CAPITOLATO TECNICO

GARA EUROPEA A PROCEDURA APERTA TELEMATICA PER L'APPALTO DI SERVIZIO DI ASSISTENZA SISTEMISTICA E MANUTENZIONE DELLE APPARECCHIATURE INFORMATICHE GIÀ IN ESERCIZIO NELL'INFRASTRUTTURA ISMEA – CIG 92385482FD

Capitolato Tecnico

1. Premessa

Ismea è dotata di un'infrastruttura hardware e software per la quale è necessario un servizio di assistenza sistemistica e manutenzione ordinaria e straordinaria.

2. Oggetto del servizio

Ismea, per le proprie attività istituzionali ed in particolare per quelle legate alla gestione, conservazione e salvaguardia dei dati, nonché all'erogazione dei servizi informatici, ha la necessità di mantenere in efficienza il proprio sistema informativo aziendale, come meglio specificato nei successivi punti.

A tal fine, l'Istituto ha la necessità di individuare, attraverso procedura di gara, un operatore economico in grado di fornire il servizio di assistenza sistemistica e manutenzione ordinaria e straordinaria delle proprie apparecchiature informatiche.

I servizi oggetto della presente procedura e descritti nel presente capitolato dovranno essere svolti sia presso la sede dell'Istituto, in viale Liegi 26 a Roma, che da remoto.

Tutti i servizi richiesti dovranno essere operativi nei giorni feriali dal lunedì al venerdì, dalle ore 8:00 alle ore 18:00. Il fornitore dovrà impegnarsi, su richiesta dell'Istituto, a fornire i servizi anche fuori dagli orari indicati o presso sedi differenti dalle attuali, qualora dovessero cambiare durante la durata del contratto.

Nei paragrafi che seguono si riporta la descrizione dei servizi richiesti.

2.1. Servizio di manutenzione e assistenza utenti

2.1.1. Manutenzione ordinaria e straordinaria delle apparecchiature informatiche specificate nell'allegato tecnico al presente Capitolato denominato "Elenco apparecchiature Informatiche Data Center Ismea".

Il servizio consiste nella manutenzione ordinaria e straordinaria di server, storage, networking, ossia di tutte le apparecchiature indicate in dettaglio nell'allegato tecnico al presente capitolato denominato "Elenco apparecchiature Informatiche Data Center Ismea", ponendo in essere ogni attività necessaria alla prevenzione tramite assistenza sistemistica e alla risoluzione dei malfunzionamenti delle apparecchiature e del software di base, nonché al ripristino dell'operatività in caso di guasti attraverso la fornitura di parti di ricambio e mano d'opera; le operazioni potenziali ordinarie o "tipiche" da effettuare possono - a titolo puramente esemplificativo - riguardare la sostituzione di un disco server guasto o la sostituzione di uno switch guasto mentre quelle di natura straordinaria, sempre a titolo esemplificativo, possono essere relative alla sostituzione di "controller" server o di PDU multipresa.

Tali operazioni sono evidentemente riferibili all'elenco delle apparecchiature riportate in allegato.

Il fornitore, all'avvio del contratto, provvederà a consolidare la lista degli apparati sul sistema di Asset Management (cfr. paragrafo 2.1.2 del presente capitolato) associando ad ogni apparato un numero di riferimento/inventario che identificherà l'apparato stesso e che verrà riportato nelle chiamate di guasto/malfunzionamento ed utilizzato per la procedura di rendicontazione della chiamata stessa.

In caso di guasto/malfunzionamento, il fornitore dovrà mettere in atto tutte le azioni necessarie alla risoluzione delle problematiche hardware, compresa la fornitura di parti di ricambio nuove e/o di nuove componenti hardware/software/licenze d'uso, anche nel caso di opportune implementazioni del sistema che si rendessero necessarie, e di mano d'opera specializzata, nonché la possibile sostituzione temporanea degli apparati, quando necessario, per rispettare i livelli di servizio fissati.

Il ripristino delle funzionalità dell'apparecchiatura guasta potrà avvenire anche mediante la sostituzione della stessa con altra equivalente; resta inteso che il fornitore dovrà provvedere affinché l'apparecchiatura riparata torni a far parte della dotazione dell'Istituto entro 30 giorni dalla data di ritiro, a meno di differenti

accordi con l'Istituto. In caso di sostituzione di componenti, deve essere garantita la piena compatibilità con quelli precedentemente installati.

