Richiesta di Offerta (RdO) a inviti tramite MePA, ai sensi dell'art. 50, comma 1, lett. b) ed e), del D. Lgs. n. 36/2023, per l'affidamento del servizio di *Penetration Test* per il sistema informativo della Cassa per i Servizi Energetici e Ambientali – CSEA – CIG BAB1CE2077

FAQ

Domanda n.1

A.1 "Attività continuativa" vs frequenza VA/PT e Analisi Deep/Dark Web

In Premessa si richiama l'esigenza di un'"attività continuativa di valutazione, monitoraggio e miglioramento della postura di sicurezza", mentre agli artt. 3.1, 3.2 e 3.3 sono previste:

· n. 2 esecuzioni di VA/PT di rete in 24 mesi;

· n. 2 esecuzioni di VA/PT applicativi in 24 mesi;

· n. 2 esecuzioni di Analisi Deep e Dark Web in 24 mesi.

Si chiede di chiarire:

· Se la locuzione "attività continuativa" sia da intendersi in senso programmatico, oppure se CSEA intenda prevedere (o valutare in offerta tecnica) forme di monitoraggio più regolari (es. scansioni periodiche, servizi continuativi di vulnerability management / dark web monitoring).

· Se la frequenza indicata (2 esecuzioni in 24 mesi per ciascun ambito) sia un requisito minimo inderogabile o se sia ammissibile una proposta tecnica che preveda maggior frequenza (es. annuale/semestrale) rimodulando ampiezza e profondità delle singole campagne.

Risposta n. 1

La richiesta della CSEA è da intendersi come definizione dei livelli minimi di servizio, come esplicitato nella documentazione di gara, ovvero:

- n. 2 esecuzioni di VA/PT di rete in 24 mesi;
- n. 2 esecuzioni di VA/PT applicativi in 24 mesi;
- n. 2 esecuzioni di analisi Deep e Dark Web in 24 mesi.

Il riferimento all'"attività continuativa" va interpretato in senso programmatico, quale obiettivo generale di mantenimento e miglioramento della postura di sicurezza nel tempo, senza implicare attività ulteriori rispetto a quelli sopra indicati.

Resta comunque facoltà del concorrente proporre, in sede di esecuzione, eventuali attività aggiuntive o una maggiore frequenza di esecuzione rispetto ai minimi richiesti. Tali elementi, pur potendo costituire un valore aggiunto in fase esecutiva, non sono oggetto di specifica valutazione ai fini dell'offerta, trattandosi di procedura aggiudicata secondo il criterio del minor prezzo.

Domanda n. 2

A.2 Ambito delle attività di Penetration Test vs Red Teaming / Kill Chain

All'art. 3.1 si prevede che le attività di Penetration Test includano, ove applicabile, escalation di privilegi, movimento laterale tra sistemi, tentativi controllati di accesso a dati sensibili e simulazione di catene di attacco.

Considerato che tali elementi sono tipici delle attività di red teaming/adversary emulation, si chiede:

· Se le attività debbano essere inquadrate come Penetration Test mirati (convalidando in modo puntuale la sfruttabilità delle vulnerabilità, anche indicando in maniera documentale scenari di escalation/movimento laterale), oppure se CSEA intenda effettivamente includere nel perimetro attività di red team più ampie.

· Nel caso si tratti di Penetration Test, se la CSEA ritenga sufficiente che il Fornitore:

– identifichi e descriva le vulnerabilità che potenzialmente consentono escalation/movimento laterale e, ove concordato nelle regole di ingaggio, ne dimostri l'impatto in modo circoscritto, senza eseguire una kill chain completa.

· Nel caso si vogliano ricomprendere attività di red teaming, se la CSEA intenda dettagliare nel Capitolato le specifiche regole di ingaggio, le esclusioni e le cautele operative, nonché riconsiderare effort e corrispettivo associati.

