CAPITOLATO SPECIALE E OBBLIGHI CONTRATTUALI

Affidamento dei Servizi per la Governance in ambito cybersecurity per la Cassa per i Servizi Energetici e Ambientali – CSEA

CIG: BAAB8EB21A

Responsabile Unico del Progetto: Pietro Abbati Marescotti

Sommario

1 Introduzione

1.1 Premessa

Il presente Capitolato Speciale e Obblighi contrattuali (di seguito "Capitolato") è parte integrante della documentazione di gara e definisce le caratteristiche e le modalità di esecuzione dei servizi e delle attività, oggetto dell'affidamento, volte a garantire la piena conformità della CSEA alla normativa NIS.

Le prescrizioni contenute nel presente Capitolato rappresentano altresì gli impegni contrattuali a cui l'operatore economico Fornitore (nel seguito Fornitore) dovrà adempiere, con rinvio al resto della documentazione di gara per ogni altra disposizione vincolante.

1.2 Profilo dell'Ente

La Cassa per i Servizi Energetici e Ambientali 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'energia e dell'ambiente.

La sua missione principale è la riscossione di alcune componenti tariffarie dagli operatori; tali componenti vengono raccolte nei conti di gestione dedicati e successivamente erogate a favore delle imprese secondo regole emanate principalmente dall'Autorità di regolazione per energia reti e ambiente (ARERA o Autorità), dal Ministero dell'Ambiente e della Sicurezza Energetica (MASE) e dal Ministero delle Imprese e del Made in Italy (MIMIT).

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

Le prestazioni patrimoniali imposte sono costituite dalle componenti tariffarie e da altri corrispettivi unitari che devono essere applicati al cliente finale in funzione dei dati di consumo e fatturazione; questi dati sono inviati dagli operatori dell'Energia e dell'Ambiente alla CSEA con dichiarazioni mensili, bimestrali, trimestrali e annuali, in parte per mezzo dei diversi servizi di data entry ospitati dal sito Internet della medesima CSEA.

La CSEA provvede alla gestione finanziaria dei fondi incassati ed alle conseguenti erogazioni di contributi a favore degli operatori del settore con impieghi in materia di fonti rinnovabili e assimilate, efficienza energetica, qualità del servizio, interrompibilità, perequazione, ricerca di sistema, decommissioning nucleare, progetti a favore dei consumatori, ecc.

La CSEA svolge, anche, nei confronti dei soggetti amministrati, attività ispettive volte ad accertamenti di natura amministrativa, tecnica, contabile e gestionale, consistenti nell'audizione e nel confronto dei soggetti coinvolti, nella ricognizione di luoghi ed impianti, nella ricerca, verifica e comparazione di documenti.

Negli ultimi anni la CSEA, in attuazione delle disposizioni dell'Autorità e del MIMIT, ha registrato un significativo incremento dei meccanismi regolatori gestiti, cumulando una serie sempre più ampia di competenze, attività e responsabilità.

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

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.

Tutti i dati e i contenuti del sistema di gestione documentale della CSEA, le procedure e le modifiche realizzate nell'alveo del contratto o comunque a supporto dell'operatività sono di esclusiva proprietà della CSEA, che ne detiene la titolarità.

1.4 Glossario

Termine	Definizione
ACN	Agenzia per la Cybersicurezza Nazionale - Autorità nazionale competente NIS di cui all'articolo 10, comma 1 del Decreto NIS
Comitato di Gestione	È l'organo che esercita tutte le funzioni di amministrazione della CSEA che non siano attribuite ad altri organi; esso è composto dal Presidente e da altri due componenti. Ai sensi dell'art. 4, comma 1, dello Statuto della CSEA, il Presidente e i componenti del Comitato di gestione della CSEA sono nominati per un triennio dall'Autorità di Regolazione per Energia, Reti e Ambiente, d'intesa con il Ministro dell'Economia e delle Finanze, e sono scelti fra persone dotate di alta e riconosciuta professionalità e competenza in materia economica, giuridica, contabile, finanziaria, energetica, servizi idrici e ambientale (art. 4, comma 1, dello Statuto della CSEA).
Decreto NIS	Decreto Legislativo n. 138 del 2024
Determinazione ACN	La determinazione del Direttore generale ACN n. 379907 del 19 dicembre 2025
DPO	Data Protection Officer
DTS	Direzione Transizione Digitale e Sistemi Informativi .
Fornitore	Il soggetto aggiudicatario della presente procedura di affidamento.
Fornitura	Si intende la fornitura di tutti i servizi oggetto del Capitolato.
Fornitori critici	I fornitori che erogano le forniture critiche
Forniture critiche	Le forniture di terze parti con potenziali impatti sulla sicurezza dei sistemi informativi e di rete.
Gestione Progetti	Software Redmine, utilizzato per la pianificazione di progetti e per il tracciamento delle attività, richieste, ticket, bug, CVE, incidenti di sicurezza ed altro tramite interfaccia web, nonché per parte della documentazione.

