CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI

AFFIDAMENTO DEL SERVIZIO DI *PENETRATION TEST* PER IL SISTEMA INFORMATIVO DELLA CASSA PER I SERVIZI ENERGETICI E AMBIENTALI - CSEA

CIG BAB1CE2077

Responsabile Unico del Progetto: Ing. Pietro Abbati Marescotti

1. PREMESSA

La Cassa per i Servizi Energetici e Ambientali (di seguito "CSEA") è un ente pubblico economico, così denominato ai sensi dell'art. 1, comma 670, della L. 208/2015 (Legge di Stabilità 2016), che opera nei settori dell'elettricità, del gas, dell'acqua e dei rifiuti.

La sua missione principale è la riscossione di alcune componenti tariffarie dagli operatori; tali componenti vengono raccolte nei conti di gestione dedicati e successivamente erogati a favore delle imprese secondo regole emanate dall'Autorità di Regolazione per Energia Reti e Ambiente (ARERA).

La CSEA è sottoposta alla vigilanza di ARERA e del Ministero dell'Economia e delle Finanze.

La CSEA è altresì qualificata quale "soggetto importante" ai sensi del D.Lgs. 138/2024, recante attuazione della Direttiva (UE) 2022/2555 (c.d. NIS2), in quanto ente operante in settore critico di rilevanza nazionale. La CSEA risulta inoltre certificata secondo gli standard ISO/IEC 27001 e ISO 22301.

In tale qualità, la CSEA è tenuta ad adottare misure tecniche, organizzative e procedurali adeguate e proporzionate al rischio, nonché a garantire un'attività continuativa di valutazione, monitoraggio e miglioramento della postura di sicurezza dei propri sistemi di rete e informativi, in coerenza con il quadro normativo vigente e con i sistemi di gestione certificati.

Il presente Capitolato speciale e obblighi contrattuali (di seguito anche "Capitolato") disciplina l'affidamento dei servizi di:

- Vulnerability Assessment e Penetration Test di rete
- Vulnerability Assessment e Penetration Test applicativi
- Analisi OSINT e Dark Web

finalizzati alla verifica della resilienza dei sistemi informativi della CSEA e alla riduzione del rischio cyber.

2. CONTESTO

Il Sistema Informativo CSEA è costituito dall'insieme dei sistemi e delle informazioni utilizzate, prodotte e trasformate nell'ambito dell'esecuzione dei processi e delle procedure aziendali, nonché dai servizi con cui esse sono gestite.

L'infrastruttura di CSEA che gestisce il parco applicativo è basata su:

1) Offerta *shared IaaS* del PSN, per l'ambiente di produzione;
2) Sistemi *Simplivity* di iperconvergenza e server Fujitsu/Siemens con virtualizzatore VMWARE, in *housing* presso il PSN, per gli ambienti di preproduzione e collaudo e, minoritariamente, per alcuni sistemi di esercizio;
3) Microsoft Active Directory, Windows Server e Microsoft 365;
4) Linux Server, principalmente in distribuzioni Debian *based*;
5) Sistemi per il *backup* centralizzato;
6) Nas di rete;
7) Bilanciatori;

8) *Firewall* applicativi.

Il parco applicativo è costituito in gran parte da c.d. *Sistemi Custom* sviluppati in JEE, nonché da una serie di sistemi (Open Source o meno) con specifiche personalizzazioni per le esigenze delle CSEA (es. SAP FI/CO, o Redmine per la gestione dei ticket, "Piuma" quale customizzazione ed estensione di Alfresco per la gestione del Protocollo, etc.), enumerati come segue:

1) Sistemi applicativi (circa 15) esposti sul web, per le dichiarazioni e la raccolta di informazioni da soggetti esterni.
2) Sistemi applicativi di *backoffice* (circa 10) per il controllo, la verifica ed ogni elaborazione necessaria da parte di CSEA, disponibili solo a personale CSEA tramite VPN/IPSEC.
3) Sistemi a supporto (circa 10) per il controllo, lo smistamento e lo scambio delle informazioni tra i sistemi, fondamentalmente di carattere finanziario, economico e contabile.
4) Sistemi di conservazione delle informazioni (database, NAS, *storage*).

Si riportano di seguito alcune metriche indicative del dimensionamento dei sistemi di CSEA, in considerazione di una ricognizione attuale degli stessi.

- Numero di utenti interni: inferiore a 200;
- Numero di utenti esterni: inferiore a 20.000;
- Sistemi Microsoft in ambiente di produzione: circa 30 server;
- Sistemi Linux in ambiente di produzione: circa 90 server.

