Capitolato Tecnico

Servizi di Penetration Test per il Sistema Informativo della Cassa per i Servizi Energetici e Ambientali - CSEA
CIG: B20972A0D4

Responsabile Unico del Procedimento: Pietro Abbati Marescotti

1. Introduzione

1.1 Premessa

Il presente Capitolato Tecnico (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 l'evoluzione e la piena operatività dei Sistemi Informativi necessari per lo svolgimento delle attività istituzionali della Cassa per i Servizi Energetici e Ambientali (di seguito CSEA).

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 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'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.

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.

Nell'ambito Sistemi Informativi, la CSEA ha inoltre ottenuto le seguenti certificazioni:

- “Progettazione, Sviluppo e Gestione della infrastruttura ICT a supporto dei servizi IT” - ISO/IEC 27001:2017;
- “Continuità operativa della infrastruttura ICT a supporto dei servizi IT” – ISO 22301:2019.

L’incremento quantitativo e qualitativo delle attività richieste alla CSEA impegna rilevanti investimenti economici e di capitale umano sul fronte informatico, con l’apprestamento di portali e sistemi dedicati a specifiche disposizioni regolatorie, nonché un’intensa attività di interlocuzione con gli operatori di settore per eventuali chiarimenti, contraddittori e supporti operativi.

Le attività del Sistema Informativo di CSEA hanno origine, quindi, dalle disposizioni normative e si manifestano fondamentalmente su tre versanti:

1) nuove aree di intervento della CSEA;
2) adeguamento continuo delle aree di intervento già presenti nel novero delle attività dell’Ente;
3) gestione del Sistema Informativo includendo in questa le attività di manutenzione correttiva e preventiva.

Il Sistema Informativo CSEA potrà essere soggetto, inoltre, ad una progressiva ristrutturazione e adeguamento alle nuove architetture e tecnologie. A titolo meramente esemplificativo, non esaustivo e non vincolante, le revisioni architetturali potranno prevedere un approccio SOA anche tramite microservizi, estensione della gestione tramite bus a tutti gli applicativi di CSEA, gestione di questi tramite container nonché utilizzo del cloud e la predisposizione e l’integrazione per servizi su blockchain.

1.3 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, comunque, 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.

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
Attività di progetto	Un insieme di attività inerenti un progetto, finalizzate ad un preciso risultato in un lasso di tempo stabilito; le attività concorrenti allo scopo possono richiedere anche interventi realizzativi, adeguativi, manutentivi o evolutivi.
ASI	Area Sistemi Informativi della CSEA
Dichiarazione	Documento tecnico ed operativo dove sono raccolte ed elaborate le informazioni inserite tramite i sistemi di raccolta dati. Possono essere firmate digitalmente e costituiscono la base per la definizione delle informazioni contabili.
FTE	Full Time Equivalent – "risorsa equivalente a tempo pieno", ovvero le risorse necessarie per svolgere una determinata attività o realizzare un progetto, dove un FTE corrisponde sostanzialmente ad un giorno-persona. Con riferimento all'organico per un'attività o un progetto un FTE corrisponde ad una risorsa disponibile a tempo pieno per l'intervallo temporale considerato.
Gestione Progetti	Software Redmine, utilizzato per la pianificazione di progetti e per il tracciamento delle attività, richieste, ticket e bug tramite interfaccia web, nonché per parte della documentazione.
Headcount	Numero di persone fisiche, per il contesto di riferimento.
Fornitore	Il soggetto aggiudicatario della presente procedura di affidamento.
Fornitura	Si intende la fornitura di tutti i servizi oggetto del Capitolato
Manutenzione adeguativa normativa	A seguito di aggiornamenti normativi (es. delibere ARERA) i sistemi dovranno essere adattati di conseguenza. Alcuni esempi sono: aggiornamento delle componenti tariffarie dei settori elettrico, gas ed idrico; aggiornamento della procedura di gestione del Bonus Sociale; adeguamento dei portali esterni, a vincoli normativi europei, ad es. GDPR.

