MODULARIO
INTERNO 314

MOD. 4 P.S.C.

Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

CAPITOLATO TECNICO

Fornitura di un sistema di Mobile Device Management per la

DIREZIONE CENTRALE DELL'IMMIGRAZIONE E DELLA POLIZIA DELLE FRONTIERE

Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

Indice

Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

1. Premessa

La **Direzione Centrale dell'Immigrazione e della Polizia delle Frontiere** ha avviato un progetto volto a a rendere disponibile, su un unico dispositivo mobile, tutte le attività di controllo documentale e le verifiche di polizia di frontiera che gli operatori svolgono attualmente con dispositivi di differente natura e tipologia.

Tali dispositivi mobili effettueranno:

- controllo documentale
- verifica dell'identità biometrica,
- controllo della persona sulle banche dati istituzionali Nazionali del Ministero dell'Interno e delle Polizie Europee.

Stante la natura di estrema riservatezza dei dati trattati e gli elevati standard di sicurezza informatica richiesti in questo ambito, il progetto prevede la realizzazione di un sistema centrale, di Enterprise Mobility Management (in seguito EMM), cui viene demandata la gestione sicura dei dispositivi mobili ed, in particolare, delle informazioni che con essi saranno scambiate.

2. Oggetto della fornitura e requisiti generali

Sono oggetto della fornitura:

- Sistema di Enterprise Mobility Management;
- Servizi di installazione e configurazione, assistenza tecnica in garanzia, direzione lavori;

La soluzione di EMM dovrà essere fornita in modalità "on premise", prevedendo l'installazione della componente server su un'infrastruttura dell'Amministrazione. Il Fornitore dovrà in ogni caso garantire, per l'intera durata di validità contrattuale, l'aggiornamento del software all'ultima release disponibile.

Il funzionamento del sistema EMM non dovrà essere, in alcun caso, subordinato all'accesso ad Internet. Si potrà, invece, prevedere un accesso alla rete pubblica solo per il download degli aggiornamenti pianificati e secondo le modalità concordate con l'Amministrazione.

Il sistema di EMM dovrà fornire le seguenti macro-funzionalità:

- **Mobile Device Management (MDM):** per l'enrollement, il provisioning, il security enforcement ed il monitoring dei dispositivi. Ovvero, più nel dettaglio:
    - **Device Enrollement** per la configurazione iniziale automatizzata e la registrazione dei dispositivi mobili nel sistema MDM, la supervisione dei dispositivi durante l'installazione.
    - **Device Provisioning** per la configurazione remota dei profili di utilizzo dei dispositivi, delle liste di app, files e dati, dei profili Wi-Fi, VPN, etc.
    - **Device Security** con la capacità di assicurare la compliance con le policies definite, procedendo al blocco, al wipe ed all'applicazione di determinate azioni in funzione dello stato del dispositivo.
    - **Device Grouping** per la gestione dei dispositivi in gruppi logici, indipendentemente dagli utenti e dal ruolo che essi ricoprono, rendendo possibile la definizione e l'applicazione delle policies sulla base dell'appartenenza a tali gruppi.
    - **Device Health Monitoring** per il probing dello stato generale, della batteria e della connettività, con la possibilità di definire alert e azioni consequenziali.
    - **Location Tracking** su mappa in tempo reale.

- **Mobile Information Management (MIM):** per la messa in sicurezza delle informazioni cruciali scambiate con i dispositivi mobili, assicurando protezione ed integrità dei dati sensibili per l'organizzazione. Il componente MIM dovrà assicurare i più alti livelli di sicurezza in relazione alla protezione delle informazioni in termini di integrità, confidenzialità e attribuzione (accountability). Tale requisito dovrà essere soddisfatto mediante la fornitura dei seguenti elementi:
    - Una soluzione **PKI (Public Key Infrastructure)** di tipo Enterprise per la emissione di certificati digitali destinati ai dispositivi mobili.
    - Un **CMS (Credential Management System)** con il compito di gestire la distribuzione dei certificati digitali ai dispositivi mobili ed il loro ciclo di vita.
    - Un servizio software per **la firma digitale e la cifratura** delle informazioni da distribuire ai dispositivi mobili.
    - Un **HSM (Hardware Security Module)** per l'esecuzione delle operazioni crittografiche e la protezione delle chiavi.