Termine	Definizione
Incidenti significativi di base	le specifiche di base che descrivono gli incidenti significativi di cui all'articolo 25 del decreto NIS e specificate per i Soggetti Importanti nell'allegato 3 della determinazione ACN 379907
Kick Off (riunione di -)	Riunione che sancisce l'inizio dell'esecuzione delle attività afferenti ai servizi oggetto del presente Capitolato.
Misure di sicurezza di base	Specifiche di base per gli obblighi di cui agli articoli 23 e 24 del decreto NIS, sviluppate in accordo al Framework nazionale e organizzate in funzioni, categorie, sottocategorie e requisiti e specificate per i Soggetti Importanti all'allegato 1 della determinazione ACN 379907
Organi di amministrazione e direttivi	Gli organi di amministrazione e direttivi del Soggetto NIS di cui all'articolo 23 del Decreto NIS
SGI	Sistema di Gestione Integrato, ovvero il sistema che integra gli aspetti e le procedure organizzative e gestionali delle normative ISO/IEC 27001 ed ISO 22301 rispetto alla sicurezza delle informazioni ed alla continuità operativa.
Sistemi informativi e di rete rilevanti	Sistemi informativi e di rete la cui compromissione comporterebbe un impatto significativo sulla riservatezza, integrità e disponibilità delle attività e dei servizi per i quali il soggetto NIS rientra nell'ambito di applicazione del decreto NIS
Soggetto Importante	Soggetto rientrante nel perimetro di applicazione del Decreto NIS e classificato come "Importante" da ACN ai sensi del Decreto NIS
Soggetto NIS	Soggetto pubblico o privato che rientra nell'ambito di applicazione del decreto NIS, così come definito dall'articolo 1, comma 1, lettera i) della determinazione del Direttore generale dell'ACN n. 38565 del 26 novembre 2024
Specifiche di base	Le specifiche adottate con la Determinazione ACN e dettagliate nei suoi allegati 1 (Misure di Sicurezza di Base) e 3 (Incidenti significativi di base) per i Soggetti Importanti
Utenti	Personale CSEA o soggetti esterni ad essa che operano sui sistemi di CSEA, scevri da capacità tecniche-informatiche.

2 Contesto

La CSEA è tenuta ad adeguare il proprio assetto organizzativo, procedurale e tecnologico alle disposizioni normative nazionali ed europee in materia di cybersicurezza, con particolare riferimento al decreto legislativo 138/2024 (Decreto NIS) di recepimento della Direttiva (UE) 2022/2555 (c.d. NIS2). In qualità di "soggetto importante", la CSEA è chiamata a garantire il tempestivo e puntuale adempimento degli obblighi previsti dal succitato Decreto NIS. Tali obblighi devono essere osservati nel rispetto delle scadenze stabilite dalla normativa vigente, ivi incluse, a titolo meramente esemplificativo e non esaustivo, quelle indicate nell'Allegato 1 della determinazione del Direttore generale ACN n. 379907 del 19 dicembre 2025 da completarsi entro il mese di ottobre 2026.

Resta altresì fermo l'obbligo di conformità alle disposizioni più generali emanate da AgID in materia di misure minime di sicurezza ICT, che costituiscono riferimento vincolante per la gestione dei sistemi informativi e per l'adozione delle misure tecniche e organizzative di sicurezza.

La CSEA risulta inoltre certificata, per i propri sistemi informativi, secondo le norme ISO/IEC 27001:2022 e ISO 22301:2019 e successive evoluzioni. Le attività oggetto del presente Capitolato dovranno pertanto essere pienamente coerenti e integrate con il sistema di gestione per la sicurezza delle informazioni e con il sistema di gestione della continuità operativa già adottati dall'Ente.

2.1 Classificazione della CSEA nell'ambito di applicazione della normativa NIS

La CSEA, con provvedimento del 12 aprile 2025, è stata inserita dall'ACN, nell'elenco dei soggetti rientranti nel relativo perimetro di applicazione del decreto NIS e classificata Soggetto Importante in relazione alla tipologia di soggetto di seguito indicata:

1. *Amministrazioni centrali, regionali, locali e di altro tipo (allegato III)*

   1.1. *Enti di regolazione dell'attività economica*

In conseguenza di tale classificazione, la CSEA rientra nel campo di applicazione delle specifiche di base adottate da ACN attraverso la propria determinazione n. 379907 di dicembre 2025 ed in particolare:

- misure di sicurezza di base per i soggetti importanti (Allegato 1 alla Determinazione ACN)
- incidenti significativi di base per i soggetti importanti (Allegato 3 alla Determinazione ACN)

I termini per l'adozione delle specifiche di base sono fissati:

- per l'adozione delle misure di sicurezza di base di cui all'Allegato 1, in diciotto mesi dalla ricezione della comunicazione di inserimento nell'elenco dei soggetti NIS
- per l'adempimento dell'obbligo di notifica degli incidenti significativi di base di cui all'Allegato 3, in nove mesi dalla medesima comunicazione di cui al punto precedente

Per la CSEA, che ha ricevuto la suddetta comunicazione tramite PEC il giorno 13 aprile 2025, il termine per l'adozione delle misure di sicurezza di base è fissato di conseguenza al 13 ottobre 2026.

La CSEA inoltre è stata oggetto di assessment da parte della ACN, concluso nel 2025, nell'ambito del Piano Nazionale Di Ripresa E Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity", specificatamente per i seguenti interventi selezionati:

- Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber
- Analisi delle capacità dei sistemi e strumenti di sicurezza in essere
- Definizione e/o potenziamento del processo a supporto della continuità operativa
- Definizione e/o potenziamento del processo di gestione delle identità digitali e degli accessi ai sistemi informativi
- Definizione di un modello di CSIRT/SOC

3 Oggetto del servizio

L'oggetto del servizio consiste nella richiesta di un insieme di attività che abbiano come obiettivo il raggiungimento della piena *compliance* alle specifiche di base adottate da ACN nei tempi previsti dalla succitata Determinazione ACN.

Tale obiettivo dovrà essere raggiunto tenendo presente, integrando ed espandendo quanto già previsto dal sistema di gestione integrato della CSEA che include la *compliance* alle normative ISO/IEC 27001:2022 e ISO 22301:2019.

Il risultato finale dovrà quindi essere un sistema di gestione della sicurezza e della continuità operativa che risulti conforme alle norme NIS, ISO/IEC 27001:2022 e ISO 22301:2019, nonché qualsiasi altra normativa o prescrizione applicabile (es. GDPR, AgID, etc.).

Oltre a quanto strettamente necessario al raggiungimento di quanto sopra, il Fornitore dovrà predisporre un piano con le attività e progettualità necessarie al mantenimento della *compliance* nel tempo, e proporre un piano evolutivo con l'obiettivo di elevare la postura generale di sicurezza della CSEA con un orizzonte temporale di breve (entro 1 anno), medio (entro 2 anni) e lungo termine (oltre i 2 anni).