Manutenzione adeguativa tecnica	A seguito di aggiornamenti tecnologici (es. librerie, sistemi operativi o versioni Java non più supportate ed il cui uso è attualmente sconsigliato in favore di una versione più recente), le componenti dei diversi sistemi dovranno essere aggiornate di conseguenza. Inoltre, definisce anche l'insieme degli adeguamenti necessari per migliorare la fruibilità, la sicurezza e la gestione del sistema. Ad esempio: la separazione su macchine distinte di Application Server e Database; l'aggiornamento della piattaforma della Java Virtual Machine ad una nuova LTS (*Long Term Support*, supporto a lungo termine); l'aggiornamento di un protocollo di comunicazione tra due sistemi applicativi in favore di termini di sicurezza (es. conversione da *http* ad *https*).
Manutenzione correttiva	Rappresenta l'insieme di azioni reattive che non concorrono ad aumentare il valore o la produttività e le prestazioni di un sistema, ma tendono ad un semplice ripristino dello status quo ante l'insorgere di un guasto o di un'avaria prevenendo che questa si ripeta ulteriormente. Include anche l'insieme delle azioni reattive atte al funzionamento di un sistema in coerenza con quanto previsto dai requisiti, espliciti ed impliciti.
Manutenzione preventiva	Rappresenta l'insieme di azioni atte a prevenire un guasto/bug/incidente per evitare ricadute sui sistemi. Ad esempio, le azioni per contenere l'utilizzo della memoria da parte di un applicativo durante il suo esercizio. Gestione delle politiche di *log rotation* e *log retenction* per prevenire la saturazione dei dischi.
Meccanismo	Tutto ciò che deve essere dichiarato dalle aziende che non rientra nell'ambito delle componenti tariffarie
Modalità *on demand*	Un servizio effettuabile anche "su chiamata" che garantisce in ogni caso la piena efficacia del servizio al committente, lasciando al contempo al Fornitore la libera organizzazione delle risorse.
No regression test	Il test di regressione, o "no regression test", è una tipologia di software testing con la quale è possibile verificare che le modifiche apportate per una finalità specifica non pregiudichino altre funzionalità già esistenti.
PMO	PMO è l'acronimo di Project Management Office/Officer e nel contesto di questo capitolato si riferisce ad una persona fisica (Officer) del Fornitore. Si occupa di analizzare complessivamente l'andamento dei diversi progetti in una unica ottica consolidata. È deputato inoltre alla verifica dell'allineamento strategico con

	quanto atteso da CSEA, al monitoraggio complessivo dei rischi, dei progressi ed in generale alla governance delle risorse. I diversi Project Manager riportano quindi al PMO lo stato di avanzamento dei progetti gestiti, il livello di completamento delle attività pianificate, l'allocazione ed il rendimento del team di progetto, il risk management e tutte le metriche ed informazioni relative all'andamento del progetto da essi gestito.
Progetto	Un insieme di attività coerenti finalizzate allo sviluppo o alla più generale gestione di una entità specifica di CSEA (es. "progetto di manutenzione del sistema Energivori" o ad esempio un progetto per una nuova attività assegnata a CSEA).
PSN	Il Polo Strategico Nazionale (PSN) è l'infrastruttura ad alta affidabilità che ha l'obiettivo di dotare la Pubblica Amministrazione di tecnologie e infrastrutture cloud che possano beneficiare delle più alte garanzie di affidabilità, resilienza e indipendenza. Il Dipartimento per la trasformazione digitale ha promosso la creazione del Polo Strategico Nazionale. Vedasi https://innovazione.gov.it/dipartimento/focus/polo-strategico-nazionale/
SII	Il Sistema informativo Integrato (SII), istituito presso l'Acquirente Unico con la legge del 13 agosto 2010, n. 129/10, ha la finalità di gestire i flussi informativi fra i soggetti che partecipano ai mercati dell'energia elettrica e del gas secondo le regole e i procedimenti definiti dall'Autorità. CSEA definisce ed organizza flussi informativi in sinergia con il SII.
SIEM	Con l'acronimo SIEM (security information and event management) ci si riferisce ad una serie di prodotti software e servizi che combinano/integrano le funzionalità offerte dai SIM (security information management) a quelle dei SEM (security event management).
Sistema di deleghe	Insieme di logiche per la gestione delle deleghe dai rappresentanti della persona giuridica verso altre persone fisiche, per specifiche attività sui sistemi della CSEA.
SPOC	Single Point of Contact, referente primario per l'ambito assegnato.