Risposta n. 2

Le attività richieste sono da intendersi come Penetration Test mirati e non come attività di red teaming in senso esteso. Nell'ambito di tali attività, il Fornitore è tenuto a verificare la sfruttabilità delle vulnerabilità individuate, procedendo, ove tecnicamente applicabile e nel rispetto delle regole di ingaggio concordate, al loro sfruttamento controllato al fine di dimostrare concretamente i possibili impatti, inclusi scenari di escalation dei privilegi e/o movimento laterale, circoscritti comunque ai soli sistemi, intervalli temporali ed ambienti di volta in volta concordati con la CSEA e limitati al perimetro preventivamente definito nel piano di test (scope).

Domanda n. 3

A.3 SLA di notifica entro 24 ore e modello di rilevazione

Il Capitolato prevede un obbligo di notifica entro 24 ore dal rilevamento di incidenti e vulnerabilità critiche (CVSS ≥ 9.0), con relative penali, in un contesto in cui le attività VA/PT e l'analisi deep/dark web sono previste solo due volte in 24 mesi.

Si chiede:

· Se lo SLA di 24 ore sia riferito esclusivamente a quanto rilevato nell'ambito delle attività oggetto del contratto (VA/PT, analisi deep/dark web) e/o ad eventi sulle infrastrutture del Fornitore potenzialmente impattanti CSEA, e non alla data di pubblicazione o scoperta "globale" delle vulnerabilità.

· Se sia previsto un meccanismo di condivisione/accordo sul punteggio CVSS in caso di divergenza di valutazione tra CSEA e Fornitore, specie per vulnerabilità prossime alla soglia 9.0.

Risposta n. 3

In relazione al quesito, si conferma che lo SLA di notifica entro 24 ore è riferito esclusivamente a quanto rilevato nell'ambito delle attività oggetto del contratto, nonché ad eventuali eventi afferenti alle infrastrutture del Fornitore che possano avere impatti sulla CSEA, e non alla data di pubblicazione o scoperta a livello generale delle vulnerabilità.

Con riferimento al punteggio CVSS, si precisa che la valutazione dovrà essere effettuata dal Fornitore secondo lo standard CVSS v3.1, tenendo conto del contesto specifico della CSEA. In caso di divergenze di valutazione, è previsto un confronto tra le parti finalizzato alla condivisione del punteggio, fermo restando che la valutazione finale terrà conto del contesto operativo, dell'esposizione effettiva e dei potenziali impatti sui sistemi e sui dati della CSEA.

Domanda n. 4

A.4 Criteri di accettazione degli output (Acceptance Test / Acceptance Criteria)

Il Capitolato prevede la verifica, in sede di SAL, dell'"effettiva esecuzione delle attività previste o richieste e con la qualità necessaria" e la "validazione da parte di CSEA dei deliverable ricevuti", ma non dettaglia criteri di accettazione specifici per i diversi output (es. struttura minima dei report tecnici, requisiti di replicabilità, formato delle evidenze, requisiti per i re-test).

Al fine di evitare fraintendimenti tra le parti in fase di esecuzione e in sede di validazione/contestazione dei deliverable, si chiede:

Se CSEA intenda adottare (o mettere a disposizione in allegato al Contratto/SAL) specifici Acceptance Test / Acceptance Criteria per le attività oggetto di fornitura (VA/PT di rete, VA/PT applicativi, analisi deep/dark web, re-test), indicanti in modo chiaro e misurabile:

– la struttura minima e i contenuti obbligatori dei report tecnici ed executive;

– i requisiti di dettaglio e di replicabilità delle evidenze (screenshot, log, POC, ecc.);

– eventuali template/formati standard che il Fornitore è tenuto ad utilizzare.

Se, qualora tali criteri di accettazione siano previsti internamente (es. schemi di reportistica o griglie di valutazione già utilizzate da CSEA), sia possibile condividerli con gli operatori economici in fase di gara, in modo da impostare fin da subito i deliverable conformemente alle aspettative dell'Amministrazione.

Se la CSEA confermi che la conformità dei deliverable a tali criteri di accettazione (una volta definiti/condivisi) costituirà il principale riferimento per la validazione dei SAL e per evitare contestazioni basate su valutazioni puramente discrezionali della qualità degli output.