- **Mobile Application Management (MAM):** per la distribuzione e gestione del software custom e delle sue configurazioni, del licensing, del rispetto e dell'allineamento delle versioni in base alle policy pre-definite, della raccolta di statistiche di utilizzo.

2.1.Requisiti organizzativi e di sistema

Di seguito si riportano alcuni dati riepilogativi relativi al controllo delle persone e dei documenti elettronici:

- N. 167 Strutture territoriali distribuite sul territorio nazionale, isole minori comprese.
- 4 Hotspot e 9 Centri di Permanenza per il Rimpatrio (CPR)
- Personale di Polizia impiegato: (circa) **4600** operatori
- Passaporti/anno da controllare: (circa) **50.000.000**
- N. visti/anno da controllare: (circa) **14.000.000**

A fronte del predetto carico di lavoro, costantemente in aumento, si riportano di seguito i requisiti che dovranno essere soddisfatti dal sistema mobile:

- n. utenti da abilitare all'amministrazione dell'EMM: (circa) **40**
- n. utenti da abilitare al/i servizio/i (a regime, DM e EMM): (circa) **1500**
- n. dispositivi da gestire: (circa) **400**

3. Descrizione della fornitura

Di seguito sono indicate le caratteristiche tecniche minime da rispettare, a pena esclusione.

Si precisa che per alcune caratteristiche è indicato un **valore minimo**, per altre è riportato l'esatto valore richiesto. E' inoltre richiesto di specificare alcune informazioni relative ai prodotti offerti.

Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

CARATTERISTICA o FUNZIONALITÀ	VALORE RICHIESTO
Tipologia licenza	Tempo Indeterminato
Unità di misura	1 infrastruttura server, 400 dispositivi mobile
Tipo di software	Enterprise Mobility Management
Compatibilità con Sistema Operativo	La componente server deve poter essere installata nei seguenti sistemi operativi su architettura a 64 bit: • Windows Server 2008 e successivi • Linux (versione kernel minima 3.16)
Lingua	ITA o EN
Versione ed Edizione	*Dichiarare Valore Offerto*
Marca	*Dichiarare Valore Offerto*
Codice articolo produttore	*Dichiarare Valore Offerto*
Nome commerciale	*Dichiarare Valore Offerto*
Sistemi operativi supportati in Gestione	L'agent mobile, deve poter gestire i seguenti sistemi operativi: • Android KitKat e successivi • Windows 10 e successivi • iOS 10 e successivi
Interfaccia web di gestione	La soluzione deve prevedere l'accesso mediante interfaccia web.
Ruoli	La soluzione deve prevedere almeno la presenza dei seguenti ruoli: • Utente • Amministratore • Super Amministratore

Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

CARATTERISTICA o FUNZIONALITÀ	VALORE RICHIESTO
Numero di dispositivi gestibili	>= 1000
Numero utenti concorrenti supportati (Amministrazione)	>= 15
Compatibilità Soluzioni di Virtualizzazione	la piattaforma deve essere installata su server virtuali basati su tecnologie VMware.
Funzionalità di reportistica	La soluzione deve poter produrre della reportistica sull'utilizzo del dispositivo almeno nei seguenti formati: • HTML • PDF
Funzionalità MDM	• La soluzione deve fornire la funzionalità di AppStore aziendale. • La soluzione deve fornire la funzionalità di motore di wrapping con supporto di SSO via Kerberos. • La soluzione deve fornire il supporto di Android Enterprise nelle sue diverse modalità. • Tutte le app devono essere configurabili centralmente dall'interfaccia grafica del sistema di gestione. Il sistema deve anche supportare lo standard AppConfig per la configurazione delle app pubbliche. • La comunicazione con i device deve prevedere la protezione tramite "identity certificate" per l'autenticazione. • La soluzione deve poter accedere agli eventi registrati sul dispositivo, per la successiva analisi. • La soluzione deve prevedere la registrazione manuale dei dispositivi. • La soluzione deve prevedere la registrazione automatica dei dispositivi.