Supporto all'operatività	Supporto agli utenti per eventuali attività per le quali non siano già previste adeguate funzionalità che consentano all'utente piena autonomia. Ad esempio, la consultazione o la rettifica in base dati di informazioni qualora non esista una interfaccia utente dedicata allo scopo
UAT	User Acceptance Test: collaudi (effettuati dall'utente CSEA) per la validazione finale di quanto implementato dal Fornitore.
Utenti	Personale CSEA o soggetti esterni ad essa che operano sui sistemi di CSEA, scevri da capacità tecniche-informatiche.

2. Contesto

Il Sistema Informativo della CSEA prevede diverse aree d'intervento, nell'ambito delle quali sono presenti servizi agli utenti, fruibili sia internamente (utenti CSEA e loro collaboratori) che esternamente (aziende, istituzioni o altri soggetti che interagiscono con la CSEA).

Nel presente Capitolato sono riportate indicazioni relative alle metodologie e agli strumenti di supporto per l'esecuzione ed il controllo del servizio, cui il Fornitore dovrà conformarsi senza oneri aggiuntivi per la CSEA.

Nel presente documento è rappresentata la situazione attuale; è previsto che nel corso del 2024 la CSEA migrerà i propri sistemi verso il Polo Strategico Nazionale, con possibili variazioni rispetto a quanto qui riportato.

2.1 Introduzione al Sistema Informativo CSEA

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.

Il sistema è ad oggi costituito in gran parte da c.d. *Sistemi Custom* sviluppati in JEE, nonché da una serie di sistemi proprietari (Open Source / freeware o meno) con specifiche personalizzazioni per le esigenze delle CSEA (es. SAP FI/CO, o "Piuma" quale customizzazione ed estensione di Alfresco per la gestione del Protocollo, etc.).

La CSEA, per quanto qui esposto e più in generale per quanto presente nel documento, si riserva il diritto di poter aggiornare ed integrare l'infrastruttura e gli elementi tecnologici che la caratterizzano nell'ottica di costante miglioramento delle architetture e delle scelte tecnologiche che su queste sono basate.

2.2 Architettura Tecnologica

L'infrastruttura CSEA è, al momento di redazione del presente documento, distribuita su due CED, connessi tra di loro mediante VPN ed in prospetto di migrazione sul PSN (Polo Strategico Nazionale);

l'ambiente virtuale è attualmente basato sulla soluzione di iperconvergenza Simplivity ed è organizzato e diviso in due versioni separate basate sull'hypervisor Vsphere su un totale di 11 nodi. L'infrastruttura di supporto all'operatività prevede la presenza di NAS che hanno lo scopo di garantire il file sharing tra i sistemi applicativi e quelli dedicati alla conservazione di informazioni, ulteriori sistemi di sicurezza perimetrale e di bilanciamento del carico, questi ultimi basati su tecnologia F5, e sistemi a supporto delle comunicazioni telematiche.

In particolare, i sistemi in opera nell'infrastruttura di CSEA sui quali il Fornitore potrebbe essere chiamato ad operare e per i quali sono richieste competenze specializzate sono, a titolo esemplificativo e non esaustivo i seguenti:

1) Simplivity per virtualizzazione tramite Vmware;
2) Microsoft Active Directory, Windows Server e Microsoft 365;
3) Linux Server, principalmente in distribuzioni Debian based;
4) Commvault, Software di backup centralizzato;
5) NetAPP, Nas di rete (usato per i backup di Commvault);
6) F5 Bilanciatori e Firewall applicativi;
7) Hyperledger;
8) La gestione dell'offerta del PSN.