Tutto quanto sopra enumerato è da ritenersi soggetto a possibili modifiche e quindi da considerare in maniera puramente indicativa e non vincolante in alcun modo per la presentazione dell'offerta e per l'esecuzione del contratto.

3. OGGETTO DELL'APPALTO

Si riporta, di seguito, la descrizione dettagliata dei servizi oggetto del presente affidamento, con indicazione delle relative modalità di esecuzione, dei presupposti operativi e dei principali elementi qualificanti delle prestazioni richieste.

La descrizione che segue è finalizzata a definire in modo puntuale il perimetro delle attività, gli ambiti di intervento e le responsabilità connesse all'erogazione del servizio, al fine di garantire chiarezza interpretativa, coerenza operativa e piena rispondenza agli obiettivi perseguiti dalla CSEA nell'ambito del presente procedimento.

Le attività oggetto del presente affidamento dovranno essere svolte secondo metodologie e pratiche riconosciute a livello internazionale in materia di *security assessment* e *penetration testing*, con particolare riferimento a *framework* quali PTES *(Penetration Testing Execution Standard*), NIST SP 800-115 e OWASP *Testing Guide*, ove applicabili.

Le attività di *penetration test* dovranno prevedere analisi manuali e tentativi di sfruttamento delle vulnerabilità e non potranno limitarsi a scansioni automatizzate mediante strumenti di *vulnerability scanning*.

3.1 *Vulnerability Assessment* e *Penetration Test* della rete

Le attività di *Vulnerability Assessment* (VA) e *Penetration Test* (PT) dovranno essere svolte esclusivamente sulla rete di produzione della CSEA, comprendendo le infrastrutture e i sistemi ospitati in ambiente *shared* IaaS presso il Polo Strategico Nazionale (PSN), nonché quelli collocati in *housing*. Il perimetro includerà apparati di rete, dispositivi perimetrali, sistemi esposti su rete pubblica, segmenti di rete interna di produzione e relativi componenti infrastrutturali.

Il *Vulnerability Assessment* di rete sarà finalizzato all'identificazione sistematica delle vulnerabilità tecniche e configurative presenti negli asset infrastrutturali oggetto di analisi, mediante scansioni automatizzate e verifiche manuali, individuazione di vulnerabilità note (CVE), servizi esposti, porte aperte, versioni software vulnerabili e configurazioni non conformi alle *best practice*, con classificazione del rischio sulla base di metriche riconosciute (CVSS) in funzione della gravità e del potenziale impatto operativo.

Il *Penetration Test* di rete sarà finalizzato alla simulazione controllata di attacchi informatici al fine di verificare la reale sfruttabilità delle vulnerabilità individuate e valutare la resilienza complessiva dell'infrastruttura di produzione.

Le attività dovranno includere, ove tecnicamente applicabile e nel rispetto delle regole di ingaggio concordate, verifiche di escalation dei privilegi, movimento laterale tra sistemi e tentativi controllati di accesso a sistemi e dati sensibili.

Per entrambe le attività (VA e PT) dovranno essere previsti i seguenti scenari di posizionamento:

- esterno non autenticato, simulando un attaccante operante da rete pubblica privo di credenziali;
- esterno autenticato, simulando un soggetto esterno dotato di credenziali valide;
- interno non autenticato, simulando la presenza su rete interna senza credenziali valide;
- interno autenticato privo di privilegi amministrativi, simulando la compromissione di una postazione o di credenziali di un utente standard.

La rete interna consta indicativamente di circa 300 indirizzi IP attivi, distribuiti su circa 200 server, comprensivi anche di eventuali ambienti non strettamente di produzione ma rilevanti ai fini della valutazione della postura di sicurezza complessiva. La CSEA metterà a disposizione credenziali VPN e, ove richiesto, macchine virtuali di supporto alle attività (ad esempio Kali Linux, Windows Server o equivalenti), secondo le esigenze tecniche rappresentate dall'aggiudicatario.

Tali risorse saranno rese disponibili esclusivamente per lo svolgimento delle attività di test e nel rispetto delle politiche di sicurezza e delle modalità operative definite dall'Ente.

La frequenza richiesta è pari a due esecuzioni nel corso della durata contrattuale.

3.2 *Vulnerability Assessment* e *Penetration Test* applicativi

Le attività di VA e PT applicativi saranno finalizzate all'analisi delle vulnerabilità presenti nelle applicazioni software o nelle componenti infrastrutturali, con l'obiettivo di individuare debolezze nel codice, nei protocolli di comunicazione, nei meccanismi di autenticazione e autorizzazione, nella gestione delle sessioni, nei controlli di accesso e nelle logiche applicative.