CARATTERISTICA o FUNZIONALITÀ	VALORE RICHIESTO
	• La soluzione deve prevedere, in caso di registrazione automatica al sistema da parte del dispositivo, una fase di "abilitazione" da parte di un Amministratore. • La soluzione deve prevedere la possibilità di raggruppare i dispositivi in "sottoinsiemi". • La soluzione deve fornire una funzionalità di "Secure boot", atta ad evitare il caricamento di software indesiderato. • La soluzione deve consentire la verifica di integrità della piattaforma e la "application sandboxing", nel senso di confinare specifici software a specifiche aree e risorse del dispositivo (definendo quindi una sandbox). • La soluzione deve fornire funzionalità di "Security policy enforcement", nel senso di poter definire un protocollo di sicurezza relativamente a cosa far accadere a fronte del verificarsi di specifici eventi. • La soluzione deve consentire il "lock" remoto di uno o più dispositivi. • La soluzione deve consentire il "wipe" remoto di uno o più dispositivi. • La soluzione deve consentire la "encryption" del dispositivo / dei dati / della mail / dei canali di comunicazione. • La soluzione deve prevedere, oltre al sistema di gestione, anche un gateway (con funzione di conditional access, ActiveSync Proxy e per-app VPN SSL).
Funzionalità MIM	• La soluzione deve consentire l'accesso alla Intranet in per-app VPN (domain-based).

CARATTERISTICA o FUNZIONALITÀ	VALORE RICHIESTO
	• La soluzione deve consentire la gestione di un Personal Information Manager (PIM) sicuro. • La soluzione deve consentire la protezione dei dati già depositati sui dispositivi mobili. • La soluzione deve poter configurare criteri di sicurezza (pass code, blocco, etc.) per proteggere i dati da minacce esterne e da eventuali smarrimenti/altro. • Tutte le operazioni inerenti la generazione e la gestione del ciclo di vita dei certificati digitali utilizzati nell'ambito dell'EMM (enrollement dei dispositivi, firma delle informazioni, etc.) dovranno essere eseguite unicamente mediante la PKI ed il CMS esterni, parti integranti della fornitura. • Le chiavi private della CA e quelle utilizzate dal servizio per la firma digitale e cifratura (circa 160), dovranno essere protette tramite il dispositivo HSM in fornitura. • Il dispositivo HSM dovrà rispettare le specifiche previste dalla direttiva BSI TR-03139. • Il dispositivo HSM dovrà essere partizionabile, in modo tale da potere essere utilizzato da differenti applicazioni di sicurezza, in maniera autonoma una dall'altra, fornendo lo stesso livello di sicurezza e compliance. • Il dispositivo HSM dovrà avere alimentazioni ridondate. • Il dispositivo HSM dovrà offrire le proprie funzionalità mediante interfaccia di rete Ethernet.

CARATTERISTICA o FUNZIONALITÀ	VALORE RICHIESTO
	• Sia per la CA che per l'HSM dovranno essere forniti i manuali di Installazione, Configurazione, Integrazione e Key Ceremony.
Funzionalità AMM	• La soluzione deve supportare la modalità "kiosk" di Android Enterprise e distribuire app al suo interno. • La soluzione deve poter distribuire sui dispositivi nuove applicazioni, aggiornarle, rimuoverle o disabilitarle. • La soluzione deve poter gestire i dettagli delle app, le restrizioni e le autorizzazioni applicate, i certificati installati. • La soluzione deve poter gestire la Richiesta/Approvazione delle applicazioni da mandare in esecuzione. • La soluzione deve poter gestire una blacklist / whitelist in termini di matrice d'applicazioni e funzionalità autorizzate (includendo il concetto di workspace / sandboxing). A titolo d'esempio, abilitazione di applicazioni e-mail ma inibizione delle funzionalità di copia/incolla e screenshot dello schermo del dispositivo. • La soluzione deve poter gestire la suddivisione fra dati (ed applicazioni) utente e quelli corporate (con diversi livelli di accesso e possibilità di configurazione di quanto è consentito e quanto non). • La soluzione deve offrire funzionalità di Identificazione delle vulnerabilità applicative.