Il presente Capitolato definisce il quadro di riferimento, i vincoli e gli indirizzi cui il Fornitore dovrà attenersi nell'erogazione dei servizi di consulenza specialistica, fermo restando che, in fase esecutiva, la CSEA potrà adeguare o integrare tali indirizzi in funzione di evoluzioni normative, regolamentari o organizzative che dovessero intervenire.

Nei successivi paragrafi vengono dettagliate le specifiche attività richieste dal presente Capitolato.

3.1 Analisi propedeutica e Master plan

L'attività richiesta prevede una fase propedeutica di analisi strutturata, volta all'individuazione precisa delle azioni che la CSEA è chiamata a intraprendere in ossequio alla conformità normativa, nonché all'individuazione di ulteriori iniziative, ancorché non cogenti, idonee a elevare in misura sostanziale e tangibile il grado di sicurezza e resilienza dei sistemi informativi dell'Ente.

Tale indagine preliminare dovrà essere condotta tenendo conto, tra gli altri, di tutta la documentazione CSEA esistente, il sistema di gestione integrato adottato, i risultati dell'*assessment* sulla postura di cybersicurezza effettuato dall'Agenzia per la Cybersicurezza Nazionale, nonché attraverso colloqui e confronti formali con le strutture organizzative competenti della CSEA.

In esito a codesta fase, il Fornitore dovrà produrre un *Master Plan* che delinei l'insieme di azioni da attuarsi nel resto della fornitura per il raggiungimento degli obiettivi sopra descritti.

Per l'intero novero delle azioni così individuate, si dovrà redigere un piano operativo, esteso all'intera vigenza contrattuale, il quale prescriva con metodo ordinato le attività da espletare, le relative cadenze temporali, e la generazione degli output pertinenti, come di seguito descritti, da ritenersi anche potenzialmente contemporanei per ciascuna azione contemplata.

3.2 Linee di azione e risultati attesi

Le azioni necessarie a coprire i gap di conformità rispetto alla normativa individuata e che saranno quindi previste nel *Master Plan* dovranno essere organizzate e programmate e monitorate dal Fornitore, in accordo e con la partecipazione di CSEA ovunque necessario.

Come linea di principio, laddove possibile, tutte le attività dovrebbero essere eseguite in modalità tale da non richiedere acquisizione di *software* e/o servizi ulteriori rispetto a quanto già in essere in CSEA a meno che tale acquisizione non possa essere fatta in maniera estremamente semplice e senza ulteriore spesa (ad esempio l'utilizzo di strumenti *open source* gratuiti).

Tuttavia, il Fornitore deve proporre, anche in ottica di evoluzione futura, eventuali strumenti e/o servizi che potrebbero aiutare ad elevare la postura di sicurezza dell'ente e/o a diminuire gli *effort* operativi manuali richiesti dalle politiche introdotte.

A puro titolo esemplificativo e non esaustivo, si riporta una lista di attività che il Fornitore dovrà eseguire nell'ambito della fornitura:

a) Gestione del rischio
    - Supporto alla definizione dei sistemi informativi e di rete rilevanti e supporto alla compilazione del relativo elenco
    - Definizione, documentazione del piano di gestione dei rischi per la sicurezza informatica

- Definizione, redazione e prima esecuzione con relativa documentazione della valutazione del rischio di sicurezza informatica anche in riferimento alle eventuali dipendenze da fornitori e partner terzi che includa almeno l'identificazione, l'analisi e la ponderazione dei rischi
- Definizione, redazione e prima esecuzione del piano di trattamento dei rischi per la sicurezza informatica che comprenda almeno le opzioni di trattamento e le misure da attuare in merito al trattamento di ciascun rischio individuato e le relative priorità, le articolazioni competenti per l'attuazione delle misure di trattamento dei rischi e le tempistiche per tale attuazione e la descrizione e le ragioni che giustificano l'accettazione di eventuali rischi residui al trattamento
- Definizione e documentazione delle misure di mitigazione adottate con la descrizione dell'eventuale rischio residuo, qualora per motivate e documentate ragioni normative o tecniche non siano attuati i requisiti di cui alla tabella 2 delle misure di sicurezza di base

b) Ruoli e responsabilità
   - Definizione e documentazione dell'organizzazione per la sicurezza informatica, con la relativa definizione dei ruoli e responsabilità, ivi inclusi il punto di contatto ed il referente CSIRT, oltre agli eventuali sostituti
   - Documentazione dell'elenco aggiornato del personale di cui al punto precedente
   - Produzione delle politiche di aggiornamento e revisione dell'organizzazione per la sicurezza informatica

c) Affidabilità delle risorse umane
   - Definizione dei criteri di esperienza, capacità e affidabilità del personale autorizzato all'accesso ai sistemi informativi e di rete rilevanti, inclusi gli amministratori di sistema e redazione delle relative procedure di valutazione

d) Conformità e audit di sicurezza
   - Redazione delle politiche di sicurezza informatica per tutti gli ambiti e ai requisiti indicati dalle misure di sicurezza di base e scrittura delle relative procedure di aggiornamento periodico
   - Definizione e redazione di un piano di adeguamento che identifichi gli interventi necessari ad assicurare l'attuazione delle politiche di sicurezza e che preveda il periodico aggiornamento sugli esiti di esecuzione del piano agli organi amministrativi e direttivi

e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento

- Definizione ed individuazione delle forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete (forniture critiche) e dei relativi soggetti fornitori critici
- Definizione e redazione delle policy e procedure relative all'affidamento di forniture critiche che prevedano il coinvolgimento dell'organizzazione per la sicurezza informatica nella definizione ed esecuzione dei processi di approvvigionamento a partire dalla fase di identificazione e progettazione della fornitura
- Definizione dei criteri di valutazione del rischio delle forniture
- Definizione e redazione dei requisiti di sicurezza delle forniture coerenti con le misure di sicurezza applicate dal soggetto NIS ed in accordo agli esiti della valutazione del rischio associato
- Definizione e redazione delle clausole di offerta economica, bandi di gara, contratti accordi e convenzioni delle forniture critiche
- Definizione delle politiche e procedure di audit delle terze parti critiche e supporto alla prima esecuzione

