fine di garantirne il corretto funzionamento ed assicurarne gli interventi di sviluppo e di implementazione, ha la necessità di dotarsi di un **servizio di manutenzione correttiva ed evolutiva**.

L'appalto per il servizio oggetto del presente capitolato avrà una durata di 24 mesi, con possibilità di rinnovo per una ulteriore annualità.

2. Oggetto del servizio

Ismea necessita di una società che eroghi il servizio di assistenza, manutenzione ed implementazione per gli applicativi di seguito elencati:

1. Il Portale per la presentazione delle domande *on line*, denominato **Portale Strumenti**
2. L'applicazione per la generazione dei Piani di Ammortamento – **PDA**
3. Il **connettore contabile** per la contabilizzazione delle rate di PDA e dei relativi incassi
4. La piattaforma per la gestione dei servizi interni ad uso del personale ISMEA, denominata **GST**
5. Il **fascicolo aziendale** interno
6. La **protocollazione automatica**
7. I **collegamenti (Web Services o altri protocolli) già esistenti tra gli applicativi ISMEA**, di seguito elencati
 - I. WS tra il portale strumenti ed il gestionale Istruttorie
 - II. WS tra il portale strumenti ed il sistema documentale Web Rainbow (WR)
 - III. Client di autenticazione tra il portale strumenti e il sistema unico di autenticazione SSO ISMEA (CAS)
 - IV. WS tra il gestionale Istruttorie e PDA
 - V. Connessione Data base tra PDA ed il connettore contabile
 - VI. *Concurrent* tra il connettore contabile e la contabilità
 - VII. WS tra portale strumenti e fascicolo aziendale SIAN
 - VIII. Integrazione con anagrafica unica ISMEA da portale strumenti e da PDA

Di seguito un dettaglio sui singoli applicativi oggetto del presente capitolato:

Portale Strumenti

Si tratta di un portale che gestisce l'inserimento, da parte di utenti esterni, delle domande di accesso agli strumenti finanziari erogati da ISMEA, nonché di altre tipologie di domande di partecipazione a

concorsi o progetti messi a disposizione di ISMEA. Il portale è raggiungibile all'indirizzo strumenti.ismea.it.

L'utente si autentica con il sistema CAS ISMEA, seleziona lo strumento a cui intende aderire ed inserisce la domanda con tutti gli allegati.

Il portale fornisce documenti PDF ed Excel compilati con i dati inseriti nelle *form*. Al momento non è gestita la firma elettronica delle pratiche.

ISMEA si riserva di valutare l'opportunità di integrare tale funzionalità prossimamente.

Al termine dell'operazione la domanda viene convalidata e l'utente riceve una PEC di conferma della convalida. La domanda viene automaticamente protocollata ed è generata una nuova PEC di conferma per l'utente. Il risultato delle domande è consultabile con una interfaccia apposita.

L'applicativo è integrato e scambia dati, via WS o altri protocolli:

- con il sistema di autenticazione CAS ISMEA per l'autenticazione e la profilazione degli utenti;
- con il fascicolo aziendale SIAN per la lettura delle informazioni catastali dei terreni interessati;
- con il prodotto ISMEA BPOL per la generazione dei *business plan* aziendali;
- con il protocollo aziendale per la protocollazione automatica delle domande (WR);
- con il gestionale Istruttorie per la trasmissione delle domande ricevute.

Il prodotto è operativo dal 2016 e ha ricevuto circa 5.000 domande/anno, con picchi di 10 domande al minuto in occasione delle chiusure dei bandi principali.

PDA

Tale applicativo gestisce la generazione di piani di ammortamento a seguito delle domande presentate. I piani di ammortamento gestiti sono realizzati secondo le specifiche dei vari regimi, comprendendo piani di tipo francese (a rate costanti) o italiano (a quota capitale costante); sono gestiti aiuti in conto interessi e in conto capitale.

Inoltre, sono gestiti i principi contabili che prevedono l'attualizzazione dei debiti e delle rate.

È attiva un'anagrafica di regimi, nella quale vengono impostati i parametri necessari alla generazione dei piani di ammortamento (tipo di ammortamento - numero di rate di preammortamento - possibile numero di rate complessivo - tipo di premio - informazioni contabili - ecc).