4. Servizi

I servizi oggetto dell'appalto sono preposti ad assicurare:

- Installazione e configurazione della soluzione EMM;
- Servizio di assistenza tecnica in garanzia;
- Direzione lavori.

4.1. Luogo di erogazione

Il sistema centrale di governo dovrà essere installato presso il CEPS di Settebagni e successivamente ricollocato presso il CEN di Napoli. In previsione del progetto DR/BC (Disaster Recovery / Business Continuity) per i sistemi informativi nella disponibilità della DCIF, in conformità alle indicazioni del CAD, si determinerà la possibile migrazione dei sistemi della DCIF verso le strutture del CEN - Centro Elettronico Nazionale di Napoli e CUB, Centro Unico di Backup di Bari.

4.2. Durata

Il periodo di durata contrattuale della fornitura avrà termine il 30/06/2022.

L'assistenza tecnica e la manutenzione e gli altri servizi in fornitura dovranno essere erogati in accordo al Piano Generale di Fornitura e con i livelli di servizio specificati**.**

4.3. Modalità di acquisizione della fornitura e corrispettivi

La modalità di acquisizione della fornitura è del tipo "chiavi in mano".

Le licenze d'uso software, i servizi di assistenza tecnica e manutenzione del sistema di governo centrale (EMM), i prodotti ed i software forniti, gestiti ed eventualmente sviluppati, le manutenzioni ed evoluzioni eventuali delle licenze d'uso del software EMM, nonché i servizi che saranno forniti nell'ambito del presente appalto e che dovranno essere erogati e/o eseguiti secondo le modalità indicate nel presente documento, sono comprensivi dei servizi di consegna, installazione, configurazione e personalizzazione e quant'altro necessario per assicurare il

regolare stato di funzionamento del sistema e dovranno essere assicurati per tutta la durata contrattuale.

Tutte le spese connesse alle operazioni di cui sopra, di qualunque natura, dovranno essere a totale carico del fornitore, senza ulteriori oneri per l'Amministrazione (se non quelli contrattualizzati).

Si fa riserva di chiedere al Fornitore di utilizzare prodotti, moduli software specifici o modulistica, messi a disposizione dall'Amministrazione, da integrare nella gestione dei servizi oggetto della fornitura (ad esempio: registrazione errori, log interventi, richiesta attività, ecc.).

5. La situazione attuale

La Direzione Centrale dell'Immigrazione e della Polizia delle Frontiere non dispone di ***Dispositivi Mobili*** per il controllo documentale e la verifica d'identità biometrica.

In ausilio alle attività degli operatori di frontiera, nel corso del tempo, sono stati assegnati dispositivi di differente tipologia.