L'Aggiudicatario si impegna a fornire prodotti hardware originali e licenze software rilasciate appositamente dal Costruttore per Ismea o, qualora non fosse possibile, da rivenditori autorizzati dal brand. Gli apparati forniti dovranno essere idonei allo scopo, autentici, nuovi di fabbrica; quindi, inclusi nel loro packaging originale e provenienti da fonti autorizzate.

Se durante le operazioni di manutenzione correttiva, il fornitore dovesse riscontrare che un bene non è più riparabile, dovrà presentare all'Istituto una "riserva di irreparabilità". Un bene si considererà non più riparabile quando il costo della riparazione, comprensiva di mano d'opera e parti di ricambio, supera l'80% del valore di listino corrente dell'apparecchiatura stessa o di una analoga. L'Istituto si riserva la facoltà di effettuare perizie sull'apparecchiatura non riparabile e, in caso di un costo inferiore a quanto indicato, far eseguire la riparazione a terzi con oneri a carico del fornitore aggiudicatario della presente gara. L'Istituto può decidere di dismettere il bene e acquisirne uno nuovo.

Nei casi in cui il fornitore presenti la "*riserva di irreparabilità*", il fornitore dovrà sostituire il bene con uno analogo per un periodo non inferiore a quattro mesi dalla data di comunicazione della non riparabilità. Durante questi quattro mesi il bene dovrà essere soggetto a manutenzione così come qualsiasi altro bene oggetto della presente gara. Contemporaneamente, il fornitore potrà presentare offerta, non vincolante per l'Istituto, per la fornitura di una nuova apparecchiatura.

Tutte le attività sopra elencate prevedono la stesura di un rapporto di intervento, controfirmato da ISMEA.

L'Ismea, inoltre, ha a disposizione nel corso del contratto biennale un budget di € 20.000,00, da cui attingere per l'acquisto di materiali HD/SW e licenze in sostituzione di beni irreparabili, che si dovessero rendere necessari durante l'intera durata contrattuale. Tali interventi verranno quotati di volta in volta dalla società aggiudicataria, che potrà effettuare la sostituzione solo previo benestare dell'ISMEA e che dovrà successivamente presentare il relativo giustificativo di pagamento.

Il predetto importo rileva ai fini della determinazione del valore complessivo del presente appalto ma non costituisce elemento a base di gara, né sarà oggetto di valutazione ai fini dell'attribuzione del punteggio per l'offerta economica.

2.1.2. Consulenza sistemistica su server, storage, networking a richiesta

Il servizio di consulenza sistemistica prevede attività su richiesta specifica dell'Istituto, a cui seguirà un preventivo di spesa da parte del fornitore, che erogherà il servizio solo previa accettazione scritta del preventivo da parte di un responsabile dell'Istituto.
Il servizio potrà riguardare qualsiasi operazione di manutenzione delle dotazioni hardware e software presenti nel data center Ismea e degli apparati Network, al fine di garantire la disponibilità dei sistemi e degli apparati anticipando, per quanto possibile, malfunzionamenti sia di natura hardware che software. Rientrano in questa categoria, a mero titolo di esempio: la verifica di eventuali criticità relative alle prestazioni e alla sicurezza dei server così come l'aggiornamento delle versioni dei vari software.
Per esigenze di manutenzione, aggiornamento e configurazione degli apparati, dei software e dei sistemi informatici che implichino interruzioni dei servizi agli utenti, le attività di assistenza dovranno essere svolte in fasce orarie serali o nei giorni festivi anche da remoto tramite accesso protetto alla rete locale (VPN), salvo diversi accordi con i referenti dell'Istituto.
Si precisa che l'assistenza sistemistica non comprende alcuna attività di assistenza funzionale sui software applicativi e gestionali in uso agli utenti Ismea (ad esempio sw di gestione segreteria, di contabilità, delle risorse umane, del protocollo, ecc, installati sul parco macchine del committente).

2.1.3. Servizio di manutenzione delle postazioni di lavoro (PDL), costituite da desktop, thin client, monitor, notebook, ecc, a richiesta

Il servizio di manutenzione delle PDL, su richiesta, prevede attività di manutenzione e/o riparazione su richiesta specifica dell'Istituto a cui seguirà un preventivo di spesa da parte del fornitore, che erogherà il servizio solo previa accettazione scritta del preventivo da parte di Ismea.