I piani di ammortamento sono modificabili a seguito di interventi di assistenza.

Sono previste diverse tipologie di assistenze, alcune di queste, modificando il debito residuo o la rata, generano effetti contabili. Il sistema applica la modifica attraverso un movimento apposito nel PDA, mantenendo identificabile la variazione.

È prevista una funzione di generazione di distinte per la trasmissione alla contabilità ISMEA delle rate in scadenza, dei movimenti di assistenza, delle attualizzazioni dei debiti e delle rate, dell'apertura di nuovi piani e di nuovi crediti.

Capitolato Tecnico

La distinta scrive in Oracle EBS su apposite tavole di confine e legge il risultato dell'importazione. L'importazione vera e propria è a cura del gruppo di supporto EBS.

Le distinte sono estratte per tipologia di operazione e per regime, oltre che per data di scadenza. Le rate o i movimenti già contabilizzati sono esclusi dalle distinte.

Il sistema dialoga via *web services* con l'applicativo istruttorie.

Gli utenti sono definiti in *Active Directory*. Per il *login* è necessario testare l'appartenenza ad un gruppo specifico, che determina anche la profilazione dell'utente.

CONNETTORE CONTABILE

Si tratta di una procedura che si occupa di convertire i dati provenienti dal gestionale PDA per poi inviarli al sistema contabile Oracle.

Questo progetto, molto complesso tecnicamente in quanto mette in comunicazione sistemi con linguaggi e tecnologie differenti, necessita di interventi di manutenzione correttiva ed evolutiva per perfezionare il funzionamento ed intervenire su possibili malfunzionamenti che emergono in corso di utilizzo.

L'architettura della procedura può essere riassunta in tre macroaree:

- Il gestionale PDA prepara le distinte di contabilizzazione su tavole di confine estraendo i movimenti che vanno contabilizzati (rate, variazioni di PDA, aperture di pratica, anagrafiche dei beneficiari e altri soggetti come i venditori)
- lo *script* Connettore Contabile converte i dati su tavole *custom* di Oracle e legge i dati di ritorno da Oracle aggiornando lo stato delle distinte su PDA;
- un *concurrent* Oracle valida i dati e li importa dalle tavole *custom* alle tavole standard di confine Oracle. Da qui, un secondo *concurrent* importa i dati in contabilità (EBS), un terzo *concurrent* che gestisce il flusso di ritorno verso lo *script* Connettore Contabile.

GST

Si tratta di una piattaforma ad uso interno degli utenti ISMEA, basata su *framework Liferay*, attraverso la quale vengono gestiti una serie di servizi, quali:

- I. il sistema di *trouble-ticketing* per gestire le richieste di assistenza utenti da parte dell'HDK ISMEA
- II. la rubrica telefonica
- III. la prenotazione sale riunioni
- IV. il magazzino / inventario per la gestione degli *asset*
- V. il sistema di Brokeraggio per la registrazione ed il monitoraggio degli utenti ISMEA che si rivolgono all'URP o ad altre Direzioni.

FASCICOLO INTERNO

Capitolato Tecnico

Si tratta di una procedura che, partendo da una lista di CUA, interroga il fascicolo SIAN via *Web Service* memorizzando su base dati locale informazioni relative all'azienda interrogata, alla composizione catastale del terreno e dei fabbricati e altre caratteristiche. La procedura gira automaticamente ogni notte, inviando una mail di risultato.

PROTOCOLLAZIONE AUTOMATICA

La procedura consente ad altre applicazioni di collegarsi mediante *Web Services* alla parte relativa alla protocollazione di una domanda e dei suoi allegati. Ad oggi è utilizzata da un applicativo, denominato "Banca della Terra", per protocollare in automatico le manifestazioni di interesse.

COLLEGAMENTI TRA I SISTEMI

I diversi applicativi utilizzati dagli utenti ISMEA, sia interni sia esterni, precedentemente elencati, sono stati messi in collegamento tra loro attivando una serie di protocolli di scambio dati, in modo tale da consentire la messa a sistema dei dati. Questi scambi dati sono oggetto di una continua manutenzione correttiva ed evolutiva per adeguarsi ai cambiamenti degli applicativi.