Le verifiche dovranno essere condotte, ove applicabile, con riferimento alle principali categorie di vulnerabilità note per le applicazioni web e API, in coerenza con le linee guida OWASP Top 10.

Per ciascuna sessione saranno individuati dalla CSEA tre tra applicativi e componenti dell'infrastruttura da sottoporre a verifica. Le attività dovranno essere eseguite due volte nel corso della durata contrattuale, su due set differenti di applicativi/componenti.

Anche per le attività applicative dovranno essere previsti i seguenti scenari di posizionamento:

- esterno non autenticato;
- esterno autenticato;
- interno non autenticato;
- interno autenticato privo di privilegi amministrativi.

La frequenza richiesta è pari a due esecuzioni nel corso della durata contrattuale.

Deliverable previsti per le attività di VA e PT:

Per tutte le attività di VA e PT, sia di rete sia applicative, dovranno essere prodotti almeno i seguenti documenti:

. Documentazione ante esecuzione

- **Piano delle attività**, contenente:
    - definizione puntuale del **perimetro di test (scope)**;
    - sistemi, applicazioni e servizi oggetto di verifica;
    - metodologie e standard di riferimento adottati (es. **PTES, NIST SP 800-115, OWASP *Testing Guide***);
    - calendario e finestre temporali di esecuzione.
- **Documento di regole di ingaggio (*Rules of Engagement*)** formalmente concordato con l'Amministrazione, contenente:
    - limiti operativi delle attività di test;
    - eventuali sistemi esclusi;
    - modalità di gestione degli incidenti;
    - modalità di comunicazione durante l'esecuzione delle attività.

2. Documentazione post esecuzione

- **Report tecnico dettagliato**, contenente almeno:

  - descrizione delle vulnerabilità rilevate;
  - classificazione della severità secondo **CVSS v3.1 o superiore**;
  - eventuale riferimento a **CVE**, ove disponibile;
  - evidenze tecniche (log, screenshot, output dei test);
  - descrizione delle tecniche utilizzate e degli eventuali **scenari o catene di attacco simulate**;
  - valutazione del rischio e dell'impatto sul sistema informativo.
- **Executive summary**, destinato al management, contenente:
  - sintesi delle vulnerabilità critiche e ad alta severità;
  - livello complessivo di esposizione del sistema;
  - indicazioni di priorità di intervento.
- **Piano di remediation**, contenente:
  - azioni correttive raccomandate;
  - livello di priorità degli interventi;
  - stima delle tempistiche di risoluzione.
- **Sessione di presentazione e debriefing tecnico** con il personale dell'Amministrazione, finalizzata alla condivisione dei risultati e alla discussione delle azioni di mitigazione.
- **Report finale**, redatto con un livello di dettaglio tale da consentire la **replicabilità delle verifiche in successive campagne di test**.

Su richiesta della CSEA, a seguito dell'implementazione delle azioni correttive, il Fornitore dovrà effettuare un'attività di re-test finalizzata a verificare l'effettiva risoluzione delle vulnerabilità precedentemente rilevate, producendo uno specifico report di verifica delle remediation effettuate. Tali attività di re-test non saranno conteggiate ai fini del numero complessivo delle esecuzioni previste dal contratto.

3.3 *Analisi del Deep e Dark Web*

Si richiede altresì l'esecuzione di una specifica attività di monitoraggio e analisi del *deep web* e del *dark web*, finalizzata all'individuazione di eventuali esposizioni illecite di dati riconducibili alla CSEA, ai propri sistemi, ai propri domini o al proprio personale.

L'attività dovrà prevedere la ricerca sistematica di informazioni, credenziali, dati sensibili, documenti riservati, configurazioni tecniche, riferimenti infrastrutturali o altre evidenze riconducibili alla CSEA, eventualmente oggetto di pubblicazione o commercializzazione su *marketplace*, forum, canali di comunicazione o repository clandestini.

Le attività di monitoraggio del deep web e del dark web dovranno includere, ove tecnicamente possibile, la ricerca e l'analisi di eventuali esposizioni riconducibili alla CSEA quali, a titolo esemplificativo e non esaustivo: pubblicazione o vendita di credenziali di accesso relative a sistemi dell'Ente, diffusione di database o documentazione interna, utilizzo fraudolento o impersonificazione di domini e servizi riconducibili alla CSEA, nonché eventuale presenza di dati o informazioni riguardanti l'Ente su marketplace, forum o siti di leak collegati ad attività criminali o ransomware. L'analisi dovrà comprendere la valutazione della credibilità delle evidenze individuate e del relativo livello di rischio per l'Ente.