Si tratta di circa 300 PDL, tutte ubicate nella sede di Viale Liegi, 26 a Roma.

È prevista la possibilità di distacco di alcuni utenti presso altre sedi, sempre in Roma.

2.1.4. Servizio di assistenza e affiancamento utenti nell'utilizzo di applicativi Software in dotazione all'Istituto

Il servizio di assistenza e affiancamento utenti nell'utilizzo di applicativi Software in dotazione all'Istituto prevede attività presso la sede finalizzata a:

- attività di helpdesk di primo livello per gli applicativi ad uso interno di Ismea, raccogliendo le esigenze di manutenzione correttiva ed evolutiva degli utenti, effettuando l'analisi delle richieste e provvedendo o ad operare direttamente negli applicativi per apportare le modifiche richieste o a comunicare le esigenze allo sviluppatore o alla società esterna che fornisce il servizio di helpdesk e manutenzione;
- attività di supporto all'helpdesk interno nelle sue attività di primo e secondo livello sull'infrastruttura interna.

Tale servizio prevede l'assistenza on-site; il numero di giornate dedicate on-site sarà schedulato e pianificato periodicamente da Ismea, sulla base delle esigenze, fermo restando che il numero massimo di giornate stimate è n.300 nel corso del biennio di durata del contratto.

2.2. Servizio di ticket management, inventario e reportistica

La ditta aggiudicataria si impegna a mettere a disposizione di Ismea, contestualmente all'avvio del servizio, un software per la tracciabilità degli asset, delle richieste e degli interventi, come meglio dettagliato di seguito.

Tale software, di seguito definito SW di Ticket/Asset Management, dovrà essere utilizzato per attivare i servizi di cui al punto 2.1.1 tramite apertura di un ticket dal personale IT Ismea.

2.2.1. Ticket Management

Il fornitore si impegna all'attivazione del servizio di Ticket Management e a fornirne tutti i riferimenti (telefono, mail, nominativo referente), nonché le modalità di utilizzo, entro 30 gg dalla firma per accettazione del contratto.

Il servizio dovrà essere accessibile via web 24 ore su 24 e dovrà gestire almeno le seguenti informazioni:

a) numero di identificazione del ticket

b) data ed orario di apertura del ticket

c) utente che ha aperto il ticket

d) tipologia della richiesta (informativa, malfunzionamento, ecc.)

e) numero identificativo/inventario del bene interessato dalla richiesta

f) descrizione del problema

g) livello di severità del problema

h) diagnosi del problema

i) descrizione della soluzione

j) indicazione dei tempi previsti per il ripristino del servizio / conclusione dell'attività

k) data ed orario di intervento

l) data ed orario di ripristino

m) dettaglio sul tipo di intervento effettuato

n) data ed orario di chiusura del ticket

2.2.2. Asset Management - Rilevazione e aggiornamento inventario

L'Istituto ad inizio contratto consegnerà all'Aggiudicatario l'elenco dell'attuale parco macchine e dei software oggetto del presente capitolato (descrizione bene, quantità, ubicazione e consegnatario). L'aggiudicatario dovrà effettuare entro 30 giorni solari dall'inizio del contratto la rilevazione delle postazioni di lavoro e delle dotazioni server, storage, rete dati e dei software in uso aggiornando tale inventario sulla base delle comunicazioni dell'ufficio Sistemi Informativi di ISMEA. Dovrà poi mantenerlo aggiornato con le acquisizioni, le dismissioni, le movimentazioni, tenendo traccia delle manutenzioni intercorse, attraverso l'utilizzo del SW "Ticket/Asset Management" per la tracciabilità degli asset, delle richieste e degli interventi.

Entro 15 giorni solari dalla data di conclusione del contratto dovrà redigere una relazione riepilogativa delle dotazioni in essere.