I sistemi server virtualizzati di CSEA, necessari all'erogazione dei servizi applicativi, sono basati su architettura x86 a 64bit. Per i servizi applicativi, a livello di sistemi operativi, è presente una infrastruttura mista che comprende sistemi Windows Server e Linux Server.
Le infrastrutture implementano strategie di *Disaster Recovery* e *Business Continuity*, parzialmente anche geografiche (attualmente, sarà implementato diversamente nel PSN), al fine di garantire la continuità nell'erogazione dei servizi.

In ogni caso gli ambienti di sviluppo ed integrazione sono e comunque dovranno essere mantenuti separati dal perimetro di esercizio.

2.3 Architettura Applicativa

Le infrastrutture di calcolo di CSEA si basano, quasi esclusivamente, su sistemi con architetture hardware e con processori *multi-core*.

La piattaforma di virtualizzazione è basata su VMWARE. L'utilizzo della piattaforma virtuale è assolutamente preferenziale: l'eventuale ricorso a server fisici deve essere opportunamente motivato o da oggettive esigenze di natura tecnica o da eventuali SLA computazionali stringenti richiesti dal business (ad esempio: elaborazioni che devono concludersi entro un tempo prefissato e che, quindi, richiedono delle risorse dedicate).

L'infrastruttura CSEA prevede l'erogazione di servizi applicativi per la raccolta, la condivisione e l'elaborazione di informazioni, finalizzate alla gestione dei processi di competenza. L'infrastruttura applicativa è prevalentemente basata sulla piattaforma di sviluppo JEE e sta progressivamente migrando verso un sistema a bus che contempla sia la SOA che i microservizi, basato sul cloud,

orchestrato (con attività di integration e di messaging) ed a container. I servizi applicativi sono erogati ad oggi principalmente tramite Apache Tomcat.

Le informazioni raccolte attraverso portali dedicati vengono acquisite e conservate in apposite basi di dati ed elaborate nelle fasi successive dei processi aziendali.

L'architettura applicativa di riferimento descritta nel documento è impostata su un modello organizzativo a più livelli (*n-tiers*), come da standard e *best practice* di settore.

L'architettura applicativa attuale è strutturata sulla base dei seguenti livelli logici:

1) Livello di presentazione (interfaccia utente)
2) Livello Logico Applicativo (*business logic*)
3) Livello di integrazione (integrazione con sottosistemi o con altri sistemi)
4) Livello Dati (persistenza delle informazioni)

Lo scambio di informazioni tra i componenti applicativi avviene ad oggi principalmente tramite:

- il modello basato sul paradigma SOA (interfacce SOAP e REST);
- alcuni servizi applicativi vengono consumati direttamente; altri sono invece esposti attraverso dei bus multicanale dedicati (TIBCO, che progressivamente è inserito come layer intermedio, e l'antecedente Enterprise Service Bus basato su soluzione open source Mule ESB), che coordina specifici processi di business; si anticipa che il cambio architetturale richiesto vedrà l'esposizione ed il consumo di tutti i servizi tramite TIBCO;
- procedure ETL che gestiscono flussi di dati asincroni costituiti da volumi rilevanti, attraverso il supporto della soluzione open source *Hitachi Pentaho data integration* ed in futuro integrate e gestite da TIBCO.

Il sistema per la gestione del database dei servizi applicativi è attualmente MariaDB/MySQL. Sono altresì presenti soluzioni basate su PostgreSQL ed SQL Server.

Il framework di riferimento per la realizzazione dei componenti applicativi basati su tecnologia Java è Spring versione 5 e successive, mentre le dipendenze sono gestite attraverso Maven.