Risposta n. 4

In relazione al quesito, si precisa che la CSEA non prevede, in questa fase, la messa a disposizione di Acceptance Test o Acceptance Criteria formalizzati e standardizzati in allegato al Capitolato. I deliverable dovranno tuttavia essere redatti secondo le best practice di settore e garantire un livello di qualità, completezza e chiarezza adeguato alle finalità delle attività richieste.

Potranno tuttavia essere concordati, preventivamente all'esecuzione, template, formati standard e criteri preventivi di accettazione che, in ogni caso, dovranno sempre includere almeno quanto definito nel capitolato alla voce "Documentazione post esecuzione".

Domanda n. 5

A.5 Re-test, remediation e rischio di “circolo vizioso”

Nel Capitolato è previsto che, a seguito dell’implementazione delle azioni correttive, il Fornitore effettui attività di re-test non conteggiate ai fini del numero complessivo delle esecuzioni previste, con produzione di uno specifico report di verifica.

Si chiede:

· Se le attività di remediation delle vulnerabilità rilevate siano da intendersi a carico esclusivo di CSEA e/o dei suoi fornitori applicativi/infrastrutturali, confermando che il Fornitore dell’appalto in oggetto non è tenuto ad attività di correzione ma solo di verifica (re-test) delle remediation effettuate.

· Se le attività di re-test siano da considerarsi incluse nel corrispettivo complessivo (e quindi senza oneri aggiuntivi per CSEA entro un certo perimetro) oppure se siano previste limitazioni quantitative/temporali (es. numero massimo di cicli di re-test per campagna, durata massima della “finestra di remediation” dopo la quale i re-test ulteriori sono da considerarsi extra-servizio).

· Considerato che, tra la data T0 del test iniziale e la data del re-test, possono emergere nuove vulnerabilità o nuovi exploit, se la CSEA possa confermare che:

· il re-test ha l’obiettivo di verificare esclusivamente la corretta chiusura delle vulnerabilità già identificate nel report originale;

· eventuali vulnerabilità “nuove” emerse nel frattempo non rientrano in quel ciclo di re-test, ma saranno gestite in successive campagne di test o attività dedicate, evitando un circolo vizioso di re-test potenzialmente infinito.

· Se, a tutela sia del Fornitore sia di CSEA, si possa prevedere una finestra temporale massima tra consegna del report e richiesta di re-test (es. 60/90 giorni), decorso il quale il re-test è considerato attività distinta rispetto alla campagna originaria.

· In relazione ai SAL e ai pagamenti, se la CSEA possa confermare che l’accettazione dei deliverable relativi alla campagna principale (VA/PT) e la relativa fatturazione non saranno subordinati alla completa chiusura di tutte le remediation e ai relativi re-test, ma che:

– i re-test saranno oggetto di verifica e accettazione separata;

– eventuali tempi lunghi di remediation interna non comporteranno un blocco indefinito dei pagamenti al Fornitore per attività già svolte e correttamente documentate.

Risposta n. 5

Si conferma che le attività di remediation delle vulnerabilità rilevate rimangono a carico esclusivo della CSEA e/o dei relativi fornitori applicativi e infrastrutturali, fatto salvo quanto previsto in casi specifici al punto 7.1 del Capitolato (Clausole di Sicurezza ai sensi della direttiva NIS2 – D.Lgs. 138/2024).

Si conferma che le attività di re-test sono incluse nel corrispettivo complessivo, senza oneri aggiuntivi per la CSEA, limitatamente a una singola ri-esecuzione per ciascuna campagna di test. Tali attività sono circoscritte alla verifica della corretta risoluzione delle vulnerabilità precedentemente individuate e oggetto di

remediation. Resta inteso che non rientra tra gli obblighi del Fornitore, nell'ambito del re-test, l'individuazione di nuove vulnerabilità o nuovi exploit eventualmente emersi successivamente.

Non è prevista una finestra temporale massima formalizzata tra la consegna del report e la richiesta di re-test; si precisa tuttavia che tali attività potranno essere richieste dalla CSEA entro un termine massimo di 6 mesi oltre la durata contrattuale prevista di 24 mesi.

Si conferma infine che l'accettazione dei deliverable relativi alla campagna principale (VA/PT) e la relativa fatturazione non sono subordinate alla completa chiusura delle remediation né all'esecuzione dei re-test, i quali costituiscono attività successive e oggetto di verifica separata.