2.2.3. Reportistica

I servizi fin qui elencati devono essere monitorati dall'Istituto mediante la redazione da parte del fornitore di un report bimestrale, disponibile via web tramite il sistema di Ticket/Asset Management, sul servizio reso (attivazione entro 30 giorni solari dall'inizio del contratto). Nella rendicontazione delle attività di manutenzione hardware e software (preventiva e correttiva) devono essere presenti almeno i seguenti elementi:

- numero di interventi previsti e effettuati
- dettaglio di ogni singolo intervento
- identificazione dell'intervento
- orario di ricezione della richiesta
- orario di inizio e fine intervento
- livello di servizio contrattuale
- livello di servizio erogato

- esito dell'intervento

Si precisa che le attività indicate nel presente paragrafo sono da intendersi contemplate nell'ambito del canone di cui al Punto 2.1.1

3. Modalità di esecuzione del servizio

3.1. Avvio del servizio

Al fine di permettere al fornitore di assumere il controllo dei sistemi, nei primi 30 giorni di contratto non saranno applicate le penali previste all'articolo 6 del presente capitolato per il mancato raggiungimento del livello di servizio desiderato (cfr. paragrafo 3.4 del presente capitolato).

Dalla data di inizio del contratto, l'Ismea metterà a disposizione tutte le informazioni e la documentazione eventualmente richieste dal fornitore, riguardanti l'articolazione e la configurazione dei sistemi in uso.

3.2. Svolgimento del servizio

Ogni richiesta di intervento dovrà essere effettuata da Ismea tramite l'apertura di un ticket sul SW di Ticket Management.

L'aggiudicatario dovrà prendere in carico la richiesta entro 2 ore dall'apertura del ticket da parte di Ismea.

Ogni informazione relativa alla richiesta dovrà essere riportata sul sistema di Ticket Management per tracciare lo stato di avanzamento (tipologia di intervento da mettere in atto – tempo stimato per la risoluzione – ecc).

Al termine di ogni intervento, l'aggiudicatario dovrà dettagliare, sempre sul sistema di Ticket Management, la prestazione effettuata ed il tempo utilizzato per la risoluzione.

Per l'esecuzione del servizio di manutenzione l'aggiudicatario avrà libero accesso alle macchine nel rispetto delle norme di sicurezza.

Qualora gli errori e/o i difetti non siano eliminabili entro il breve termine, la società aggiudicataria si farà parte diligente nell'approntare soluzioni provvisorie atte a ripristinare l'operatività.

La società aggiudicataria è tenuta a mantenere aggiornata una Banca Dati delle apparecchiature oggetto del contratto, comprensiva delle informazioni circa gli interventi effettuati, da rendere disponibile sul sistema informatico di "Ticket/Asset Management".

La società aggiudicataria è tenuta ad attivare tutti i servizi di gestione operativa, compresi la configurazione iniziale e/o la riconfigurazione straordinaria per qualsiasi motivo, necessari al corretto e buon funzionamento sia ordinario che straordinario delle apparecchiature e dei programmi per i quali è previsto il servizio di gestione operativa e di manutenzione.

Le attività dovranno essere svolte esclusivamente dal personale tecnico specializzato.

In caso di interventi su apparati irreparabili o implementazioni necessarie che comportino l'esigenza di nuovi acquisti (crf. paragrafo 2.1.1 del presente capitolato), in caso di richiesta di consulenza specialistica (crf. paragrafo 2.1.2 del presente capitolato), e in caso di interventi a richiesta su PDL (crf. paragrafo 2.1.3 del presente capitolato) l'aggiudicatario dovrà sottoporre ad Ismea un preventivo contenente le seguenti informazioni tecnico-commerciali:

- Nuovo materiale hw/sw/licenze da fornire (tipo e costo)

- Attività sistemistica / consulenza specialistica (tempo e costo)

- Tempi di intervento e ripristino.

Solo a seguito di accettazione del preventivo da parte di Ismea, l'aggiudicatario procederà con gli interventi.

3.3. Aggiornamento Elenco Apparecchiature Informatiche

L'oggetto dell'appalto può essere soggetto a modifiche ed integrazioni, determinate dalla normale evoluzione del parco macchine e l'aggiudicatario è tenuto ad estendere il servizio alle nuove apparecchiature e a decurtare quelle dismesse, secondo la seguente procedura:

- i Sistemi Informativi di ISMEA comunicano l'elenco dei nuovi apparati da manutenere e il periodo di manutenzione richiesto (da individuare entro e non oltre il periodo di durata del contratto) e di quelli da dismettere.

- La società aggiudicataria deve confermare l'accettazione in manutenzione dei nuovi prodotti e la decurtazione dalla manutenzione di quelli dismessi, presentando il preventivo di integrazione / decurtazione del servizio.