f) Gestione degli asset

- Definizione e prima redazione dell'inventario degli apparati fisici, dei software, dei sistemi e dei servizi che compongono i sistemi informativi e di rete, inclusi i servizi erogati da terze parti, ivi inclusi i servizi cloud

g) Gestione delle vulnerabilità

- Definizione e documentazione di un piano di gestione delle vulnerabilità che comprenda almeno le modalità di identificazione delle stesse, ivi compreso il monitoraggio dei canali di comunicazione del CSIRT Italia e di altre sorgenti rilevanti e le modalità di analisi e risposta
- Definizione dei ruoli e responsabilità e redazione delle relative procedure

h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi

- Definizione e redazione del piano di continuità operativa, del piano di ripristino in caso di disastro e del piano per la gestione delle crisi informatiche per almeno i sistemi informativi e di rete rilevanti
- Definizione e redazione delle politiche e procedure di revisione ed aggiornamento dei piani di cui al punto precedente

i) Gestione dell'autenticazione, delle identità digitali e del controllo accessi

- Definizione e redazione delle politiche e procedure relative alla gestione delle credenziali delle utenze, ivi incluse quelle con privilegi amministrativi

- Definizione e redazione delle politiche e procedure relative al processo di verifica periodica delle utenze e delle relative autorizzazioni
- Definizione e documentazione delle modalità di autenticazione delle utenze per accedere ai sistemi informativi e di rete commisurate al rischio connesso ai privilegi concessi, alla criticità dei sistemi e alla tipologia delle operazioni effettuabili
- Definizione e documentazione dell'elenco dei sistemi ai quali è possibile accedere da remoto e delle relative modalità
- Definizione e documentazione delle eventuali attività consentite da remoto, definizione di adeguate misure di sicurezza per l'accesso e supporto alla loro implementazione, almeno per i sistemi informativi e di rete rilevanti

j) Sicurezza fisica

- Definizione e redazione delle politiche e procedure di accesso fisico ai sistemi informativi e di rete rilevanti

k) Formazione del personale e consapevolezza

- Progettazione ed erogazione, in accordo con gli uffici di competenza della CSEA di un piano di formazione in materia di sicurezza informatica, corredato di tutta la documentazione formativa a supporto, nonché dell'indicazione delle modalità di erogazione e della durata di ogni intervento formativo, in un'ottica di coinvolgimento trasversale dell'intera popolazione aziendale , ivi inclusi gli organi di vertice, nei termini nei quali risulta previsto da normativa
- Redazione di una proposta di GANTT di svolgimento delle attività formative, articolato in un arco temporale di copertura complessiva di vigenza del contratto
- Definizione ed implementazione del registro della formazione, da condividere con gli uffici di competenza della CSEA, che includa l'elenco dei/delle discenti coinvolti negli interventi formativi previsti dal piano di cui al punto precedente, nonché l'indicazione sommaria dei relativi contenuti e gli esiti delle eventuali verifiche/test svolte/i.

l) Sicurezza dei dati

- Definizione e redazione delle politiche e procedure relative all'adozione di protocolli ed algoritmi di cifratura per la trasmissione dei dati da e verso l'esterno, almeno per i sistemi informativi e di rete rilevanti, ivi inclusi quelli di comunicazione vocale, video e testuale
- Definizione e redazione delle politiche e procedure di backup dei dati e delle configurazioni in accordo alle esigenze di continuità operativa e di ripristino in caso di disastro.

m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete

- Definizione e redazione delle politiche e procedure di utilizzo del software, inclusi i sistemi operativi
- Definizione delle modalità di registrazione degli accessi eseguiti da remoto e quelli effettuati con utenze con privilegi amministrativi
- Definizione e redazione delle politiche di gestione centralizzata almeno dei log necessari ai fini del monitoraggio degli eventi di sicurezza, ivi compresi quelli relativi agli accessi di cui al punto precedente, incluse le tempistiche di conservazione in accordo agli esiti della valutazione del rischio
- Definizione e redazione delle politiche e procedure di sviluppo sicuro del software

n) Protezione delle reti e delle comunicazioni.

- Definizione delle politiche e procedure di implementazione, aggiornamento, manutenzione e configurazione dei firewall e degli altri sistemi perimetrali

o) Monitoraggio degli eventi di sicurezza

- Definizione e redazione delle politiche e procedure di gestione dei sistemi di monitoraggio, almeno per i sistemi informativi e di rete rilevanti, in grado di rilevare tempestivamente gli incidenti significativi
- Definizione e documentazione del livello di servizio attesi dei servizi e delle attività anche ai fini di rilevare tempestivamente gli incidenti significativi
- Definizione e documentazione delle politiche e procedure relative ai sistemi di protezione degli endpoint per il rilevamento del codice malevolo

p) Risposta agli incidenti e ripristino

- Definizione e redazione del piano per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia, in accordo a quanto previsto dall'articolo 25 del decreto NIS
- Definizione delle politiche e procedure relative all'aggiornamento periodico del piano di cui al punto precedente
- Definizione e redazione delle procedure di comunicazione, in caso di necessità, verso i destinatari dei servizi potenzialmente interessati degli incidenti di sicurezza informatica e delle azioni correttive o di mitigazione da adottare
- Definizione e redazione delle procedure di comunicazione al pubblico sugli incidenti occorsi, qualora intimato dall'ACN
- Definizione e redazione delle procedure di ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti dagli incidenti di sicurezza informatica

I risultati che deriveranno da ciascuna linea di azione identificata nel *Master Plan* saranno classificati secondo le seguenti **tipologie**, distinte in funzione della natura dell'intervento e del relativo impatto organizzativo, procedurale e tecnologico.