Sugli applicativi sopra descritti, l'aggiudicatario dovrà realizzare interventi di manutenzione correttiva, integrazione applicativa tra i sistemi e di manutenzione evolutiva.

Le modifiche da realizzare dovranno integrarsi con le procedure già presenti, senza modificarne o interromperne le funzionalità e dovranno obbligatoriamente essere sviluppate utilizzando la stessa tecnologia dell'applicazione originale.

Nei paragrafi che seguono sono descritti i servizi richiesti.

2.1. Servizio di help desk- Interventi di manutenzione correttiva e assistenza utenti

Si tratta di interventi di manutenzione ordinaria, di sistemazione, di aggiustamenti e di eliminazione di bug che impediscono o rallentano l'utilizzo degli applicativi oggetto del presente bando.

Tali interventi dovranno essere gestiti da un servizio di HDK messo a disposizione del fornitore e attivato attraverso un sistema di *trouble-ticketing* che permetta di tracciare:

- Giorno e ora di apertura della richiesta da parte di ISMEA;
- Presa in carico del ticket (entro 4 ore dall'apertura) con l'indicazione del tempo di risoluzione stimato;
- Chiusura del ticket.

Per questa attività è richiesto un servizio di help desk a cura del fornitore dalle 9,00 alle 18,00, dal lunedì al venerdì.

Si riporta nella tabella 1, solo a titolo **indicativo e non esaustivo**, una sintesi delle tipologie più significate delle attività richieste scaturite dal sistema di *trouble-ticketing* di Ismea, nell'ultimo triennio di manutenzione.

Tab. 1 – Interventi “tipo” per l’attività 2.1 - Servizio di help desk PORTALE, PDA E GST a CANONE

| N. | Interventi “tipo” |
|----|--|
| 1 | creazione e profilazione utenze |
| 2 | interventi correttivi su malfunzionamenti registrazione al portale |
| 3 | interventi correttivi su malfunzionamenti PDA |
| 4 | interventi correttivi su malfunzionamenti web services con altri applicativi |
| 5 | interventi correttivi su malfunzionamenti Piattaforma GST |
| 6 | interventi correttivi su malfunzionamenti Connettore Contabile |
| 7 | Assistenza al caricamento dati su Connettore contabile ad ogni scadenza di rata (mensile, semestrale e annuale), e a chiusura di bilancio (da PDA a Sistema contabile Oracle). |

Il servizio di help desk dovrà utilizzare il sistema di *trouble ticketing* ISMEA attraverso le seguenti fasi:

- ricezione delle richieste/ticket aperti dagli utenti, attraverso l’applicativo proprietario GST;
- presa in carico della richiesta **entro le 4 ore lavorative successivo all’apertura**.
- notifica agli utenti dell’ipotesi di soluzione delle richieste avanzate;
- risoluzione dei malfunzionamenti segnalati, laddove possibile;
- test di funzionamento con l’utente;
- notifica del ripristino delle funzionalità
- chiusura del ticket
- Tempi di risoluzione, per ripristino funzionalità già esistenti: **entro 3h lavorative dalla presa in carico**

2.2. Manutenzione evolutiva e sviluppi di nuove funzionalità a richiesta

Per gli applicativi oggetto del presente Capitolato, potranno manifestarsi esigenze di aggiornamenti procedurali, implementazione di nuove procedure, creazione di nuovi portali e, più in generale, necessità di sviluppi evolutivi a richiesta.

A seguito della richiesta di ISMEA, dunque, il fornitore dovrà produrre un’analisi dettagliata di tempi e costi, espressi in giorni/uomo, con il dettaglio delle figure professionali impiegate per la realizzazione. Solo a seguito di approvazione dell’analisi da parte di ISMEA il fornitore potrà procedere con l’attività.

Nella tabella 2, al fine di fornire elementi utili per la formulazione dell’offerta, per ciascuna tipologia viene riportato il numero degli interventi richiesti nell’ultimo triennio, espresso sia come numero di richieste che di fabbisogno di giornate uomo.