Domanda n. 6

A.6 Analisi Deep e Dark Web: frequenza, scope e non divulgazione delle fonti

All'art. 3.3, l'analisi deep/dark web è prevista con frequenza di due esecuzioni in 24 mesi, con obbligo di reportistica, raccomandazioni e supporto in caso di data breach, incluso il riferimento a possibili attività di rimozione dei contenuti.

Si chiede:

· Se l'attività debba consistere in due campagne puntuali, o se CSEA consideri ammissibile un modello di monitoraggio continuativo (con attività di raccolta continuata e reporting consolidato almeno in due momenti formali).

· Se le eventuali attività di rimozione dei contenuti (takedown, interazioni con piattaforme terze, etc.) siano da considerarsi incluse nell'importo o qualificate come attività straordinarie/aggiuntive.

· Considerato che le fonti e i metodi di raccolta sul dark web costituiscono asset sensibili del Fornitore, se la CSEA confermi che non sarà richiesta la divulgazione dettagliata delle singole fonti, canali, account o infrastrutture operative, ma esclusivamente:

– le evidenze pertinenti alla CSEA (indicatori, estratti, screenshot anonimizzati ove possibile),

– la classificazione del rischio e le raccomandazioni operative,

· fermo restando l'obbligo del Fornitore di descrivere in modo chiaro la metodologia e il livello di copertura.

Se la CSEA ritenga opportuno inserire/esprimere nel Capitolato una clausola esplicita di non divulgazione dei metodi specifici di raccolta delle informazioni sul deep/dark web, a tutela della sicurezza operativa del Fornitore.

Risposta n. 6

In relazione al quesito, si precisa che le attività di analisi deep e dark web sono previste dal Capitolato in termini di due esecuzioni nel periodo contrattuale. Resta tuttavia ammessa la possibilità per il Fornitore di adottare un modello di monitoraggio continuativo, purché garantisca un livello di efficacia almeno equivalente e assicuri la produzione della reportistica nei momenti formali previsti.

Con riferimento alle attività di supporto in caso di data breach, incluse eventuali iniziative di rimozione dei contenuti, si precisa che le stesse si intendono comprese nel perimetro del servizio nei limiti delle attività

tecniche e operative ordinariamente eseguibili. Restano escluse eventuali attività che comportino oneri straordinari verso terze parti o costi aggiuntivi non riconducibili alla normale operatività, che saranno oggetto di specifica valutazione.

È richiesto che il Fornitore fornisca evidenze pertinenti alla CSEA, adeguatamente documentate, unitamente alla classificazione del rischio, alle raccomandazioni operative e a una descrizione chiara della metodologia adottata e del livello di copertura.

Con riferimento specifico alle fonti e ai metodi di raccolta delle informazioni sul deep/dark web, ove eventualmente richiesto, inclusi i casi di eventuali obblighi di legge previsti dalla normativa vigente o dietro richiesta delle autorità competenti, dovranno essere forniti, anche tramite specifici accordi di riservatezza (NDA) il dettaglio delle fonti e delle metodologie utilizzate.

Domanda n. 7

A.7 Perimetro degli asset e ampiezza delle campagne VA/PT

In §2 "Contesto" e §3.1–3.2 il perimetro è descritto in termini indicativi (numero di server, indirizzi IP, applicativi esposti, ecc.), ma non sono specificati limiti quantitativi massimi per singola campagna né le modalità di definizione puntuale dello scope di ciascuna esecuzione di VA/PT di rete e applicativi.

Si chiede di chiarire:

· se, per ciascuna esecuzione di Vulnerability Assessment e Penetration Test di rete, sia previsto un numero massimo di indirizzi IP/server da includere nello scope effettivo, e con quali criteri tali asset saranno selezionati (es. elenco nominativo concordato nel Piano delle attività / Rules of Engagement);

· se le quantità riportate a titolo esemplificativo in §2 (utenti, server, applicativi) debbano intendersi come perimetro integrale oggetto di verifica in ogni campagna oppure come dimensionamento complessivo dal quale saranno di volta in volta individuati sottoinsiemi rappresentativi.