Le tipologie di seguito descritte **non sono da intendersi come mutuamente esclusive**, potendo ciascun intervento ricadere in una o più categorie in modo congiunto.

1. **Assetto procedurale e organizzativo**

Interventi finalizzati all'adozione, revisione o aggiornamento di policy, regolamenti, procedure operative, modelli organizzativi e assetti di governance della cybersicurezza, privi di impatti diretti sui sistemi informativi e sulle infrastrutture tecnologiche, ma essenziali ai fini della conformità normativa, della responsabilizzazione degli attori coinvolti e della tracciabilità delle decisioni.

Deliverable previsti:

- Redazione e/o aggiornamento di documentazione di processo e di procedura, nonché di modelli organizzativi e documenti di governance
- Prima esecuzione delle attività periodiche previste (ad esempio: redazione di elenchi ed inventari, valutazione del rischio, individuazione delle forniture critiche, etc.)

2. **Formazione**

Interventi di formazione per il personale di CSEA al fine di rispettare le prescrizioni normative, aumentare la consapevolezza e la comprensione delle politiche, delle procedure e delle pratiche di sicurezza implementate

Deliverable previsti:

- Progettazione, in accordo con gli uffici di competenza della CSEA, di un piano di formazione in materia di sicurezza informatica, corredato di tutta la documentazione formativa a supporto, nonché dell'indicazione delle modalità di erogazione e della durata di ogni intervento formativo, in un'ottica di coinvolgimento trasversale dell'intera popolazione aziendale, ivi inclusi gli organi di vertice, nei termini nei quali risulta previsto da normativa
- Proposte di ipotesi di interventi formativi e campagne di sensibilizzazione a breve, medio e lungo termine, a copertura dell'intera vigenza contrattuale e in un'ottica di adempimento degli obblighi formativi previsti dalla normativa
- Erogazione, con il coinvolgimento di tutta la popolazione aziendale, degli interventi di formazione previsti dal Piano Formativo, secondo le modalità concordate insieme alla

CSEA, che includano almeno delle sessioni sincrone di docenza, inclusa la redazione e diffusione di materiale didattico e informativo di supporto

- Eventuali indicazioni, se richieste, di supporto agli uffici di competenza della CSEA per la definizione dell'investimento di *budget* annuale, da destinare alla formazione in ambito di sicurezza informatica

3. Applicazione operativa diretta sui sistemi

Interventi consistenti nell'implementazione di configurazioni, controlli e misure di sicurezza applicabili in modo immediato ai sistemi informativi esistenti, senza necessità di acquisizione di nuovi prodotti *software* né di competenze aggiuntive rispetto a quelle già disponibili presso l'Ente.

Deliverable previsti:

- Supporto alla definizione e alla redazione di manuali operativi, linee guida e *playbook* tecnici, coerenti con la specifica azione considerata.

4. Applicazione operativa sui sistemi con acquisizione di software

Interventi che comportano l'introduzione, l'acquisto o l'integrazione di soluzioni software dedicate, funzionali all'implementazione delle misure di sicurezza previste, inclusi strumenti di monitoraggio, controllo, gestione degli accessi, protezione dei dati o supporto alla gestione degli incidenti.

Deliverable previsti:

- Supporto alla software selection
- Supporto alla redazione di capitolati tecnici per la pubblicazione di procedure di gara o per l'adesione a convenzioni Consip, con particolare riferimento alla definizione delle metriche per la quantificazione economica, dei livelli di servizio (SLA), delle penali e di ogni ulteriore elemento tecnico-economico utile allo scopo.
- Supporto alla definizione dei budget annuali per l'acquisizione del software a supporto della sicurezza informatica

5. Applicazione operativa sui sistemi con competenze specialistiche

Interventi che richiedono l'impiego di competenze tecniche altamente specialistiche per la progettazione, l'implementazione e la validazione delle misure di sicurezza, anche in assenza di nuove acquisizioni software, e che possono includere attività avanzate di analisi, configurazione, integrazione, verifica e messa in esercizio o servizi gestiti.

Deliverable previsti:

- Supporto alla redazione di capitolati tecnici per la pubblicazione di procedure di gara o per l'adesione a convenzioni Consip, con particolare riferimento alla definizione delle metriche per la quantificazione economica, dei livelli di servizio (SLA), delle penali e di ogni ulteriore elemento tecnico utile alla corretta esecuzione degli interventi.

- Supporto alla definizione dei *budget* annuali per l'acquisizione di servizi di sicurezza informatica

4 Modalità di esecuzione dei Servizi

4.1 Stato di Avanzamento Lavori (SAL)

Durante tutta l'esecuzione del contratto dovrà essere condiviso con CSEA, con cadenza bisettimanale (o secondo diverse indicazioni della CSEA) un *SAL operativo intermedio* finalizzato alla gestione coordinata con DTS delle linee di azione individuate.

I *SAL operativi intermedi* riporteranno l'avanzamento, le eventuali criticità e le relative azioni di nonché i principali KPI di project management che saranno concordati con CSEA.

Durante il SAL operativo intermedio, il Fornitore presenterà le evidenze per il riscontro dei livelli di servizio attesi e le eventuali non conformità.

La documentazione prodotta potrà essere oggetto di verifica di conformità da parte di CSEA, che si riserva la possibilità di richiederne al Fornitore la revisione in termini sia di contenuti che di impostazione, leggibilità e formattazione.

La reportistica sarà redatta secondo modelli stabiliti da CSEA e che quest'ultima potrà richiedere nel corso del tempo.

L'insieme delle attività di Project Management dovrà essere eseguita e coordinata principalmente tramite lo strumento Gestione Progetti di CSEA ed altri strumenti complementari per i SAL (es. PowerPoint, Microsoft Project, etc.) che il Fornitore e CSEA valuteranno concordemente.

4.2 SAL trimestrale

Successivamente alla chiusura di ciascun trimestre solare, il Fornitore presenterà a CSEA un SAL trimestrale riportante almeno:

- i dati complessivi propedeutici alla fatturazione delle attività consuntivate;
- le evidenze per i calcoli dei KPI, SLA e relative penali;
- ulteriori aspetti rilevanti emersi nel trimestre considerato o comunque come prossime azioni.