- Ismea si riserva di approvare il preventivo e di aggiornare l'elenco dei prodotti oggetto di manutenzione. La data di inizio del servizio per i nuovi prodotti verrà concordata con i Sistemi Informativi di ISMEA entro e non oltre i 30 giorni solari successivi alla data di inoltro della richiesta di estensione.

3.4. Tabella riepilogativa dei servizi richiesti e relative tempistiche

Parametro	**Livello di servizio minimo - rilevazione bimestrale**
Tempo di presa in carico del ticket	Entro 2 ore dall'apertura del ticket- nel 95% dei casi
Tempo di intervento per manutenzione correttiva ***server, storage*, rete**	Entro 3 gg dalla presa in carico del ticket - nel 95% dei casi
Tempo di ripristino per manutenzione correttiva ***server, storage,* rete**	Entro il tempo proposto **nel sistema di ticket management** (di cui al punto 2.2.1 – lettera j) nel 99% dei casi
Tempo di intervento per consulenza sistemistica ***server, storage*, rete,**	Entro 3 gg dalla presa in carico del ticket - nel 95% dei casi
Tempo di intervento per manutenzione correttiva **PDL**	Entro 3 gg dalla presa in carico del ticket - nel 95% dei casi
Tempo *di ripristino* per manutenzione correttiva **PDL**	Entro il tempo proposto **nel sistema di ticket management** (di cui al punto 2.2.1 – lettera j) nel

	99% dei casi
Attivazione servizi, consegna elaborati: • attivazione Ticket/Asset Management e formazione personale (30 giorni inizio contratto) • attivazione reportistica (30 gg inizio contratto)	Entro 48 ore lavorative dalla scadenza prevista nel 99% dei casi

Definizioni relative ai livelli di servizio:

a) Tempo di intervento per manutenzione correttiva: viene misurato l'intervallo intercorso tra il tempo di apertura del ticket e il tempo di inizio lavorazione, riportato nel rapporto di intervento.

b) Tempo di ripristino per manutenzione correttiva: viene misurato l'intervallo intercorso tra il tempo di apertura del ticket e il tempo di chiusura dell'intervento di manutenzione riportato nel Rapporto di intervento.

c) Attivazione servizi, consegna elaborati: viene misurato l'intervallo intercorso tra la scadenza prevista per l'attivazione o la consegna degli elaborati richiesti e l'effettiva attivazione o consegna.

3.5. Cessazione del servizio

Con almeno due mesi di anticipo rispetto alla data di scadenza del contratto, il fornitore consegnerà un documento, riguardante l'articolazione e la configurazione dei sistemi in uso, affinché Ismea possa impiegarli in futuro.

Per ogni giorno di ritardo rispetto al suddetto termine, si applicheranno le penali previste nel successivo par. 6.

4. Clausole di sicurezza

I. 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 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.

II. 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.

III. 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.

IV. 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.

V. 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.

VI. 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.

VII. 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.

VIII. 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.

IX. 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.

X. 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.

XI. 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.

XII. 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.

XIII. 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.

XIV. Amministratori di sistema: 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.

XV. Smaltimento sicuro: nel caso l'apparato in manutenzione risultasse non riparabile o comunque da dismettere, il fornitore dovrà adottare una procedura certifica per la cancellazione irreversibile dei dati ospitati sulle memorie del dispositivo.

XVI. Sicurezza fisica: proteggere le aree dove verranno custodite le apparecchiature ISMEA attraverso appropriati controlli per l'ingresso atti ad assicurare che solo il personale autorizzato abbia il permesso di accedervi. Dotarsi di Sistemi Antintrusione e di impianto di allarme collegato alla Vigilanza o alle forze dell'ordine

XVII. Exit strategy: alla cessazione o alla scadenza del contratto, il fornitore restituirà tempestivamente tutti 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.

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.

5. 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 che

rappresentano un **requisito minimo, pena esclusione,** 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.**
- **Sistemista senior,** esperto nelle attività di manutenzione di apparati EMC2, Network e call manager Cisco, Virtualizzazione VMWARE, firewall Cisco, Microsoft; **per tale figura è richiesto il possesso di un'esperienza professionale di almeno 5 anni.**
- **Sistemista junior,** esperto nelle attività di manutenzione di apparati EMC2, Network e call manager Cisco, Virtualizzazione VMWARE, firewall Cisco, Microsoft**; per tale figura è richiesto il possesso di un'esperienza professionale di almeno 3 anni.**
- **Operatore di helpdesk applicativo, esperto nelle attività di manutenzione hardware e sistemista base Windows e OsX;** helpdesk sistemistico con conoscenza dei Sistemi operativi Windows, Linux e OsX e dei database: SQL Server, MySql e Postgresql. Linguaggi di programmazione front-end e object oriented**, con esperienza di almeno 3 anni.**

Nel gruppo di lavoro dovrà essere presente – pena esclusione - almeno una figura per ciascun profilo.