Dovrà essere assicurata l'analisi di eventuali indicatori di compromissione, la correlazione con potenziali incidenti di sicurezza e la valutazione della fondatezza e della gravità delle evidenze rinvenute, distinguendo tra informazioni effettivamente riconducibili all'Ente e dati obsoleti o non pertinenti.

In caso di riscontro di possibili *data breach* o di diffusione non autorizzata di dati, l'aggiudicatario dovrà fornire supporto alla CSEA per:

- la qualificazione tecnica dell'evento;
- la valutazione del potenziale impatto sui sistemi, sui dati e sugli interessati;
- la definizione delle azioni di contenimento e mitigazione;
- l'eventuale attivazione di procedure di rimozione dei contenuti, ove tecnicamente e giuridicamente possibile;
- la predisposizione di elementi tecnici utili alla gestione degli obblighi di notifica previsti dalla normativa vigente.

L'attività dovrà essere svolta nel rispetto della normativa applicabile e senza porre in essere comportamenti che possano comportare perdita di informazioni, accessi abusivi o attività non consentite.

La frequenza richiesta è pari a due esecuzioni nel corso della durata contrattuale.

Deliverable previsti per l'attività di analisi *deep* e *dark web*:

- piano di monitoraggio con indicazione delle fonti e delle metodologie di ricerca;
- report periodico contenente le evidenze rilevate, la valutazione del rischio e la classificazione della criticità;
- segnalazione tempestiva in caso di individuazione di informazioni ad alta criticità;
- relazione tecnica di dettaglio in caso di accertato o presunto *data breach*;
- raccomandazioni operative per la mitigazione e il rafforzamento delle misure di prevenzione.

Nel corso delle attività di Vulnerability Assessment, Penetration Test ed Analisi di Deep e Dark Web, il Fornitore potrebbe venire a conoscenza di informazioni tecniche, configurazioni di sistema, credenziali o altri dati sensibili appartenenti alla CSEA. Il Fornitore dovrà garantire la massima riservatezza su tali informazioni e adottare adeguate misure tecniche e organizzative per la loro protezione. Al termine delle attività dovrà essere assicurata la cancellazione o distruzione sicura di

tutte le informazioni acquisite durante le attività di test, fatta eccezione per quelle strettamente necessarie alla documentazione delle evidenze contenute nei report consegnati alla CSEA.

4. DESCRIZIONE DEL SERVIZIO

Scopo del presente articolo è integrare quanto già esposto con ulteriori informazioni valevoli per tutto il novero delle attività considerate.

4.1 Profili impiegati e loro gestione

Il Fornitore garantirà un alto grado di responsabilizzazione dei profili impiegati, organizzazione, disciplina documentale ed operativa, specifica attitudine a lavorare per obiettivi, capacità di lavorare in *team* e rispetto delle scadenze pianificate, oltre che una stretta aderenza alle metodologie riportate nel presente Capitolato o comunque successivamente comunicate da parte della CSEA.

Il Fornitore garantirà, altresì, flessibilità applicativa nel fronteggiare eventuali situazioni straordinarie, che dovessero intercorrere durante l'affidamento del contratto, e per le quali dovessero risultare necessarie attività integrative dei servizi previsti e disciplinati dal presente Capitolato.

Per ciascuna attività oggetto del presente affidamento si richiede che ogni risorsa professionale impiegata disponga di comprovate capacità espressive, sia scritte sia verbali, in lingua italiana non inferiori al livello C2 del *Common European Framework of Reference for Languages* (CEFR) ovvero, in alternativa, in lingua inglese non inferiori al livello C2 del medesimo quadro di riferimento.

Resta fermo che tutta la documentazione ufficiale destinata alla CSEA, nonché le comunicazioni formali, i report tecnici, gli *executive summary* e ogni altro *deliverable* contrattuale, dovranno essere redatti in lingua italiana, salvo diversa espressa autorizzazione della CSEA.

Qualora l'aggiudicatario impieghi risorse non in possesso di competenza linguistica C2 in lingua italiana, dovrà comunque garantire la presenza, stabile e continuativa, di almeno una risorsa con competenza linguistica C2 in lingua italiana, responsabile del coordinamento, della validazione e della conformità linguistica e contenutistica di tutti i documenti e delle interlocuzioni ufficiali con la CSEA.

La mancata osservanza del presente requisito costituisce inadempimento contrattuale rilevante ai fini dell'applicazione delle penali previste e, nei casi di reiterazione o particolare gravità, potrà determinare la risoluzione del contratto.