4.3 Utilizzo di Sistemi di Intelligenza Artificiale

La CSEA promuove l'impiego di strumenti basati sull'Intelligenza Artificiale da parte del Fornitore laddove tale impiego contribuisca concretamente al miglioramento dell'efficacia, dell'efficienza e della qualità dei servizi.

Tale impiego è tuttavia subordinato al rispetto della normativa vigente, in particolare:

- del Regolamento Europeo sull'Intelligenza Artificiale (AI Act, L. 132/2025);
- della normativa sulla protezione dei dati personali (Regolamento UE 2016/679 - GDPR);
- delle Linee guida etiche per un'IA affidabile promosse dalla Commissione Europea;
- dei principi fondamentali in materia di diritti umani, non discriminazione, trasparenza e responsabilità.

Il Fornitore è tenuto a dichiarare espressamente, in fase di presentazione dell'offerta e in corso di esecuzione del contratto, l'eventuale utilizzo di sistemi, moduli o strumenti che impiegano tecnologie di intelligenza artificiale, sia sviluppati internamente che forniti da terze parti.

Tale dichiarazione dovrà contenere almeno:

- la descrizione del sistema o strumento utilizzato;
- la finalità specifica dell'utilizzo;
- i benefici tangibili (ad esempio: percentuali di efficientamento, indicatori quantitativi di qualità, etc.) derivanti dall'utilizzo dello strumento;
- le modalità di funzionamento principali;
- la classificazione del rischio del sistema secondo l'AI Act;
- le misure adottate per garantire trasparenza, riservatezza, sicurezza e controllo umano.

In tale contesto, l'Ente appaltante ha la necessità di valutare in modo oggettivo, trasparente e documentato i benefici derivanti dall'adozione di tali sistemi, sia in relazione all'esecuzione del contratto, sia rispetto al valore aggiunto apportato alle attività della CSEA.

Il Fornitore dovrà quindi indicare delle metriche (KPI) che consentano di misurare e valutare:

- l'efficacia delle soluzioni adottate (es. accuratezza, affidabilità, qualità dei risultati);
- l'efficienza ottenuta (es. riduzione dei tempi di esecuzione, contenimento dei costi, riduzione degli errori);
- il valore aggiunto apportato ai processi interni e ai servizi rivolti all'utenza.

5 Composizione del *team*

Il fornitore dovrà possedere organizzazione, mezzi e risorse idonee e adeguate, sia sotto il profilo dei requisiti normativi, sia sotto il profilo dei servizi professionali, ed essere in grado di offrire un servizio con elevato standard di qualità, alle condizioni previste dal Capitolato e dai documenti da esso richiamati.

Il servizio dovrà essere eseguito con la massima cura, diligenza, tempestività e riservatezza, mediante l'impiego di un'organizzazione efficiente, risorse e mezzi adeguati. Il fornitore inoltre dovrà essere in regola con tutte le prescrizioni di legge attinenti ai servizi appaltati, gestiti a proprio esclusivo rischio e sotto la propria direzione, sorveglianza e diretta responsabilità.

Il fornitore si impegna, inoltre, a svolgere tutte le attività, anche se non espressamente indicate negli atti della gara e nel contratto, che si dovessero rendere necessarie per garantire l'efficiente svolgimento del servizio.

Il servizio deve essere organizzato e svolto con disponibilità di risorse umane e tecnologiche adeguate e a norma di legge rispetto alla consistenza qualitativa/quantitativa ed all'osservanza dei parametri di sicurezza delle persone fisiche e delle strutture coinvolte.

Il modello organizzativo che il Fornitore adotterà nell'esecuzione del contratto dovrà consentire che, nei limiti della ragionevolezza, sia in grado di supportare la CSEA anche in occorrenza di possibili situazioni straordinarie che dovessero verificarsi durante l'affidamento del contratto e per le quali dovessero risultare necessarie attività e/o risorse aggiuntive.

5.1 Caratteristiche generali delle risorse impiegate

Il Fornitore dovrà garantire per tutta la durata del contratto d'appalto 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.

Per ogni attività si richiede che ciascuna risorsa impiegata abbia capacità espressive scritte e verbali della lingua italiana pari al livello C2 nel quadro di riferimento europeo Common European Framework of Reference for Languages (CEFR).

Tutte le risorse impiegate nell'esecuzione delle attività oggetto del presente appalto dovranno possedere certificazione individuale **Lead Auditor ISO/IEC 27001** e **Lead Auditor ISO 22301**, rilasciata da organismo accreditato e in corso di validità.

Il Fornitore dovrà garantire che ciascuna risorsa assegnata al Team di progetto sia formalmente qualificata per la conduzione di audit di terza parte sui Sistemi di Gestione per la Sicurezza delle Informazioni e sui Sistemi di Gestione per la Continuità Operativa, assicurando comprovata

esperienza nell'applicazione pratica dei requisiti normativi, nella valutazione dei controlli, nell'analisi dei rischi e nella verifica dell'efficacia delle misure organizzative e tecniche.

Su richiesta della CSEA, il Fornitore dovrà fornire idonea documentazione attestante il possesso delle certificazioni richieste e la relativa validità, nonché evidenza dell'esperienza maturata in contesti organizzativi complessi e regolamentati.

Il Fornitore dovrà sottoporre preventivamente alla CSEA i CV delle risorse candidate e, su richiesta, organizzare un colloquio di approfondimento, il tutto propedeutico all'approvazione dell'inserimento nel *team* di lavoro.

La CSEA si riserva in ogni momento di richiedere la sostituzione di una o più risorse allocate nel caso queste siano ritenute non adeguate al compito; in tali casi il Fornitore dovrà garantirne la sostituzione nel minor tempo possibile assicurando in ogni caso la continuità complessiva delle attività assegnate.