Risposta n. 7

Nel paragrafo 3.2 "Vulnerability Assessment e Penetration Test applicativi" è specificato che, per ciascuna sessione, saranno individuati dalla CSEA fino a tre applicativi e/o componenti dell'infrastruttura da sottoporre a verifica, selezionati di volta in volta in funzione delle priorità operative e del livello di rischio.

Per quanto riguarda i Vulnerability Assessment e i Penetration Test di rete, lo scope è riferito all'ambiente di produzione e si intende esteso all'intero perimetro infrastrutturale oggetto del servizio, come descritto nel Capitolato. Le quantità riportate nel §2 devono pertanto intendersi come dimensionamento complessivo del perimetro e, per le attività di rete, come ambito di riferimento integrale per ciascuna campagna.

Domanda n. 8

A.8 Finestre temporali di esecuzione e limitazioni operative sui test

Nel Capitolato non risultano disciplinate le fasce orarie e le eventuali restrizioni operative per l'esecuzione delle attività di VA/PT su sistemi di produzione (es. divieto di svolgere test in orario di esercizio, limitazioni su attività ad alto impatto, ecc.).

Al fine di una corretta pianificazione, si chiede:

· se la CSEA intenda definire, nel Piano delle attività e/o nelle Rules of Engagement, finestre temporali preferenziali o vincolanti per l'esecuzione dei test (es. orario non lavorativo, weekend, change window concordate);

· se siano previste particolari esclusioni o limiti in merito a specifiche tipologie di prova (es. test di tipo DoS/DoS-like, brute force intensivo, attività che possano degradare significativamente le performance dei sistemi di produzione) e, in tal caso, se tali vincoli possano comportare un adeguamento dell'effort e/o del perimetro delle verifiche.

Risposta n. 8

Le finestre temporali di esecuzione delle attività saranno definite e concordate di volta in volta con la CSEA nell'ambito del Piano delle attività e delle Rules of Engagement, tenendo conto dei possibili impatti sui sistemi e sulla continuità operativa. In maniera puramente esemplificativa e non vincolante, le attività su sistemi che supportano i servizi istituzionali della CSEA dovranno essere pianificate al di fuori dell'orario lavorativo, mentre – sempre a titolo esemplificativo e non vincolante – per alcuni sistemi di backend si potrebbero anche valutare esecuzioni in orario lavorativo ordinario.

Con riferimento alle limitazioni operative, eventuali restrizioni relative a specifiche tipologie di test (quali, a titolo esemplificativo, attività di tipo DoS/DDoS, brute force intensivo o altre prove potenzialmente impattanti) potranno essere valutate preventivamente con la CSEA, sulla base di criteri di proporzionalità, minimizzazione del rischio operativo e tutela della continuità del servizio.

Resta inteso che tali eventuali limitazioni non dovranno compromettere la significatività complessiva delle verifiche e non comporteranno alcuna revisione dell'effort o del perimetro delle attività, che rimangono quelli previsti dal Capitolato.

Domanda n. 9

A.9 Tempistiche e prerequisiti per l'attivazione degli accessi (VPN, account, VM)

In §3.1 è previsto che la CSEA metta a disposizione credenziali VPN e, ove richiesto, macchine virtuali di supporto alle attività (es. Kali Linux, Windows Server o equivalenti), ma non sono specificate le tempistiche e le modalità operative per l'attivazione di tali risorse né il loro impatto sul conteggio degli SLA di avvio delle attività.

Si chiede di chiarire:

· entro quali tempi, decorrenti dalla richiesta del Fornitore, CSEA si impegna a fornire: credenziali VPN, account applicativi/di dominio necessari ai test, eventuali VM di supporto;

· se eventuali ritardi, sospensioni o indisponibilità degli accessi imputabili a CSEA o a propri fornitori (es. tempi di provisioning, problemi di rete, change freeze) sospendano o meno il conteggio dei 20 giorni di SLA relativi all'avvio delle attività e l'eventuale applicazione delle penali connesse.