Inoltre, è facoltà del concorrente indicare il possesso di specifiche certificazioni da parte dei componenti del gruppo di lavoro, ovvero delle figure sopra indicate.

Esclusivamente il possesso delle seguenti certificazioni **in capo al profilo del sistemista senior/junior** è contemplato nei criteri di valutazione (par. 17.1 del Disciplinare di gara):

a) Cisco - CCNP ROUTING AND SWITCHING
b) Cisco - CCNP Voice
c) VMWARE - vSphere 6 o superiori
d) EMC DELL - VNX Specialist 7 o superiori

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 ed eventuali certificazioni possedute) rispetto a quello delle persone sostituite.

6. Penali

In caso di inadempimento dell'aggiudicataria relativamente ai tempi e/o alla modalità di esecuzione definite nel capitolato tecnico e/o concordate con ISMEA, nel rispetto delle procedure e dei termini di cui all'articolo 16 dello schema di contratto facente parte della documentazione di gara, saranno applicate le penali esposte in tabella:

Penali rispetto ai livelli di servizio		
Nome indicatore	Valore soglia	Penale
Tempo di presa in carico del ticket	Entro 2h dall'apertura del ticket.	100 euro per ogni 2 or2 di ritardo rispetto al valore soglia
Tempo di ripristino per manutenzione correttiva *server, storage,* rete,	il tempo proposto **nel sistema di ticket management** (di cui al punto 2.1.1 – lettera j)	200 euro per ogni gg di ritardo rispetto al valore proposto
Tempo di ripristino per manutenzione PDL	il tempo proposto **nel sistema di ticket management** (di cui al punto 2.1.1 – lettera j)	100 euro per ogni gg di ritardo rispetto al valore soglia

Al di fuori dei casi sopra richiamati, in caso di eventuali ulteriori prestazioni non conformi a quanto indicato nelle modalità di espletamento descritte nel capitolato tecnico, verrà applicata una penale variabile tra lo 0,05‰ (zerovirgolazerocinquepermille) e il 5% (cinquepercento) dell'importo contrattuale, IVA ed oneri della sicurezza esclusi, per ogni inadempimento riscontrato e a seconda della gravità del medesimo.

Gli eventuali inadempimenti contrattuali che daranno luogo all'applicazione delle penali verranno contestati all'Appaltatore per iscritto. L'Appaltatore dovrà comunicare, in ogni caso, le proprie deduzioni nel termine massimo di cinque giorni lavorativi dalla contestazione. Qualora l'ISMEA ritenga non fondate dette deduzioni ovvero non vi sia stata risposta o la stessa non sia giunta nel termine, potranno essere applicate le penali sopra indicate.

Resta pattuito che in ogni caso di mancato o inesatto adempimento, o di risoluzione del contratto per fatto imputabile all'aggiudicataria, ISMEA avrà il diritto di attivare la garanzia prestata.

Nel caso di gravi o reiterati inadempimenti, ISMEA potrà diffidare l'aggiudicatario a rispettare gli impegni contrattuali ai sensi dell'art.1454 c.c.. Qualora la società aggiudicataria nel termine assegnato o comunque nel termine massimo di 15 (quindici) giorni non avesse provveduto ad adempiere integralmente ai propri obblighi contrattuali, ISMEA, oltre a poter attivare la garanzia prestata per coprire gli oneri derivanti dal mancato o inesatto adempimento, avrà la facoltà di risolvere di diritto il contratto, oltre al diritto di richiedere il risarcimento dei danni.