Le risorse dovranno avere una solida capacità comunicativa verso il personale CSEA (tecnico e non), una sostanziale attitudine al *problem solving* con approcci strutturati ed orientati ad una qualità adeguata.

Il team impiegato dovrà includere almeno una risorsa con certificazione professionale in ambito *penetration testing* (es. OSCP, CREST, GIAC GPEN o equivalenti) e comprovata esperienza di almeno 3 anni in attività analoghe.

5. DURATA DEL CONTRATTO

Il servizio di cui all'articolo 3 del presente Capitolato avrà durata 24 (ventiquattro) mesi decorrenti dalla stipula contratto, ovvero dalla data dell'ultima sottoscrizione, o comunque dall'effettivo avvio del servizio, in caso di esecuzione anticipata del contratto, secondo quanto previsto al paragrafo successivo.

La CSEA si riserva la facoltà, intervenuta l'aggiudicazione, valida ed efficace, tenuto conto della necessità di garantire la continuità delle funzioni istituzionali dell'Ente, di dare avvio all'esecuzione del Contratto anche prima della stipula stesso, ai sensi dell'articolo 50, comma 6 del D. Lgs. 36/2023.

6. PENALI

L'aggiudicatario ai sensi dell'art. 126 del D. Lgs. 36/2023 incorrerà nelle penali in caso di inadempienza e ritardo nelle prestazioni di cui al presente Capitolato.

In relazione alle attività oggetto del servizio, si elencano di seguito, in modo specifico, gli SLA attesi e le penalità applicabili in caso di mancato raggiungimento dei livelli richiesti. L'eventuale applicazione delle penali non esclude né sostituisce l'obbligo di esatto adempimento della prestazione.

Il mancato rispetto reiterato degli SLA potrà costituire grave inadempimento ai fini dell'eventuale risoluzione del contratto, fatto salvo il risarcimento del maggior danno.

Si riportano di seguito gli SLA previsti e le relative penali:

Oggetto	**SLA**	**Penale**	**Tolleranza**
Disponibilità all'esecuzione delle attività richieste	Avvio delle attività entro 20 giorni solari dalla richiesta della CSEA	2.000 € per ogni settimana solare di ritardo	Prima settimana
Consegna dei *deliverable* previsti	Trasmissione dei *deliverable* entro 21 giorni solari dalla conclusione delle attività tecniche	1.000 € per ogni settimana solare di ritardo	Prima settimana
Mancata notifica entro 24 ore dal rilevamento di incidenti di sicurezza, vulnerabilità critiche (CVSS>=9.0) o compromissioni sui sistemi della CSEA	Notifica formale entro 24 ore dal rilevamento	10.000 € per ogni evento non notificato nei termini	Nessuna tolleranza

Mancata notifica entro 24 ore dal rilevamento di incidenti di sicurezza, vulnerabilità critiche o compromissioni delle infrastrutture dell'affidatario che possano impattare la CSEA	Notifica formale entro 24 ore dal rilevamento	10.000 € per ogni evento non notificato nei termini	Nessuna tolleranza
Conformità qualitativa dei report	Report completi, replicabili, coerenti con le metodologie dichiarate e privi di carenze sostanziali	15% del valore della singola attività in caso di report respinto per non conformità	Prima richiesta di integrazione

7. ASPETTI CONTRATTUALI

7.1 Clausole di Sicurezza ai sensi della direttiva NIS2 (D.Lgs. 138/2024)

Ai sensi dei controlli GV.SC-1 e GV.SC-5 ("**Governance della Sicurezza**"), l'aggiudicatario garantisce che la fornitura oggetto del presente contratto sia gestita nel rispetto di misure di sicurezza tecniche e organizzative adeguate al rischio, coerenti con il quadro normativo NIS2. L'aggiudicatario si impegna inoltre ad applicare misure di sicurezza lungo la *supply chain*, assicurando che eventuali subappaltatori o partner adottino standard di sicurezza equivalenti. L'aggiudicatario dovrà integrare inoltre nei propri processi interni misure di sicurezza per la protezione dei sistemi di rete e informativi con potenziale impatto sulla continuità operativa della CSEA.