Risposta n. 9

La Stazione Appaltante precisa che le tempistiche di messa a disposizione delle credenziali VPN, degli account applicativi/di dominio e delle eventuali macchine virtuali di supporto non sono oggetto di specifici impegni temporali predeterminati.

Tali attività saranno comunque svolte dalla CSEA con la massima diligenza e tempestività possibile, compatibilmente con i processi interni, i vincoli organizzativi e le eventuali dipendenze da fornitori terzi o infrastrutture esterne.

Resta inteso che eventuali ritardi, sospensioni o indisponibilità nell'attivazione degli accessi e delle risorse, qualora non imputabili al Fornitore, non saranno computati ai fini del calcolo degli SLA relativi all'avvio delle attività né ai fini dell'eventuale applicazione delle penali connesse.

Le modalità operative di attivazione e coordinamento saranno definite in fase esecutiva, anche nell'ambito della pianificazione delle singole attività.

Domanda n. 10

A.10 Coordinamento con altri fornitori e gestione delle indisponibilità dei sistemi

Nel Capitolato non è esplicitata la modalità di coordinamento tra l'aggiudicatario e gli altri fornitori di servizi ICT di CSEA, né il regime applicabile in caso di indisponibilità temporanea dei sistemi dovuta ad attività di terzi (change, manutenzioni, incidenti) che impediscano l'esecuzione delle attività di VA/PT o di analisi deep/dark web.

Si chiede:

· se sia previsto un processo strutturato di coordinamento (es. Change Advisory Board, calendario change, referenti tecnici per applicativi/infrastrutture) tramite il quale CSEA comunichi con adeguato preavviso finestre di indisponibilità dei sistemi;

· se eventuali impossibilità di proseguire i test per cause non imputabili al Fornitore (es. blocchi operativi decisi da CSEA, incidenti su infrastrutture gestite da terzi, freeze di produzione) sospendano gli SLA e l'applicazione delle penali, con conseguente ridefinizione congiunta di calendario e finestra di esecuzione.

Risposta n. 10

La Stazione Appaltante precisa che il coordinamento tra l'aggiudicatario e gli altri fornitori ICT sarà gestito dalla CSEA, nell'ambito dei propri processi organizzativi e operativi e le indisponibilità saranno definite e comunicate nell'ambito della pianificazione esecutiva delle attività.

Con riferimento agli SLA, eventuali indisponibilità dei sistemi o impossibilità di proseguire le attività per cause non imputabili al Fornitore, ivi incluse quelle derivanti da decisioni della Stazione Appaltante o da interventi di terzi, non saranno computate ai fini del calcolo delle tempistiche contrattuali né dell'eventuale applicazione delle penali.

In tali circostanze, le parti procederanno alla ridefinizione del calendario e delle finestre di esecuzione, nel rispetto degli obiettivi del servizio.

Domanda n. 11

A.11 Analisi dei domini impersonati / typosquatting – metodologia e copertura attesa

In §3.3, tra le attività di analisi del deep/dark web, è incluso l'"utilizzo fraudolento o impersonificazione di domini e servizi riconducibili alla CSEA", ma non è specificato il livello di copertura atteso né l'approccio metodologico alla ricerca di domini impersonati (es. typosquatting.

Si chiede:

· un chiarimento sul livello di copertura sia atteso nella ricerca di tali domini (ad es. utilizzo di servizi/strumenti di generazione di varianti del nome a dominio, monitoraggio di nuove registrazioni su specifici TLD, o altro) e se sia sufficiente che il Fornitore proponga e descriva nel piano di monitoraggio la propria metodologia, fermo restando il rispetto dei vincoli normativi applicabili

Risposta n. 11

Si precisa che il Capitolato non definisce uno specifico livello di copertura né una metodologia vincolante per l'individuazione di domini impersonati o fenomeni tipo typosquatting o assimilabili. Il Fornitore è pertanto tenuto a proporre, in fase esecutiva, un approccio metodologico coerente con le best practice di settore, garantendo un livello di copertura adeguato al contesto della CSEA.

Resta inteso che tale metodologia dovrà essere descritta nel piano delle attività o di monitoraggio e potrà essere oggetto di condivisione e affinamento con la CSEA, nel rispetto dei vincoli normativi applicabili.