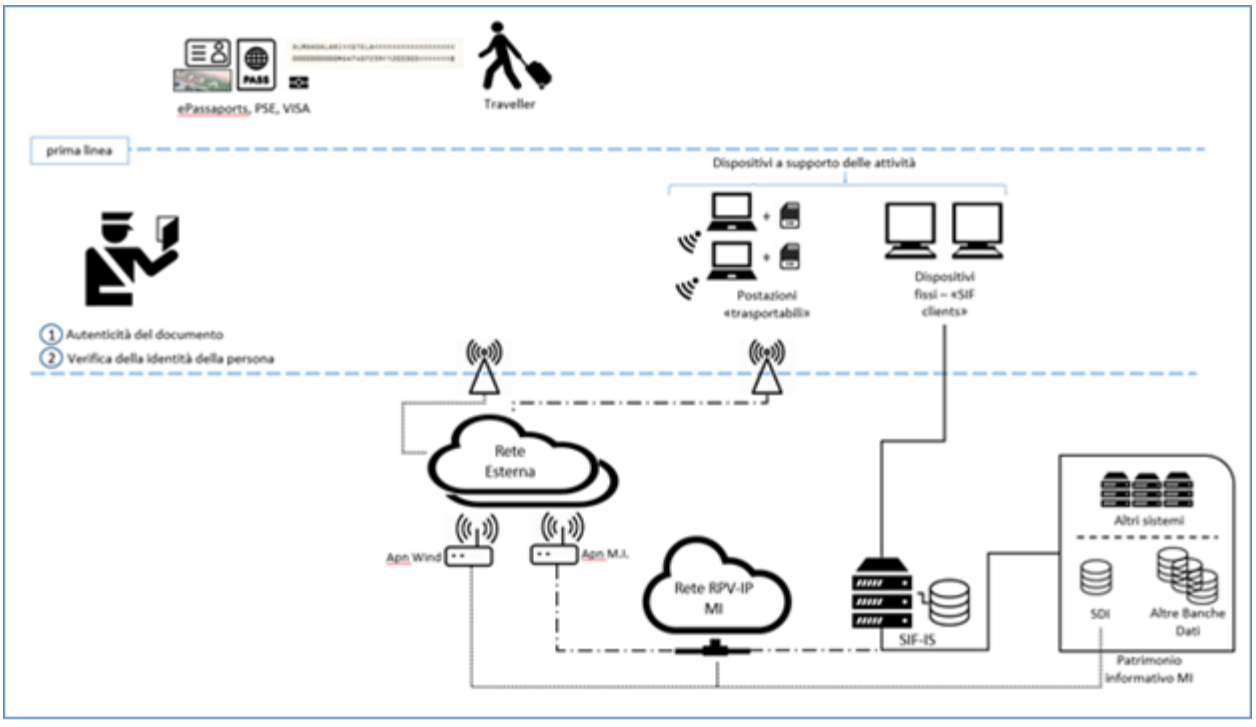
In tutte quelle aree dei sedimi portuali e aeroportuali ove è possibile procedere ad una installazione stabile nel tempo, vengono oggi utilizzate delle postazioni fisse denominate "SIF client". I *SIF client* sono dei terminali fissi attestati sulla rete interna del ministero, dotati di quelle periferiche capaci di espletare i controlli di autenticità del documento e raccolta dei dati biometrici "live" del passeggero, a scopo di verifica con le informazioni presenti o ricavabili dal documento in possesso dello stesso.

Altro dispositivo a supporto delle attività degli operatori di frontiera prevede una replica delle funzionalità equipaggiate sui SIF client, su dispositivi in wireless. Tale dispositivo è denominato "*SIF Trasportabile*" e consente alla Polizia di Frontiera di disporre di postazioni trasportabili. Queste postazioni trasportabili, non attestate sulla rete ministeriale, seguono un percorso di connessione al SIF che, partendo da una connessione dei laptop (dotati di SIM card) su reti cellulari commerciali, accedono alla rete RPV-IP del Ministero dell'Interno tramite APN.

I *SIF client* ed i *SIF Trasportabili* dialogano con la componente server del sistema informativo delle frontiere, SIF-IS, deputata alla trasmissione biunivoca delle informazioni del passeggero verso le banche dati di riferimento e verso altri sistemi, ad esempio a fini statistici.

Le informazioni accedute dalle postazioni SIF (client e trasportabili) in uso prevedono la capacità di lettura e controllo ottico della banda MRZ (machine-readable zone), lettura del chip RFID, accesso via BAC/SAC, supporto per la procedura EAC (Extended Access Control), lettura ottica del visto. I dispositivi fissi e trasportabili, inoltre, dispongono di periferiche capaci di visualizzare le caratteristiche di sicurezza dei documenti che consentono di eseguire i controlli di genuinità dei documenti in prima linea.