Ai sensi del controllo ID.IM-4 ("**Comunicazione incidenti e vulnerabilità**") e del controllo RC.RP-1 ("**Collaborazione al ripristino**"), l'aggiudicatario si obbliga a comunicare tempestivamente alla CSEA, e comunque entro 24 ore dal rilevamento, eventuali incidenti di sicurezza, vulnerabilità critiche o compromissioni che possano incidere sui sistemi o servizi oggetto della fornitura, collaborare attivamente alla gestione dell'incidente, fornendo tutte le informazioni tecniche necessarie nonché cooperare nell'attuazione delle misure di mitigazione e ripristino previste dai piani di risposta agli incidenti della CSEA anche tramite fornitura di supporto tecnico qualificato in caso di conseguenze delle attività oggetto del contratto;

Ai sensi del controllo PR.AA-1, ("**Protezione dell'accesso ai sistemi della CSEA**"), l'aggiudicatario garantisce la gestione sicura delle credenziali di accesso; applica il principio del minimo privilegio; assicura la revoca immediata degli accessi in caso di cessazione del rapporto verso la CSEA o di un suo dipendente o collaboratore o comunque su richiesta della CSEA; consente verifiche e audit sulle modalità di gestione degli accessi.

7.2 Garanzie e Responsabilità

L'aggiudicatario si assume ogni responsabilità per danni alle persone ed alle cose che potessero derivare per fatto della stessa o dei suoi dipendenti durante l'espletamento della fornitura.

7.3 Garanzia definitiva

A garanzia del corretto adempimento di tutte le obbligazioni contrattuali, l'aggiudicatario dovrà prestare una garanzia definitiva, ai sensi dell'art. 106 del D. Lgs. n. 36/2023 e s.m.i. (Codice dei contratti pubblici), tramite cauzione o fidejussione, sottoscritta a favore di CSEA secondo le modalità di cui all'art. 106, commi 2 e 3, del Codice medesimo.

La garanzia dovrà essere presentata a CSEA entro 10 giorni di calendario dalla data di comunicazione dell'efficacia dell'aggiudicazione e dovrà, ai sensi dell'art. 117 co. 7 del D. Lgs. 36/2023, essere conforme agli schemi tipo approvati con decreto del Ministro delle imprese e del made in Italy di concerto con il Ministro delle infrastrutture e dei trasporti e con il Ministro dell'economia e delle finanze (ad oggi gli schemi tipo vigenti sono quelli approvati con il decreto ministeriale 16 settembre 2022, n. 193).

La garanzia, inoltre, dovrà prevedere espressamente, ai sensi dell'art. 117 co. 7 del D. Lgs. 36/2023, la rinuncia al beneficio della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'articolo 1957, comma 2, del codice civile, nonché l'operatività della garanzia medesima entro quindici giorni, a semplice richiesta scritta da parte della CSEA.

L'importo della garanzia e del suo eventuale rinnovo può essere ridotto ai sensi e per gli effetti dell'art. 106 co. 8 del D. Lgs. 36/2023.

Ai sensi dell'articolo 193, comma 6, del D. Lgs. n. 36/2023, la mancata costituzione della garanzia determina la decadenza dell'affidamento e CSEA aggiudicherà l'appalto al concorrente che segue nella graduatoria. La garanzia copre gli oneri per il mancato o inesatto adempimento e cessa di avere effetto solo alla data di emissione del certificato di regolare esecuzione e ad avvenuto passaggio di consegne al nuovo affidatario del servizio. La mancata presentazione di tale cauzione costituisce grave inadempimento contrattuale.

7.4 Subappalto e divieto di cessione del contratto

Il concorrente indica le prestazioni che intende subappaltare o concedere in cottimo.

In caso di mancata indicazione il subappalto è vietato.

Non può essere affidata in subappalto l'integrale esecuzione delle prestazioni oggetto del contratto.

L'aggiudicatario e il subappaltatore sono responsabili in solido nei confronti della stazione appaltante dell'esecuzione delle prestazioni oggetto del contratto di subappalto.

7.5 Modalità di pagamento

L'aggiudicatario provvederà ad emettere fattura elettronica successivamente all'avvio del servizio.

L'importo complessivo di aggiudicazione si intende riferito all'esecuzione integrale delle sei attività previste nel presente Capitolato, ovvero:

- due esecuzioni di Vulnerability Assessment e Penetration Test della rete;
- due esecuzioni di Vulnerability Assessment e Penetration Test applicativi;
- due esecuzioni di Analisi del *Deep* e *Dark Web*.

Ai fini della fatturazione, l'importo massimo riconoscibile per ciascuna singola attività è determinato in misura pari a un sesto (1/6) dell'importo complessivo risultante dall'offerta economica dell'aggiudicatario.

La maturazione del diritto alla fatturazione della quota relativa a ciascuna attività è subordinata al completamento integrale della medesima attività, alla consegna di tutti i *deliverable* previsti, nonché alla verifica di conformità e alla formale accettazione da parte della CSEA.