Domanda n. 12

Riferimenti ai controlli GV.SC-1, GV.SC-5, ID.IM-4, RC.RP-1, PR.AA-1

All'art. 7.1 vengono richiamati i controlli "GV.SC-1, GV.SC-5, ID.IM-4, RC.RP-1, PR.AA-1" come se fossero riferimenti diretti al D.Lgs. 138/2024 (attuazione Direttiva NIS2).

Si chiede:

· Se tali riferimenti siano da intendersi come richiamo al Framework Nazionale di Cybersecurity / NIST CSF 2.0 utilizzato da CSEA come modello interno, e non come denominazione di controlli contenuti testualmente nel D.Lgs. 138/2024.

· Se la CSEA possa confermare che detti controlli rappresentino criteri di riferimento/buone pratiche cui il servizio deve essere coerente, senza introdurre oneri normativi ulteriori rispetto a quanto previsto dalla legge.

· Se esista un documento interno (scheda di controllo, policy) che declini tali controlli in requisiti concreti per i fornitori e se sia possibile metterlo a disposizione degli operatori economici.

Risposta n. 12

La Stazione Appaltante precisa che i riferimenti ai controlli "GV.SC-1, GV.SC-5, ID.IM-4, RC.RP-1, PR.AA-1" sono da intendersi quelli specificati da ACN quale Autorità nazionale competente NIS, di cui all'art 10 comma1 del D.Lgs138/2024 (Decreto NIS), con propria determinazione n. 379907/2025, allegato 1, applicabili a CSEA in qualità di soggetto rientrante nel perimetro di applicazione del decreto NIS.

Con riferimento alla documentazione interna di dettaglio, si rappresenta che la stessa potrà essere resa disponibile, ove necessario, esclusivamente in favore dell'aggiudicatario, previo perfezionamento di idonei accordi di riservatezza (NDA), in coerenza con le esigenze di sicurezza della Stazione Appaltante.

Domanda n. 13

Incongruenze nella numerazione degli articoli e clausole ex artt. 1341–1342 c.c.

In §7.8–7.9 si rilevano alcune discrepanze:

"Subappalto e divieto di cessione del contratto" rubricato nel testo come art. 7.4, ma richiamato come "7.5";

"Modalità di pagamento" rubricato come art. 7.5, ma citato talvolta con numerazione non coerente;

Foro competente indicato nel corpo come art. 7.12, ma richiamato come "7.13 (Foro competente)" tra le clausole da approvare ex artt. 1341–1342 c.c.

Si chiede:

· Conferma della numerazione corretta degli articoli 7.4, 7.5, 7.12 e 7.13.

· Conferma puntuale dell'elenco delle clausole che CSEA intende sottoporre a specifica approvazione ai sensi degli artt. 1341 e 1342 c.c., con numerazione definitiva (es. "art. 7.x – …").

Risposta n. 13

Si conferma che l'errata numerazione degli articoli è un mero errore materiale.

Pertanto, la numerazione corretta è la seguente: 7.4. "Subappalto e divieto di cessione del contratto"; 7.5 "Modalità di pagamento"; 7.12 "Foro Competente": 7.13 "Normativa di rinvio".

Le clausole contrattuali che dovranno essere specificatamente approvate mediante ulteriore sottoscrizione da parte del contraente, ai sensi degli artt. 1341 e 1342 c.c., sono: 5 ("Durata del contratto"); 6 ("Penali"); 7.4("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"); 7.12 ("Foro Competente").

Domanda n. 14

Accettazione e sostituzione delle risorse chiave

In §4.1 sono previsti specifici requisiti in termini di competenze tecniche e linguistiche per le risorse impiegate, ma non è esplicitato come l'eventuale richiesta di sostituzione di una risorsa da parte di CSEA incida sul rispetto degli SLA e sull'applicazione delle penali.

Si chiede:

· se il rifiuto o la richiesta di sostituzione di una risorsa da parte di CSEA, per motivazioni non riconducibili a inadempimento del Fornitore, possa incidere sull'applicazione delle penali per ritardi e se, in tal caso, siano previste forme di sospensione degli SLA per il periodo necessario alla sostituzione.