Di seguito uno schema generale della situazione attuale relativa alle postazioni SIF fisse e trasportabili in uso presso gli Uffici di Frontiera:



Per quanto riguarda il processo di registrazione dei dati presso gli hotspot, attualmente esistono alcune attività di raccolta dati effettuate con l'ausilio di modelli cartacei che devono essere sottoscritti dall'interessato, dal mediatore culturale e dall'Operatore di Polizia e successivamente digitalizzati tramite inserimento manuale.

6. Criterio di aggiudicazione delle offerte

La gara verrà aggiudicata mediante il criterio **dell'offerta economicamente più vantaggiosa ai sensi** dell'art. 95 comma 2 del D.lgs.50/2016.La valutazione tecnico economica delle offerte ricevute sarà effettuata dalla Commissione di Aggiudicazione sulla base dei seguenti elementi:

Criterio	Punteggio Massimo (PM)
Offerta Tecnica	70 (PTM)
Offerta Economica	30 (PEM)
Totale	100

Di seguito viene riportato il calcolo del punteggio complessivo in base alla somma algebrica del punteggio economico (PE) e del punteggio tecnico (PT).

$$P_i = PT_i + PE_i$$

P_i = punteggio totale ottenuto dalla concorrente i-esimo;

PT_i = punteggio ottenuto a seguito della valutazione tecnica dell'offerta i-esima;

PE_i = punteggio dell'offerta economica i-esima;

La commissione giudicatrice procederà alla valutazione delle offerte tecniche e all'attribuzione del relativo punteggio con riguardo alle caratteristiche tecniche migliorative rispetto a quanto previsto dal Capitolato Tecnico in base ai criteri indicati nella tabella di valutazione tecnica (Tabella - Punteggi offerta tecnica).
I punteggi ottenuti dall'esame tecnico ed economico saranno quindi sommati al fine di ottenere la graduatoria provvisoria, aggiudicando la gara al concorrente che ha ottenuto il punteggio maggiore.
La gara viene aggiudicata all'offerta che consegue la massima valutazione totale. A parità di punteggio complessivo l'aggiudicazione avviene a favore dell'offerente che ha ottenuto il maggiore punteggio tecnico.

7. Definizione dell'offerta tecnica

Si sottolinea che l'assegnazione di ogni singolo punteggio deve essere il risultato non di una valutazione complessiva del servizio sotto esame, ma esclusivamente degli eventuali elementi migliorativi presentati rispetto alle caratteristiche minime richieste. Il mancato rispetto, oggettivamente riscontrato, di una o più di tali caratteristiche deve infatti portare ad una esclusione dell'offerta dalla procedura di gara e non, bensì, ad una discrezionale valutazione di inadeguatezza. Di seguito vengono proposti i criteri che verranno utilizzati dalla Commissione per la valutazione delle Offerte Tecniche.

Criterio	Descrizione	Max	Possibili valori	Totali
	Possesso, nell'organico con contratto di lavoro subordinato, di una risorsa professionale avente le seguenti certificazioni: • CSSLP - Certified Software Security Lifecycle Professional • GWAPT – GIAC Web Application Penetration Tester	**10**	Una delle 2 = 5 punti Tutte = 10 punti	**30**
	Possesso, nell'organico con contratto di lavoro subordinato, di almeno una risorsa professionale avente le seguenti certificazioni: • CISSP - Certified Information Systems Security Professional • CISM - Certified Information Security Manager	**10**	Una delle 2 = 5 punti Tutte = 10 punti	
	Possesso, nell'organico con contratto di lavoro subordinato, di almeno una risorsa professionale avente le seguenti certificazioni: • Prince2 Practitioner	**10**	Una delle 3 = 2 punti Due = 5 punti Tutte = 10 punti	