2.4 Aree Applicative

Nel novero di quanto sopra enunciato si evidenziano le seguenti principali aree applicative oggetto del presente Capitolato; ove non diversamente indicato i sistemi sono da intendersi *legacy*:

1) Sistemi applicativi per le dichiarazioni e la raccolta di informazioni da soggetti esterni;
    a. Anagrafica
    b. Data Entry Elettrico
    c. Data Entry Gas
    d. Data Entry Idrico
    e. Data Entry Rifiuti, con possibile dismissione a breve
    f. Portale istanze

g. Portale Elettrivori (precedentemente noto come Energivori)
h. Portale Gasivori
i. Portale per la Perequazione Elettrica
j. Portale per la Perequazione Gas
k. Portale Elenco Esperti
l. RAB (portale dedicato alle aziende con un numero di POD (*Point Of Delivery*) inferiore a 25.000)
m. PQS (portale per la Qualificazione degli Sportelli delle Associazioni dei Consumatori)

2) Sistemi applicativi di *backoffice* per il controllo, la verifica ed ogni elaborazione necessaria da parte di CSEA:
   a. Gestionale
   b. Bonus Sociale
   c. Sistema Indennitario
   d. Flussi Banca
   e. RNA, applicazione desktop Java per l'integrazione e l'interazione con il portale RNA (Registro Nazionale degli Aiuti di Stato)
3) Sistemi a supporto per il controllo, lo smistamento e lo scambio delle informazioni tra i sistemi, fondamentalmente di carattere finanziario, economico e contabile:
   a. Flussi SAP, che estende le sue funzionalità anche oltre le comunicazioni con il sistema SAP
   b. Flussi Banca
   c. Flussi Sepa
   d. Pago PA (sistema legacy per l'integrazione con i servizi offerti dal partner tecnologico di Pago PA)
   e. Mule ESB
   f. Suite TIBCO per l'Integration e Messaging, la gestione delle code, delle API e delle ETL nonché l'orchestrazione
   g. Nagios per il c.d. monitoraggio preventivo dei sistemi, a livello sistemistico, di risorse e di responsività applicativa. In corso di implementazione al tempo di redazione del presente capitolato.
4) Integrazioni, scambio file ed API verso:
   a. Piuma, quale sistema di protocollazione e conservazione documentale, applicativo basato su Alfresco
   b. Sistema di gestione dei processi amministrativo-contabili, SAP
   c. SAS quale sistema di reportistica

5) Sistemi di conservazione delle informazioni (database)
   a. MariaDB/MySQL
   b. PostgreSQL
   c. SQL Server
   d. Filesystem (NAS)

e. Sistemi S3 sul cloud
f. Sistemi di backup, anche a nastro

2.5 Dimensionamento dei sistemi

Si riportano di seguito alcune metriche indicative del dimensionamento dei sistemi di CSEA, in considerazione di una ricognizione attuale degli stessi. *Questi volumi o stime ed ulteriori riportate nel presente capitolato sono da ritenersi puramente indicative e non vincolanti in alcun modo per la presentazione dell'offerta e per l'esecuzione del contratto.*

- Numero di utenti interni: inferiore a 200;
- Numero di utenti esterni: inferiore a 10.000;
- Sistemi Microsoft: circa 50 server per l'erogazione dei soli servizi qui riportati ed in ambiente di esercizio; complessivamente si contano circa 90 server Windows;
- Sistemi Linux: circa 20 server per l'erogazione dei soli servizi di esercizio qui riportati ed in ambiente di esercizio; complessivamente si contano circa 40 server Linux.

3. Descrizione dei servizi e modalità di erogazione della fornitura

Ferma restando la più generale definizione del contesto della CSEA, si riporta di seguito la descrizione dei servizi richiesti, corredata delle ulteriori informazioni a supporto