Capitolato Tecnico

Tab. 2 - Tipologia di interventi richiesti per l'attività 2.2 - Manutenzione evolutiva e sviluppi di nuove funzionalità a richiesta

| <i>PORTALE STRUMENTI, PDA e CONNETTORE</i> | | Dati riferiti a 3 anni | |
|--|--|------------------------|--------------|
| N. | Tipo di intervento | Numero di interventi | Tot. Gg/uomo |
| 1 | Realizzazione di nuovi Bandi per Regimi di finanziamento già esistenti sul Portale Strumenti | 2 | 10 |
| 2 | Realizzazione di nuovi Regimi di finanziamento sul Portale Strumenti | 15 | 150 |
| 3 | Creazione PDA per i nuovi regimi | 15 | 150 |
| 4 | Implementazione dei PDA in relazione a: assistenze, rinvii rate e/o rimodulazione piano, cambio tasso, cambio durata, riscatto anticipato, cambio periodicità. | 28 | 280 |
| 5 | Bonifica dati di piani importati da sistemi dismessi che richiedono interventi su DB (RIFO, Subentro, Finanza agevolata) | 12 | 120 |
| 6 | Implementazione algoritmo per attualizzazione dei crediti in base ai principi contabili | 6 | 60 |
| 7 | Restyling della domanda on line per i diversi regimi attivati (grafica e architettura) | 3 | 30 |
| 8 | Sviluppo nuovi Web Services tra il gestionale PDA, Protocollo, Connettore contabile e il gestionale Istruttorie e viceversa. | 15 | 15 |
| 9 | Generazione della stampa dei PDA in diversi formati (pdf – Excel – Word) | 15 | 30 |
| 10 | Integrazione tra PDA e Connettore Contabile | 18 | 18 |
| Totale | | | 863 |
| <i>PIATTAFORMA GST</i> | | Numero di interventi | Tot. Gg/uomo |
| 1 | Adeguamento piattaforma per nuove tipologie di richieste | 3 | 90 |
| N. | Tipo di intervento | Numero di interventi | Tot. Gg/uomo |
| 1 | Arricchimento del fascicolo interno di nuove informazioni rilasciate dal SIAN sul fascicolo Aziendale | 1 | 19 |
| 2 | Reingegnerizzazione e integrazione tra Portale/PDA e Anagrafe Unica | 1 | 28 |
| Totale | | | 47 |
| Totale complessivo | | | 1.000 |

Su richiesta di ISMEA l'aggiudicatario dovrà far fronte ad eventuali ulteriori interventi, di natura straordinaria, e quindi non ricompresi nelle attività di cui ai punti precedenti; per tali interventi è previsto un separato budget (si rimanda al disciplinare di gara).

2.3. Formazione utente/programmatore a richiesta

Potrà essere richiesta la fornitura di giornate formative da erogare su richiesta per uno/due utenti ISMEA con profilo da amministratore/programmatore per poter intervenire sulla piattaforma ed apportare le eventuali modifiche che potrebbero rendersi necessarie a seguito di cambiamenti normativi e/o procedurali.

2.4. Documentazione tecnica e Manuale utente

Al completamento di ogni intervento per sviluppi evolutivi di nuove funzionalità e per adeguamenti normativi, il fornitore dovrà trasferire agli utenti le necessarie competenze attraverso la redazione di documentazione ad hoc da rilasciare contestualmente alla messa in esercizio della nuova funzione.

In particolare, per ciascun intervento rilasciato sul sistema dovrà essere prodotto:

- il manuale utente, contenente informazioni sufficienti ad un orientamento nel funzionamento operativo della procedura. Il documento sarà in formato elettronico, editabile. Si richiede un rilascio in formato Microsoft Word (.docx);
- la documentazione tecnica della procedura, mediante commenti esaustivi nel codice applicativo e nella struttura dati. La documentazione del codice dovrà specificare l'uso di ogni classe e funzione, indicando tipo e utilizzo dei parametri di ingresso e di uscita. Il codice all'interno delle classi dovrà essere documentato dove opportuno;
- un documento che dettagli l'architettura della procedura e della base dati con le relazioni fra le classi e lo schema della struttura dati, con relative integrazioni. Nel caso di utilizzo di semilavorati, come framework o CMS, sarà sufficiente documentare le personalizzazioni al prodotto di base.