	• PMP - PMI Project Management Professional • PgMP - PMI Program Management Professional			
Qualità della soluzione	Presenza del concorrente nel report "Critical Capabilities for High-Security Mobility Management" di Gartner, dalla versione del 2018.	**10**	On / Off	**10**
MDM	Soluzione disponibile sotto forma di virtual appliance hardenizzata e certificata CommonCriteria con base SO Linux	**5**	On / Off	**15**
	Soluzione che non richieda componenti di terze parti aggiuntive (es. licenze di SO o server per database)	**5**	On / Off	
	Disponibilità di una componente antimalware all'interno del client MDM/EMM e non tramite app esterna, per avere copertura immediata del 100% dei device gestiti e remediation immediata e offline.	**5**	On / Off	
MIM	Integrazione tra CMS ed MDM, che consenta di lasciare al solo MDM la funzione di interfacciamento con i Dispositivi Mobili senza richiedere che anche il CMS debba esporre una propria URL.	**5**	On / Off	**15**
	Disponibilità della funzione di revoca delle credenziali integrata (tra CMS e MDM), che in caso di	**5**	On / Off	

	eliminazione dal MDM di un dispositivo (es. per smarrimento/furto) richieda automaticamente alla PKI la revoca dei certificati ad esso associati.			
	Dispositivo HSM in grado di consentire la gestione delle operazioni di gestione e di attivazione in modalità "m-of-n" con segreti distribuiti su token.	**5**	On / Off	
TOTALE				**70**

Tabella - Punteggi offerta tecnica

7.1. Offerta Tecnica

L'offerta tecnica dovrà essere prodotta in lingua italiana priva di qualsiasi indicazione di carattere economico, dalla quale dovranno evincersi in maniera dettagliata le caratteristiche del servizio offerto.

Lo schema di offerta tecnica richiesto dovrà avere la struttura del capitolato tecnico (rispettando la sequenza dei capitoli e paragrafi), dalla quale si evincono in maniera diretta e dettagliata le caratteristiche di quanto offerto, mettendo a confronto le caratteristiche tecniche minime richieste e quelle offerte, le modalità di fornitura e di presentazione dei servizi oggetto di fornitura, con riferimento dei requisiti indicati nel capitolato tecnico.

Tale relazione dovrà:

- essere presentata su fogli singoli di formato DIN A4, non in bollo, con una numerazione progressiva ed univoca delle pagine;
- essere fascicolata con rilegatura non rimovibile;
- essere contenuta entro le 100 (cento) pagine;
- rispettare lo schema di risposta proposto.

Alla relazione in originale dovrà essere aggiunta una copia in formato elettronico non modificabile con la possibilità di eseguire ricerche di testo.

8. Valutazione Economica

Il punteggio relativo all'offerta economica sarà calcolato sulla base della seguente formula di tipo lineare che tiene conto dei prezzi offerti dai concorrenti:

$$P_E = \text{PEM} \times \frac{P_{min}}{P_{off}}$$

Dove:

- PE è il punteggio economico assegnato all'offerta in esame;
- PEM è il punteggio economico massimo
- Poff è il prezzo offerto oggetto di valutazione;
- Pmax è il prezzo massimo offerto;
- Pmin è il prezzo minimo offerto;

Si precisa che saranno considerate le prime due cifre dopo la virgola senza procedere a alcun arrotondamento (es. PE: 3,2345 punteggio attribuito 3,23)

8.1. Offerta Economica

L'offerta economica dovrà essere presentata mediante la compilazione della seguente tabella, ovvero, in qualsiasi altra forma stilistica purché rappresenti, a pena di esclusione, almeno i medesimi livelli di dettaglio e di informazioni:

Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

PRODOTTO	**Q.tà**	**Prezzo Unitario**	**Prezzo complessivo**
Software MDM			
Software PKI			
Software CMS			
Software di firma digitale e cifratura			
Modulo HSM			
Software MAM			
Servizi di installazione e configurazione, assistenza tecnica in garanzia, direzione lavori			
TOTALE OFFERTA IVA ESCLUSA			
di cui oneri previsti per sicurezza, specifici di attività di impresa			