I requisiti di esperienza pregressa e il possesso delle certificazioni richieste in capo alle risorse di seguito descritte costituiscono requisito minimo essenziale per lo svolgimento del servizio; la loro assenza, incompletezza o non conformità rispetto a quanto previsto nel presente Capitolato comporterà l'esclusione dell'operatore economico dalla gara.

In particolare, si richiede che nel Team di progetto siano presenti almeno le figure professionali di seguito indicate.

5.2 Responsabile di Progetto

Il Fornitore deve nominare una figura di Responsabile di Progetto che ha la responsabilità dell'esecuzione complessiva delle attività del contratto e rappresenta il punto più alto di *escalation* per qualsiasi criticità che dovesse emergere nel corso dell'affidamento.

La figura del Responsabile di Progetto deve essere una persona con comprovata *seniority* e *skill* tecniche, manageriali e relazionali; inoltre, deve possedere all'interno dell'organizzazione del Fornitore la necessaria *agency*, intesa come capacità ed autonomia decisionale per la tempestiva risoluzione delle criticità.

Ha la responsabilità di monitorare e garantire il rispetto dei livelli di servizio concordati e di far sì che la qualità dei servizi erogati sia sempre allineata con le esigenze della CSEA;

Dovrà vantare almeno dieci anni di esperienza maturata nella gestione di progetti complessi relativi all'adeguamento a normative nazionali e internazionali, alla definizione e implementazione dei principali aspetti dei modelli di governo della sicurezza delle informazioni, nonché alla gestione delle risorse, al Project Management e alle attività di PMO in ambito Information e Cyber Security;

dovrà aver consolidato competenze nell'ambito dell'IT Audit e della compliance dei processi e dei sistemi ICT in materia di sicurezza e privacy, avendo guidato progetti di certificazione ISO 27001 e

ISO 22301 e avendo operato per un periodo significativo con clienti del settore pubblico, dimostrando capacità di coniugare rigorosi requisiti normativi con le esigenze operative degli enti;

Dovrà essere in possesso, alla data di presentazione dell'offerta, delle seguenti certificazioni obbligatorie, rilasciate da organismi accreditati o enti di certificazione riconosciuti a livello nazionale o internazionale, a comprova della qualificazione professionale nelle materie oggetto dell'affidamento:

- PRINCE2 Foundation, CAPM® - Project Management, o equiparabile

Tali certificazioni sono richieste in quanto connesse alla natura dell'incarico, che richiede competenze strutturate in materia di gestione progettuale, conoscenza dei sistemi di controllo, sicurezza delle informazioni e continuità operativa, ambiti centrali nell'attuazione dei presidi organizzativi e tecnici previsti dalla Direttiva NIS2 e dalla normativa nazionale di recepimento.

5.3 Esperto/a di conformità

La figura dell'Esperto/a di conformità ha il compito di assicurare l'osservanza dei requisiti normativi NIS, oltre alle norme ISO/IEC 27001 e ISO 22031, e alle altre correlate (ad. es GDPR, rispondenza a quanto emanato da AgID, etc.), sviluppando il relativo piano di conformità.

Si richiede, pertanto il possesso di una conoscenza approfondita delle metodologie e delle linee guida ISO in materia di Risk Assessment e Risk Treatment e degli strumenti a supporto delle fasi di gestione del rischio, oltre che dei modelli per l'analisi dello stesso.

È richiesta, altresì, la conoscenza della normativa e delle linee guida e best practices di settore in materia di sicurezza informatica, oltre che una conoscenza della normativa in materia di Privacy.

Si ritiene necessaria, infine, anche la conoscenza delle policy e delle linee guida di sicurezza a supporto dei processi organizzativi su diversi ambiti di applicazione (es. gestione del rischio, classificazione delle informazioni, gestione degli incidenti, utilizzo sicuro dei servizi informatici).

Deve aver maturato un'esperienza professionale documentata di almeno otto anni su tematiche di cyber compliance, con particolare riferimento all'implementazione, adeguamento e verifica di sistemi di gestione della sicurezza delle informazioni, alla conduzione di attività di risk assessment e risk treatment, nonché al supporto alla conformità rispetto a normative nazionali ed europee in ambito cybersecurity.

Inoltre, deve aver maturato comprovate esperienze progettuali in ambito certificazione ISO/IEC 27001 e ISO 22301, avendo partecipato, con ruoli di responsabilità o coordinamento tecnico, a progetti di implementazione, mantenimento o rinnovo delle suddette certificazioni anche per clienti operanti nel settore pubblico, inclusi enti e organismi soggetti a obblighi di continuità operativa e resilienza operativa digitale.

5.4 Esperto/a di processi di cybersecurity

L'Esperto/a di processi di cybersecurity è una figura con comprovata esperienza nella progettazione e nel governo dei processi operativi di sicurezza informatica, con focalizzazione sugli aspetti esecutivi, organizzativi e di coordinamento operativo, ed opera in complementarità rispetto al ruolo di Esperto di conformità.

Tale figura opera per rendere concretamente attuabili, efficaci e sostenibili nel tempo i processi di cybersecurity definiti, assicurandone l'integrazione con i processi IT, organizzativi e di servizio della CSEA.

In particolare, l'Esperto/a di processi di cybersecurity:

- supporta la strutturazione e l'ottimizzazione dei processi operativi di gestione degli incidenti di sicurezza informatica, incluse le modalità di attivazione, escalation, coordinamento interno e chiusura degli eventi;
- fornisce supporto operativo nella predisposizione e nell'utilizzo della documentazione di esercizio (procedure operative, playbook, modelli di registrazione e tracciamento);
- affianca le strutture della CSEA nella gestione operativa delle interazioni con i soggetti tecnici interni, i fornitori e i servizi esterni potenzialmente coinvolti nella risposta agli incidenti;
- supporta l'organizzazione e il coordinamento delle attività di monitoraggio, risposta e ripristino, assicurando la coerenza tra processi, ruoli e strumenti in uso;
- contribuisce alla verifica dell'effettiva applicazione dei processi di cybersecurity anche attraverso simulazioni, esercitazioni e analisi operative degli eventi occorsi, fornendo elementi di miglioramento continuo.