La documentazione dovrà essere rilasciata entro 7 gg lavorativi dalla messa in produzione della nuova funzionalità, dovrà essere approvata dall'ufficio IT ISMEA e sarà parte integrante del collaudo.

3. Tabella riepilogativa dei servizi richiesti e relative tempistiche

| Servizio | Valore soglia |
|---|---|
| Servizio di Help Desk (2.1 del presente capitolato) | Tempo di presa in carico del ticket: entro 4h lavorative dall'apertura del ticket Rispetto del tempo di risoluzione: Collaudo entro la data specificata nel ticket |

Capitolato Tecnico

| | |
|---|---|
| Servizi a richiesta (2.2 – 2.3 del presente capitolato) | <ul style="list-style-type: none"> • Tempo di invio del programma di intervento comprensivo dell'offerta: entro 4 gg lavorativi dalla richiesta di Ismea; • Rispetto del programma di intervento: Collaudo entro la data specificata nel programma di intervento. |
| Rilascio Documentazione (2.4 del presente capitolato) | <ul style="list-style-type: none"> • Entro 7 gg dalla messa in produzione |

4. Team dedicato

Per team dedicato si intende l'insieme delle risorse che il fornitore dovrà mettere a disposizione per l'esecuzione delle attività oggetto del presente capitolato, anche in caso di eventuale subappalto, sulla base dei profili professionali indicati di seguito e che, quindi, indicherà nella proposta tecnica. L'aggiudicatario è responsabile dell'operatività e del coordinamento del suddetto team.

Per ciascuna delle figure professionali richieste, il concorrente dovrà evidenziare gli anni di esperienza maturati nel profilo di seguito riportato, allegando anche un dettagliato Curriculum Vitae.

Il team di lavoro dovrà essere comprensivo almeno dei seguenti profili professionali richiesti per l'esecuzione dei servizi:

- **Project manager**, esperto nella gestione di progetti, nella raccolta requisiti utente, nel coordinamento e attribuzione delle risorse in base alle specifiche progettuali, anche con funzione di capo progetto al fine di organizzare le risorse umane e tecniche per il raggiungimento degli obiettivi sostanziali del progetto; **per tale figura è richiesto il possesso di un'esperienza professionale di almeno 5 anni su tecnologia Liferay.**
- **N. 1 Architetto software**, esperto nella progettazione ad alto livello, nella organizzazione strutturale dei sistemi, comprese le relazioni fra le sue componenti e l'interoperabilità con i sistemi circostanti, nonché nell'evoluzione dei sistemi in termini di scalabilità, performance, manutenibilità, sicurezza, affidabilità, ecc.; **per tale figura è richiesto il possesso di un'esperienza professionale di almeno 5 anni su tecnologia Liferay.**
- **N. 1 Analista programmatore**, esperto nelle attività di analisi, progettazione e sviluppo sw sulla base di specifiche tecniche e requisiti utente; **per tale figura è richiesto il possesso di un'esperienza professionale di almeno 3 anni su tecnologia Liferay e Java.**
- **N.1 Grafico/Web designer**, esperto nella creazione dei vari elementi dell'interfaccia grafica ad uso utente; **per tale figura è richiesto il possesso di un'esperienza professionale di un'esperienza professionale di almeno 3 anni.**

Capitolato Tecnico

Si sottolinea che le risorse umane presentate come Team di lavoro in sede di gara dovranno corrispondere alle risorse che saranno effettivamente impiegate nelle attività, fermo restando sostituzioni che potranno intervenire in corso d'opera, a partire dal **sesto mese** dall'avvio del contratto, ma che dovranno essere formalmente giustificate con valida motivazione che la stazione appaltante si riserverà di accettare. Si precisa che la sostituzione potrà essere ammessa solo se i sostituti presentino requisiti di valore analogo o più qualificato (anche in termini di anni di esperienza) rispetto a quello delle persone sostituite.