Le fatturazioni avranno luogo con cadenza trimestrale, previo positivo esito delle attività di verifica che la Direzione Transizione Digitale e Sistemi Informativi (DTS), il Responsabile Unico del Progetto (RUP) o il Direttore dell'Esecuzione del Contratto effettueranno, anche disgiuntamente, in occasione di ciascun Stato di Avanzamento Lavori (SAL) formalmente attestato.

In sede di SAL saranno oggetto di verifica, in particolare:

- l'effettiva esecuzione delle attività previste o richieste, nel rispetto delle tempistiche e con il livello qualitativo richiesto dal Capitolato;
- la validazione da parte della CSEA dei *deliverable* ricevuti.

In caso di esito negativo delle suddette verifiche, i pagamenti saranno sospesi sino al completamento delle attività oggetto di rilievo e al conseguimento di esito positivo delle verifiche stesse, senza che ciò comporti oneri aggiuntivi per la CSEA.

Non sono ammessi pagamenti parziali relativi a frazioni della singola attività, salvo diversa e motivata autorizzazione della CSEA. Resta fermo che eventuali penali applicate ai sensi del contratto saranno detratte dagli importi maturati e, ove necessario, compensate nelle successive fatturazioni

La liquidazione della fattura elettronica, a seguito della verifica della documentazione attestante la regolarità contributiva, sarà effettuata tramite bonifico bancario a 30 (trenta) giorni dalla data di ricezione della stessa, intestata a:

Cassa per i servizi energetici e ambientali

Via Barberini, 11

00187 Roma

C.F. – 80198650584

Si applica lo *split payment*; il codice univoco per la fatturazione è **UFVE7Y**.

7.6 Obblighi di tracciabilità dei flussi finanziari

L'aggiudicatario dovrà assumere tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3 della Legge 13 agosto 2010, n. 136 e successive modifiche e integrazioni.

L'accertata inosservanza, da parte dell'aggiudicatario, delle disposizioni in materia di tracciabilità dei flussi finanziari è causa di risoluzione del contratto.

7.7 Codice Etico, MOGC, PTPCT e Regolamento per l'utilizzo di dotazioni e strumenti informatici

L'aggiudicatario si obbliga a uniformare la propria condotta a principi e disposizioni contenuti nel Codice Etico, nel Modello di organizzazione, gestione e controllo, di cui al D. Lgs. n. 231/01 e s.m.i. (MOGC), e nel Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT) adottati dalla CSEA e pubblicati sul sito www.csea.it, nella sezione "Amministrazione Trasparente", in quanto applicabili.

La mancata osservanza dei suddetti principi e disposizioni è causa di risoluzione del contratto.

L'Affidatario si obbliga altresì a rispettare, per quanto applicabile, il "Regolamento per l'utilizzo di dotazioni e strumenti informatici della CSEA", che costituisce parte integrante del Contratto.

7.8 Stipula del contratto

Il contratto verrà stipulato tramite MePA, mediante invio a sistema del Documento di Stipula sottoscritto con firma digitale dalla CSEA previa presentazione di garanzia definitiva ai sensi dell'art. 106 del Codice dei contratti pubblici, nei termini di cui all'art. 7.3 del Capitolato.

Al contratto verrà unito, quale parte integrante e sostanziale, un separato allegato, che dovrà essere formato dall'affidatario e inviato tempestivamente alla CSEA, nel quale dovranno essere richiamate, ai sensi e per gli effetti degli artt. 1341 e 1342 Codice civile, le seguenti clausole contrattuali, specificatamente approvate mediante ulteriore sottoscrizione da parte del contraente, con specifico riguardo ai seguenti articoli del Capitolato: 5 ("Durata del contratto"); 6 ("Penali"); 7.5 ("Subappalto e Divieto di cessione del contratto"); 7.5 ("Modalità di pagamento"); 7.6 ("Obblighi di tracciabilità dei flussi finanziari"); 7.7 ("Codice etico, MOGC, PTPCT e Regolamento per l'utilizzo di dotazioni e strumenti informatici"); 7.9 ("Risoluzione del contratto"); 7.10 ("Recesso"); 7.13 ("Foro Competente").

Non si applica il termine dilatorio di cui all'art. 18, comma 3 del Codice dei contratti pubblici, in quanto trattasi di affidamento ai sensi dell'art. 50, comma 1, lett. e), e quindi, di contratto di importo inferiore alle soglie europee, ai sensi dell'articolo 55, comma 2.

Qualora nel corso di esecuzione del contratto, al verificarsi di particolari condizioni di natura oggettiva, si determinerà una variazione, in aumento o in diminuzione, del costo della fornitura superiore al cinque per cento, dell'importo complessivo, i prezzi saranno aggiornati, nella misura dell'ottanta per cento della variazione, in relazione alle prestazioni da eseguire.