Risposta n. 14

La Stazione Appaltante precisa che l'eventuale richiesta di sostituzione di una risorsa è da intendersi quale misura a tutela della CSEA, finalizzata a garantire il conseguimento dei risultati attesi in termini di qualità delle prestazioni e rispetto delle tempistiche contrattuali, ivi inclusi gli SLA previsti.

Gli SLA devono pertanto intendersi comprensivi dell'insieme delle responsabilità in capo al Fornitore, incluse quelle relative al corretto dimensionamento e alla adeguata qualificazione delle risorse impiegate nel servizio.

Ne consegue che eventuali esigenze di sostituzione delle risorse non determinano, di per sé, sospensioni o esclusioni dal computo degli SLA, restando in capo al Fornitore l'onere di assicurare la continuità operativa e il rispetto degli obblighi contrattuali mediante tempestiva individuazione di risorse idonee.

Domanda n. 15

Subappalto di attività specialistiche

In §7.4 è ammesso il subappalto, con divieto di affidare in subappalto l'integrale esecuzione delle prestazioni oggetto del contratto, ma non è esplicitata la possibilità di subappaltare singole componenti specialistiche del servizio mantenendo la responsabilità complessiva in capo all'aggiudicatario.

Si chiede di confermare:

· che sia ammesso il subappalto di specifiche attività specialistiche, nel rispetto dei limiti di legge e fermo restando il vincolo di responsabilità solidale dell'aggiudicatario nei confronti di CSEA;

· se CSEA applichi, oltre ai limiti percentuali previsti dal Codice dei contratti pubblici, ulteriori soglie interne massime di subappalto in relazione al valore complessivo dell'appalto

Risposta n. 15

Si conferma che è ammesso il subappalto di specifiche attività specialistiche, nel rispetto dei limiti di legge e fermo restando il vincolo di responsabilità solidale dell'aggiudicatario nei confronti della CSEA.

Non sono previste soglie interne massime di subappalto.

Domanda n. 16

Con riferimento al capitolato tecnico, Cap. 6 "Penali", sono previsti due distinti SLA con relative penali per la mancata notifica entro 24 ore di incidenti. Si chiede di specificare meglio le caratteristiche di questi SLA in quanto la fornitura non prevede un monitoraggio continuativo dell'infrastruttura di CSEA, ma degli *assessment* e test in determinati periodi condivisi con CSEA.

Risposta n.16

La Stazione Appaltante precisa che il servizio oggetto dell'appalto non prevede un monitoraggio continuativo dell'infrastruttura CSEA, confermando che le attività sono eseguite nei periodi pianificati e condivisi con la Stazione Appaltante.

Ciò premesso, l'obbligo di notifica entro 24 ore di eventuali incidenti di sicurezza, compromissioni dei sistemi o vulnerabilità critiche (CVSS ≥ 9.0) deve intendersi riferito a tutte le evidenze rilevate dal Fornitore nell'ambito delle attività svolte, sia durante la fase operativa di esecuzione delle attività, sia in fasi successive anche, ma non solo, connesse alle medesime, quali, a titolo esemplificativo e non esaustivo, l'analisi delle risultanze e la redazione della reportistica.

In tali casi, la comunicazione dovrà avvenire tempestivamente al momento della rilevazione, senza attendere, ad esempio nel citato caso, la formalizzazione del report finale o altri momenti di rendicontazione e riscontri.

Resta altresì inteso che il medesimo obbligo di notifica, con le relative tempistiche e penali, si applica anche agli eventuali incidenti di sicurezza, vulnerabilità critiche o compromissioni che dovessero interessare le infrastrutture del Fornitore e che possano avere un impatto, diretto o indiretto, sulla CSEA, quali, a titolo esemplificativo, accessi non autorizzati a dati, informazioni o risultanze riferibili alla Stazione Appaltante. Tale ultimo obbligo ha carattere continuativo e non è limitato ai soli periodi di esecuzione delle attività contrattuali.

Restano fermi in ogni caso tutti gli altri obblighi di legge previsti per la notifica di incidenti da parte dei fornitori verso le stazioni appaltanti.