5. Penali

In caso di inadempimento dell'aggiudicataria relativamente ai tempi e/o alla modalità di esecuzione definite nel presente capitolato tecnico e/o concordate con ISMEA, saranno applicate le penali espresse in tabella:

| Penali rispetto ai livelli di servizio | | |
|--|---|--|
| Nome indicatore | Valore soglia | Penale |
| Tempo di presa in carico del ticket per il servizio di helpdesk (2.1) | Entro 4h dall'apertura del ticket. | 100 euro per ogni ora di ritardo rispetto al valore soglia |
| Tempi di ripristino di funzionalità già esistenti ma andate in errore, di cui all'elenco del punto 2.1 | entro 3h lavorative dalla presa in carico (o dall'indicazione di riavvio del sistema) | 100 euro per ogni ora di ritardo rispetto al valore soglia |
| Tempo di invio del programma di intervento per i servizi a richiesta (2.2 – 2.3), comprensivo dell'offerta economica | Entro 4 gg lavorativi dalla richiesta di Ismea. | 200 euro per ogni gg di ritardo rispetto al valore soglia |
| Rispetto del programma di intervento (2.2 – 2.3) | Rilascio per Collaudo entro la data specificata nel programma di intervento. | 200 euro per ogni gg di ritardo rispetto al valore soglia |
| Tempo per il rilascio della documentazione (2.4) | Entro 7 gg dal rilascio in produzione della nuova funzionalità | 100 euro per ogni gg di ritardo rispetto al valore soglia |

6. Clausole di sicurezza delle informazioni

- Conformità agli standard industriali:** il fornitore utilizzerà politiche, standard e controlli organizzativi, amministrativi, fisici e tecnici per proteggere i dati ISMEA contro il trattamento non autorizzato o

Capitolato Tecnico

illegittimo e contro la perdita accidentale, la distruzione o la violazione. Tali misure saranno ispirate agli attuali standard industriali accettati (quali a titolo esemplificativo: *NIST Cyber Security Framework*, *ISO/IEC 27001/27002*) e conformi alle leggi applicabili riguardanti la protezione dei dati personali.

Per il periodo in cui il fornitore avrà accesso ai dati ISMEA o a suoi sistemi/reti, aggiornerà le sue pratiche e controlli di sicurezza a proprie spese per continuare a ottemperare gli standard industriali accettati.

2. **Audit:** su richiesta di ISMEA, e di norma non più di una volta l'anno a meno che non vengano identificati un rilievo materiale o anomalia, il fornitore garantisce a ISMEA il permesso e tutti gli accessi necessari alle strutture e sistemi del fornitore al fine di condurre un audit di conformità. Il fornitore collaborerà nel corso dell'audit fornendo accesso al personale competente, ai locali, ai sistemi/reti, alle politiche, agli standard, alla documentazione, e quando possibile agli stessi strumenti usati dalle società subappaltatrici del fornitore per prestare servizi a o per conto di ISMEA. Il fornitore non è obbligato a rilasciare o rendere disponibile alcun Sistema o informazione che sia una informazione riservata di terze parti. A sue spese, il fornitore dovrà prontamente rimediare a ogni risultanza dell'audit, e nel caso in cui il fornitore non sia d'accordo con tali risultanze, dovrà adoperarsi in buona fede per negoziare una strategia di mitigazione soddisfacente per le parti. Nell'eventualità che le parti non raggiungano un accordo su una strategia di compromesso, ISMEA avrà diritto di risolvere l'accordo con preavviso di 30 giorni a mezzo di comunicazione scritta senza alcuna sanzione, responsabilità o altra obbligazione. In alternativa, ISMEA potrebbe scegliere di accettare una verifica indipendente della conformità del fornitore con questo documento.
3. **Valutazione e Revisione:** il fornitore deve attuare un processo per testare, verificare e valutare regolarmente l'efficacia delle misure adottate al fine di garantire la sicurezza dei dati ISMEA.
4. **Crittografia:** il fornitore non conserverà informazioni proprietarie o relative a ISMEA su alcun dispositivo portatile o media (es. Laptop, flash drive, smartphone) che non impieghi la crittografia completa del disco (ove applicabile). Le informazioni riservate e i dati personali devono essere cifrati in transito e memorizzati nel rispetto degli standard industriali di cifratura accettati.
5. **Applicazioni abilitate per il web:** tutti i siti internet messi eventualmente a disposizione dal fornitore e integrati con sistemi ISMEA devono essere dotati di Web Application Firewall (WAF) regolati su standard industriali e devono essere scansionati e corretti utilizzando per le criticità relative alla sicurezza standard industriali accettati (es. *Open Web Application Security Project and Open Web Application Security Project Top 10*). Scansioni e ripristini devono essere completati prima del lancio della applicazione. Dopo il lancio, il fornitore condurrà controlli a una frequenza appropriata per la applicazione, la tecnologia e il rischio dei dati in questione. I siti web dovranno attuare e mantenere secondo standard industriali accettati i controlli di gestione account e password, incluso:
 - a. Blocco dopo non più di dieci tentativi di accesso non riusciti;
 - b. evitare la visualizzazione di ID utente, password e Dati Personali in un URL;
 - c. Memorizzazione delle password utente e delle domande di sicurezza reimpostate/dimenticate in modo crittografato;
 - d. La ri-autenticazione è necessaria dopo non più di 30 minuti di inattività;
 - e. evitare l'archiviazione di password o Dati Personali in memoria locale persistente (cache, ecc.) o in qualsiasi cookie, Javascript o altra tecnologia di tracciamento web.