3.1 Penetration Test di rete

- La voce consiste nella valutazione della sicurezza informatica progettata per individuare e analizzare vulnerabilità, debolezze o falle nei sistemi informatici, nelle reti o nelle applicazioni simulando gli approcci e le tecniche degli aggressori informatici al fine di identificare e mitigare i rischi per la sicurezza. Lo scopo principale dei Penetration Test è quello di fornire un'analisi dettagliata della sicurezza di un sistema e raccomandazioni per migliorare la sua resilienza agli attacchi. Si richiede che il posizionamento venga effettuato in modalità "utente esterno autenticato" (ovvero da rete pubblica e simulando una impresa che si relaziona con la CSEA) nonché un utente interno (ovvero da rete interna simulando di aver acquisito il controllo della postazione e credenziali di un collega CSEA, senza privilegi di amministratore).
- Informazioni a supporto: la rete interna consta indicativamente di 225 IP attivi, distribuiti su 147 server. La CSEA fornirà credenziali VPN e, se richiesto, le macchine virtuali (es. Kali Linux, Windows Server 2019, etc.) secondo le indicazioni che l'aggiudicatario richiederà. Si specifica che, a seguito di movimentazione verso il PSN la configurazione di rete e delle macchine potrebbe subire dei lievi cambiamenti; La CSEA renderà inoltre disponibili, previa firma di un NdA, le risultanze dei Vulnerability Assessment e Penetration Test svolti in precedenza.
- Frequenza: si chiede l'esecuzione due volte durante l'esecuzione del contratto.

3.2 Penetration Test applicativi

- I Penetration Test applicativi sono un tipo specifico di test di sicurezza informatica focalizzati sull'analisi delle vulnerabilità presenti nelle applicazioni software. Questi test mirano a identificare e valutare le potenziali debolezze nei codici, nei protocolli di comunicazione e

nelle funzionalità dell'applicazione stessa. Gli obiettivi includono la scoperta di vulnerabilità che potrebbero essere sfruttate per l'accesso non autorizzato, la manipolazione dei dati o altri attacchi dannosi. Durante i Penetration Test applicativi, gli esperti di sicurezza informatica utilizzano una serie di tecniche, strumenti e metodologie per eseguire simulazioni di attacchi e analizzare la resistenza dell'applicazione agli stessi.

- Informazioni a supporto: dovranno essere effettuati su due applicativi, da selezionare con la CSEA.
- Frequenza: si chiede l'esecuzione due volte durante l'esecuzione del contratto (su due set di applicativi diversi).

Al termine delle attività dovranno essere consegnati i report con un livello di dettaglio tale da consentire la replicazione delle azioni in futuro.

3.3 Analisi del Dark Web

- La voce consiste nella individuazione e rimozione di violazioni di dati sensibili e casi di *data breach* su *deep* e *dark web*;
- Informazioni a supporto: al momento della redazione del presente capitolato non sono mai state effettuate attività di analisi del *dark web*.
- Frequenza: si chiede l'esecuzione una volta durante l'esecuzione del contratto.

4. Modalità di esecuzione dei Servizi

Scopo del presente capitolo 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 sola ASI. 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 ogni attività si richiede che ciascuna risorsa impiegata abbia capacità espressive (scritte, verbali) della lingua italiana pari al livello C2 nel quadro di riferimento europeo *Common European Framework of Reference for Languages* (CEFR).

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.

La CSEA richiede la preventiva condivisione del CV delle risorse ed un colloquio con queste per una sua valutazione antecedente all'inserimento di queste nel gruppo di lavoro ad essa dedicato. La CSEA si riserva inoltre, in ogni momento dell'esecuzione del servizio, di richiedere la sostituzione di

una o più risorse allocate dal Fornitore per la CSEA. Il Fornitore dovrà sempre garantire la sostituzione delle risorse richieste che dovranno essere prontamente e nel minor tempo possibile sostituite con ulteriori, rimanendo responsabile in ogni caso della continuità complessiva delle attività assegnate al fornitore.

In ogni caso, per le nuove risorse del Fornitore inserite nel contesto CSEA, siano esse in sostituzione di ulteriori o meno, il periodo di formazione, qualora necessario, rimarrà a carico del Fornitore. In questo caso le attività dovranno essere necessariamente consuntivate ed esplicitamente categorizzate come "formazione". La formazione potrà essere verificata tramite gli strumenti messi a disposizione da CSEA.

5. 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 ASI, il RUP, o il Direttore dell'esecuzione effettueranno anche disgiuntamente, 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, i pagamenti saranno sospesi sino a completamento con esito positivo delle suddette verifiche.

Firmato digitalmente da: PIETRO ABBATI MARESCOTTI
Luogo: Roma
Data: 10/06/2024 17:08:17