Si precisa, inoltre, che il presente Capitolato nonché l'Offerta che risulterà aggiudicataria costituiranno parte integrante e sostanziale del contratto stipulato su MePA.

7.9 Risoluzione del contratto

In caso di grave e reiterato inadempimento dell'aggiudicatario dovuto anche a uno solo degli obblighi assunti con la sottoscrizione del contratto, la CSEA, mediante posta elettronica certificata, assegna

allo stesso, ex art. 1454 del Codice civile, un termine non inferiore a 15 (quindici) giorni dalla ricezione della comunicazione per porre fine all'inadempimento.

La CSEA, inoltre, si riserva di risolvere il contratto qualora dai controlli effettuati dal Responsabile della fornitura emergano difformità con quanto offerto in sede di gara e prescritto dal Capitolato.

In ogni caso, la CSEA, senza bisogno di assegnare previamente alcun termine per l'adempimento, e fermo il diritto al risarcimento del danno subito, potrà risolvere di diritto il contratto, ai sensi dell'art. 1456 c.c., previa dichiarazione da comunicarsi all'aggiudicatario con posta elettronica certificata, nei seguenti casi:

a) accertamento del venir meno dei requisiti minimi richiesti per la partecipazione alla procedura di selezione;

b) mancata reintegrazione, entro il termine di 10 (dieci) giorni lavorativi dal ricevimento della relativa richiesta da parte della CSEA, della garanzia eventualmente escussa;

c) nel caso di violazione di quanto disposto agli artt.: 5 ("Durata del contratto"); 6 ("Penali"); 7.5 ("Subappalto e Divieto di cessione del contratto"); 7.5 ("Modalità di pagamento"); 7.6 ("Obblighi di tracciabilità dei flussi finanziari"); 7.7 ("Codice etico, MOGC, PTPCT e Regolamento per l'utilizzo di dotazioni e strumenti informatici"); 7.9 ("Risoluzione del contratto"); 7.10 ("Recesso"); 7.13 ("Foro Competente").

d) qualora dai controlli effettuati dal Responsabile della fornitura emergano difformità con quanto offerto in sede di gara e prescritto dal Capitolato.

La risoluzione si verifica di diritto mediante unilaterale dichiarazione della CSEA, da effettuare con posta elettronica certificata.

7.10 Recesso

La CSEA si riserva la facoltà, in caso di sopravvenute esigenze d'interesse pubblico e senza che da parte dell'aggiudicatario possano essere vantate pretese, salvo che per le forniture già consegnate o in corso di consegna, di recedere in ogni momento dal contratto, con preavviso di almeno 30 (trenta) giorni solari da notificarsi all'aggiudicatario tramite posta elettronica certificata.

In caso di recesso l'aggiudicatario ha diritto al pagamento da parte dell'amministrazione delle sole forniture consegnate, purché correttamente, secondo il corrispettivo e le condizioni previste nel contratto.

7.11 Titolarità del software e dei dati, obbligo di riservatezza e tutela della privacy

Il.Fornitore sarà nominato Responsabile esterno del Trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679 (GDPR). Il Responsabile esterno del Trattamento o il sub-responsabile tratterà i dati personali in nome e per conto della CSEA in conformità alle finalità definite dalla stessa e nel rispetto delle disposizioni di cui al GDPR.

Il Fornitore si impegna a garantire la riservatezza in merito a dati, informazioni e documenti di cui venga a conoscenza o entri in possesso nell'esecuzione del servizio, anche ai sensi delle disposizioni previste dal GDPR nonché dal D. Lgs. n. 196/2003 s.m.i..

Il Fornitore adotterà e manterrà un programma sulla sicurezza delle informazioni che includa misure di sicurezza amministrative, tecniche e fisiche, progettate per garantire la sicurezza, la riservatezza e l'integrità dei dati.

A tal fine l'aggiudicatario è tenuto a rispettare gli obblighi di riservatezza in conformità al *Non-Disclosure Agreement*, che dovrà essere debitamente sottoscritto per accettazione in fase di stipula contrattuale, unitamente al contratto medesimo.

7.12 Foro competente

In caso di controversia il foro competente in via esclusiva è quello di Roma, sede della CSEA.

7.13 Normativa di rinvio

Per tutto quanto non specificatamente disciplinato dal presente Capitolato speciale, si farà riferimento alle disposizioni della Richiesta di Offerta (RdO) ad inviti che costituisce parte integrante del Capitolato stesso.

Il Responsabile Unico del Progetto
Ing. Pietro Abbati Marescotti