6. **Sviluppo sicuro**¹: il fornitore adotterà misure tecniche e organizzative appropriate per garantire la consegna di codice sicuro come definito nelle *Linee Guida AGiD sullo sviluppo del software sicuro* e nello standard *OWASP Application Security Verification ("OWASP Verification Standard")*, inclusa, ma non solo, la gestione della configurazione avanzata, i test di sicurezza delle applicazioni, la prevenzione degli exploit di runtime e nessun codice open source vulnerabile. Lo sviluppo del fornitore non sarà completo fino a quando la sicurezza del codice e dell'applicazione non sarà stata dimostrata tramite un rapporto di sicurezza basato sullo standard di verifica OWASP. Tale rapporto di sicurezza deve essere fornito dal fornitore e rivisto e accettato da ISMEA.
7. **Consapevolezza e formazione**: il fornitore fornirà una formazione adeguata al rafforzamento della consapevolezza della sicurezza informatica a tutti i suoi dipendenti con accesso a informazioni o sistemi/reti ISMEA, trattando in particolare i requisiti di sicurezza di questo documento.
8. **Autenticazione avanzata**: nel caso dovesse integrare i suoi Servizi con i sistemi ISMEA. Il fornitore utilizzerà l'autenticazione a due fattori per i seguenti tipi di accesso:
 - a. Accesso privilegiato (ad es. accesso amministrativo a livello di sistema o database) a qualsiasi server e/o applicazione che ospita informazioni ISMEA;
 - b. Qualsiasi accesso remoto da parte del fornitore a informazioni ISMEA.
9. **Hosting**: il fornitore informerà ISMEA per iscritto ogni qual volta Dati Personali o dati ISMEA vengano memorizzati utilizzando un ambiente condiviso o cloud. Il fornitore proteggerà (o farà in modo che il suo subappaltatore protegga) tali dati utilizzando controlli rispettosi degli standard di settore accettati (ad esempio, *Cloud Security Alliance Cloud Controls Matrix*). Il fornitore collaborerà in buona fede per identificare un'alternativa a tale hosting se ISMEA dovesse farne richiesta. Il fornitore dovrà verificare tutte le patch di sicurezza rilevanti per l'ambiente e classificare la necessità e la priorità con cui esse devono essere installate, senza provocare discontinuità nel servizio.
10. **Exit strategy**: alla cessazione o alla scadenza del contratto, il fornitore restituirà tempestivamente tutte i dati a ISMEA, salvo che la legge ne preveda l'obbligatorietà della conservazione, nonché tutti gli apparati hardware e software eventualmente ricevuti in uso temporaneo.
11. **Distruzione dei dati**: dopo la restituzione, il fornitore distruggerà le informazioni ISMEA quando tali dati non sono più necessari né per l'esecuzione del contratto né per obbligo di legge. La distruzione avverrà utilizzando un mezzo sicuro di smaltimento, quali ad esempio per i supporti cartacei incenerimento o triturazione trasversale ovvero applicando per i dati memorizzati su supporto digitale metodologie di cancellazione sicura come richiamate ad esempio dalle norme D.o.D. oppure dalle indicazioni dell'Autorità Garante per la protezione dei dati personali.
12. **Gestione dei dispositivi**: il fornitore utilizzerà solo dispositivi aziendali configurati in modo sicuro (cioè dispositivi non BYOD o ibridi/di uso personale) per connettersi a reti e sistemi di ISMEA o per accedere o conservare informazioni ISMEA.
13. **Accesso**: il fornitore limiterà l'accesso ai sistemi di ISMEA e alle informazioni ISMEA alle persone autorizzate in base a necessità stringente e tali persone saranno tenute a rispettare un accordo di riservatezza. Il fornitore manterrà un processo che monitora e applica i diritti di accesso ai sistemi e alle informazioni di ISMEA. L'accesso wireless alle reti e ai sistemi di ISMEA deve avvenire tramite connessioni sicure (ad esempio VPN) e router wireless privati. Il fornitore assicurerà inoltre che i propri sistemi impediscano adeguatamente i tentativi di accesso da parte di utenti non autorizzati, ad esempio bloccando l'accesso dopo la ripetizione di un numero minimo di tentativi.