L'Esperto/a di processi di cybersecurity opera come figura di raccordo tra governance e operatività, con l'obiettivo di trasformare indirizzi, policy e requisiti definiti in ambito di conformità in processi realmente eseguibili, misurabili e integrati nel funzionamento quotidiano e nei sistemi della CSEA.

La risorsa proposta dovrà avere maturato almeno due anni di esperienza documentata nella gestione di progetti di cyber compliance e implementazione di certificazioni ISO presso clienti operanti anche nel settore pubblico.

È richiesta comprovata capacità di supportare attività di assessment, gap analysis, definizione di policy e procedure conformi agli standard ISO, nonché esperienza nella collaborazione con enti pubblici nel rispetto delle normative vigenti in materia di sicurezza delle informazioni e continuità operativa.

6 Fatturazione, SLA e Penali

In relazione alle attività oggetto del servizio si elencano di seguito, in modo specifico, gli SLA attesi e le penalità applicate in caso di mancato raggiungimento dei livelli richiesti.

Le fatturazioni avranno luogo, con cadenza trimestrale, al positivo esito delle seguenti attività che il RUP, in qualità altresì di Direttore dell'esecuzione, effettuerà in occasione di ciascun SAL formale:

- verifica che siano state effettuate le attività, previste o richieste e con la qualità necessaria;
- validazione da parte di CSEA dei deliverable ricevuti.

In caso di esito negativo delle suddette attività di verifica in sede di SAL, dagli importi oggetto di fatturazione saranno decurtate le eventuali penali come di seguito determinate. Si precisa che le stesse saranno calcolate a partire dal giorno dell'accertamento da parte di CSEA.

Si precisa che la valutazione di adeguatezza dei *deliverable* è rimessa al giudizio della CSEA.

L'applicazione delle penali sarà preceduta da regolare contestazione dell'inadempienza, verso cui il Fornitore avrà la facoltà di presentare le proprie controdeduzioni entro e non oltre 5 (cinque) giorni dalla ricezione della comunicazione della contestazione inviata dalla CSEA.

In caso di assenza o di non accoglimento delle controdeduzioni, la CSEA procederà all'applicazione delle sopra citate penali a decorrere dall'inizio dell'inadempimento.

È fatta salva, in ogni caso, la facoltà della CSEA di risolvere il contratto in qualsiasi momento, con un preavviso di almeno 10 (dieci) giorni comunicato a mezzo posta elettronica certificata, senza che l'Aggiudicatario possa pretendere per questo alcun indennizzo.

Per tutte le penali si applica quanto previsto dall'art. 126, comma 1, del D.lgs. 36/2023.

6.1 Penali

ID	Oggetto	SLA	Penale	Tolleranza
PPM1	Mancato rispetto delle tempistiche di progetto o inadeguata qualità dei deliverable previsti	Scadenza pianificata ed attesa dalla CSEA	€ 350,00 per ogni giorno lavorativo ulteriore	5 giorni lavorativi
PPM2	Consegna completa di tutta la documentazione di SAL operativo intermedio	Scadenza pianificata ed attesa dalla CSEA	€ 50,00 per ogni giorno lavorativo ulteriore	5 giorni lavorativi
PPM3	Consegna completa di tutta la documentazione di SAL trimestrale	Scadenza pianificata ed attesa dalla CSEA	€ 50,00 per ogni giorno lavorativo ulteriore	5 giorni lavorativi
PCO1	Mancato rispetto dei termini previsti dalla determinazione ACN 379907/2025 per la compliance alle specifiche di base	Entro il 30 settembre 2026	€ 1000 per ogni giorno lavorativo ulteriore	Non prevista

7 Aspetti contrattuali

7.1 Garanzie e Responsabilità

L'Appaltatore 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 del servizio.

7.2 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.

7.3 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'affidatario deve eseguire direttamente tutte le attività che incidono sulle scelte metodologiche, sulle valutazioni tecniche, sulle attività di analisi del rischio, sulla conduzione degli audit, e sulle responsabilità progettuali e di coordinamento del servizio.

Tale limitazione è prevista in ragione dell'esigenza di garantire l'unitarietà dell'esecuzione contrattuale, la piena tracciabilità delle responsabilità, la coerenza metodologica delle attività svolte e l'adeguato presidio dei rischi connessi alla sicurezza delle informazioni e alla continuità operativa dell'Ente, anche con riferimento ai profili di rischio della catena di fornitura.

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

7.4 Modalità di pagamento

Con riferimento alle modalità di fatturazione si veda quanto indicato nel precedente paragrafo 6.

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**.

7.5 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.

7.6 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.

7.7 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. 6.1 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: 6 ("Fatturazione, SLA e Penali"); 7.1 ("Garanzie e responsabilità"); 7.3 ("Subappalto e Divieto di cessione del contratto"); 7.4 ("Modalità di pagamento"); 7.5 ("Obblighi di tracciabilità dei flussi finanziari"); 7.6 ("Codice etico, MOGC, PTPCT e Regolamento per l'utilizzo di dotazioni e strumenti informatici"); 7.8 ("Risoluzione del contratto"); 7.9 ("Recesso"); 7.10 ("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.

7.8 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. 6 ("Fatturazione, SLA e Penali"); 7.1 ("Garanzie e responsabilità"); 7.3 ("Subappalto e Divieto di cessione del contratto"); 7.4 ("Modalità di pagamento"); 7.5 ("Obblighi di tracciabilità dei flussi finanziari"); 7.6 ("Codice etico, MOGC, PTPCT e Regolamento per l'utilizzo di dotazioni e strumenti informatici"); 7.8 ("Risoluzione del contratto"); 7.9 ("Recesso"); 7.10 ("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.

7.9 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.

7.10 Foro competente

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

7.11 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.