ALLEGATO

Elenco apparecchiature Informatiche Data Center Ismea

SERVER (9)

N.	MODELLO APPARATO	SERIAL NUMBER
1	HP DL 380 G5	CZC9120W4C
2	HP DL 380 G6	CZ20154D97
3	HP DL 320 G6	CZ10190095
4	HP DL 380 G5	CZ10190095
6	HP DL 380 G7	ND
7	DELL POWEREDGE R510	ND
8	FUJITSU RX 100 S5	ND
9	FUJITSU RX 100 S5	ND

KVM (2 apparati)

N.	MODELLO APPARATO	SERIAL NUMBER
1	INTELLINET KVM	ND
2	INTELLINET KVM	ND
3	TASTIERA + MONITOR OXCA	ND
4	TASTIERA + MONITOR OXCA	ND

STORAGE (7 apparati)

N.	MODELLO APPARATO	SERIAL NUMBER
1	PROMISE VTRACK E630F	ND
2	PROMISE VTRAK E610fD	I4SUA8105672
3	NETAPP FAS2240-4	ND
4	QNAP TS-809U-RP 1	ND
5	QNAP TS-809U-RP 2	ND
6	QNAP TS-879U-RP 3	ND
7	SYNETO	HW id: 9981321FDA25CCB896AD27366994D55D

Cisco UCS (4 apparati)

N.	MODELLO APPARATO	SERIAL NUMBER
1	BLADE UCS 5108 composto da:	FOX1523GTTA
1a	- UCS B200 M2 (4 unità)	ND
1b	- UCS B200 M3 (2 unità)	ND
2	BLADE UCS 5108 composto da:	FOX1502H1DH
2a	- UCS B200 M2 (4 unità)	ND
2b	- UCS B200 M3 (2 unità)	ND
3	N10-S6120-XP	SSI150205JA
4	N10-S6120-XP	SSI15240L7A

Cisco NETWORK (55 unità)

N.	MODELLO APPARATO	SERIAL NUMBER
1	CATALYST 4500-X (2 unità)	ND
2	ASA 5525-X V04	FGL19317090
3	ASA 5525-X V04	FGL1931708Z
4	WS-C3750G-24-TS-1U	FOC1409Z2TA
5	WS-C3750G-24-TS-1U	FOC1409Z2RS
6	WS-C3750X-24T-S	FDO1528P0AY
7	WS-C3750X-24T-S	FDO1528P0A7
8	WS-C3750X-24T-S	FDO1528K09A
9	IRONPORT S170 V06	FTX203610RL
10	IRONPORT S170 V06	FTX203610RJ
11	IRONPORT C170 V03	FTX1650M0AL375
12	IRONPORT C170 V05	FTX1924M005
13	WS-C3560-24	FD01231Z2EU
14	WS-C3560-24	FOC1231Z2EA
15	WS-C3560-24P (6 unità)	ND
16	WS-C3560-48 POE (6 unità)	ND
17	MDS-9124 (2 unità)	
18	Cisco Meraki MR44 HW (35 unità)	ND
19	Cisco MDS 9148S (2 unità)	ND

Intelligent PDU (9 unità)

N.	MODELLO APPARATO	N. Unità
1	INFRA POWER V16C13/C19-32A	8
2	IP DONGLE IPD-02S	2
3	APC AP8653	2

Cisco VoIP (289 unità)

MODELLO APPARATO	N. Unità
CP-7962G	238
CP-7965G	10
CP-7916=	10
CP-7962G	2
CP-7915	12
5.CP-7937G	2
5.C2911-VSEC/K9	2
5.VWIC2-2MFT-T1/E1	2
5.PVDM3-128	2
5.PVDM3-16U128	2
5.CUSM-1040-2PK=	2
5.VG204	5
Cisco ISR4331	2

Ripetitori GSM/WCDMA

MODELLO APPARATO	N. Unità
Gcpr-ew23	4

Sottosistema UNIFIED VNX5400 (in garanzia EMC2 fino al 15/05/2019)

N.	MODELLO APPARATO	SERIAL NUMBER
1	EMC VNX5400 composto da:	CKM00151901562
	2 x Data Mover	
	31 x 600GB 15KRPM Disk drive (30 + 1 HS)	
	33x2TBNLSAS(32+1HS)	

Sottosistema EMC ISILON (acquisto febbraio 2016 – garanzia scaduta febbraio 2017)

N.	MODELLO APPARATO	SERIAL NUMBER
1	X210-SATA-003 composto da:	
	(1 unità)	CEGER160500017
	(1 unità)	CEGER160500018
	(1 unità)	CEGER160500019
2	851-0167 composto da:	
	(1 unità)	MT1603X08429
	(1 unità)	MT1603X08458