¹ Requisito non valido per il software già sviluppato, salvo migliorie di sicurezza volontariamente introdotte dal fornitore.

14. **Organizzazione della sicurezza:** il fornitore dovrà allestire una sua organizzazione per il monitoraggio e il miglioramento continuo della sicurezza delle informazioni e della data protection, corredata da un insieme di politiche e procedure approvate dalla direzione. Dovrà altresì fornire a ISMEA comunicazione dei referenti della sicurezza e della privacy.
15. **Amministratori di sistema:** laddove applicabile con l'oggetto del contratto, il fornitore dovrà provvedere alla nomina del proprio/i amministratore/i di sistema, in adempimento di quanto previsto dal provvedimento del Garante del 27.11.08, pubblicato in G.U. n. 300 del 24.12.2008, ove ne ricorrano i presupposti, comunicandolo prontamente a ISMEA, curando, altresì, l'applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento. Il fornitore dovrà inoltre mettere a disposizione i log su connessioni e accessi, includendo gli adempimenti per gli amministratori di sistema (salvo diverse indicazioni concordate) per i componenti che esso fornisce e di cui esegue la manutenzione tra sistemi operativi, database e applicativi.
16. **Adempimenti in caso di incidenti di sicurezza delle informazioni:** il fornitore dovrà risolvere le violazioni di sicurezza nel più breve tempo possibile fornendo adeguata reportistica e tempestive segnalazioni a ISMEA.

7. Modalità di pagamento

Il pagamento del corrispettivo contrattuale di cui all'art.2 del presente contratto avverrà mediante bonifico bancario, dietro presentazione di regolare fattura, con cadenza bimestrale, nelle seguenti modalità:

a) per il servizio di help desk di cui all'art.2, punto 2.1, l'appaltatore emetterà regolari fatture bimestrali posticipate pari ad €_____ oltre IVA,

b) per gli sviluppi evolutivi di nuove funzionalità a richiesta di cui all'art.2, punti 2.2 e 2.3 (formazione), il compenso sarà corrisposto bimestralmente all'appaltatore, a seguito dell'effettiva realizzazione degli stessi. Ogni fattura dovrà essere accompagnata dai documenti di collaudo riportanti la data, la descrizione dell'intervento, il numero di giornate impiegate e l'autorizzazione del referente Ismea.

Per eventuali interventi di natura straordinaria non contemplati nelle attività di cui ai punti 2.1-2.2-2.3, la Società dovrà emettere regolare fattura a seguito dell'effettiva realizzazione degli stessi, al medesimo costo gg/uomo offerto in sede di gara. Allo stesso modo, ogni fattura dovrà essere accompagnata dai documenti di collaudo riportanti la data, la descrizione dell'intervento, il numero di giornate impiegate e l'autorizzazione del referente Ismea.