ENGINEERING

SERVIZI DI ASSESSMENT DI SICUREZZA INFORMATICA

PROPOSTA TECNICO-ECONOMICA

NS. RIF OFF258/gm/2021_PTE **Roma, 30/09/2021**

INDICE GENERALE

1 PREMESSA

I recenti attacchi cyber hanno mostrato l'imprescindibile necessità di mettere in sicurezza le infrastrutture aziendali, al fine di renderle sempre meno vulnerabili di fronte ad intrusioni e minacce esterne.

Prendendo atto di questa esigenza, il presente documento si pone l'obiettivo di illustrare la Proposta Tecnico-Economica di Engineering Ingegneria Informatica S.p.A. (d'ora in poi anche Engineering) relativa alla **mappatura dell'Information Security dei macro-processi di business, attraverso security assessment, vulnerability assessment e penetration test**, così fornendo uno fotografia chiara del livello di postura aziendale ed identificando in maniera puntuale le azioni di remediation da porre in essere a salvaguardia dell'Azienda.

Il presente documento costituisce parte integrante della documentazione contrattuale unitamente ai seguenti documenti:

- Condizioni Generali di Vendita – Off258/gm/2021_CGV
- Lettera d'accompagnamento – Off258/gm/2021_LA
- Informativa per i Clienti sul trattamento dei dati ex art. 13 Regolamento UE 2016/ - Off258/gm/2021_PRV.

1.1 OBBLIGO DI RISERVATEZZA

Le informazioni contenute nel presente documento devono ritenersi strettamente confidenziali ed il Cliente è tenuto, pertanto:

- a non utilizzarle per finalità diverse dalla valutazione della proposta;
- a non divulgarle e a fare in modo che non vengano divulgate direttamente o indirettamente a soggetti diversi dal proprio personale direttamente coinvolto nella valutazione della stessa;
- a non copiarle, riprodurle, duplicarle, senza il preventivo consenso scritto di Engineering I.I. S.p.A.

1.2 LE CERTIFICAZIONI

Il gruppo Engineering ha definito un proprio Sistema Gestione Qualità Aziendale, ovvero ha individuato la struttura organizzativa, le procedure, i processi e le risorse in grado di attuare la Politica per la Qualità enunciata dall'Alta Direzione aziendale.

Le aziende del Gruppo sono dotate di certificazioni ISO 9001.
Nell'ambito dello sviluppo software, la Capogruppo ha superato l'assessment al livello 3 secondo il modello CMMI® (CMMI-SE/SW v1.2 staged representation).
Infine, le sedi del Gruppo che ospitano i data center possiedono le certificazioni ISO 27001 – 27017 – 27018: per i sistemi di gestione della sicurezza nelle tecnologie dell'informazione e ISO 20000 per la gestione dei servizi IT

2 PERIMETRO DEI SERVIZI OGGETTO DI FORNITURA

Di seguito vengono sinteticamente elencate le fasi di progetto per i servizi oggetto della presente offerta:

Oggetto di fornitura	Tipologia di Servizio	Vincoli/quantità
Service Management	A corpo	5gg
Security Assessment	A corpo	80gg
Vulnerability Assessment	A corpo	Fino a 500 IP Interni
Penetration Test	A corpo	Max 10 IP perimetro esterno, black box

Nel successivo capitolo 3 verranno dettagliatamente descritti tutti i servizi che compongono la fornitura.

3 SERVIZI OGGETTO DI FORNITURA

Di seguito vengono illustrati nel dettaglio i servizi oggetto della presente offerta, suddivisi in servizi di Service Management e servizi di valutazione della sicurezza.
Al fine di poter ottenere una visione completa partendo da un livello alto dello stato attuale dell'Organizzazione, si propone di applicare la Metodologia proprietaria di cui il Gruppo Engineering si è dotato per i processi delle strutture Sanitarie.

3.1 SERVICE MANAGEMENT

Il service manager definisce la roadmap che individui con maggiore precisione possibile:

- il percorso di attuazione del progetto;
- le attività da svolgere;
- i tempi di realizzazione;
- l'insieme degli interlocutori coinvolti;
- l'insieme dei rischi da considerare;
- la pianificazione delle attività;
- il delivery della fornitura.

Inoltre, saranno pianificati momenti e modalità ben precise di verifica per assicurare il rispetto del piano di rilasci.

Le attività di Project Management si svolgeranno trasversalmente a tutte le fasi del progetto, dall'avvio sino al suo completamento.

3.2 SECURITY ASSESSMENT - VULNERABILITY ASSESSMENT - PENETRATION TEST

I servizi di sicurezza del settore Auditing sono finalizzati a rilevare e valutare oggettivamente sul campo il grado di efficacia, efficienza e robustezza delle misure di sicurezza implementate dal Cliente sui propri asset, identificando le eventuali vulnerabilità o debolezze e fornendo al Cliente le indicazioni necessarie per eliminarle o ridurle. Il seguente schema della norma ISO IEC 15408-1 del 2005 chiarisce le relazioni tra i vari concetti di sicurezza.

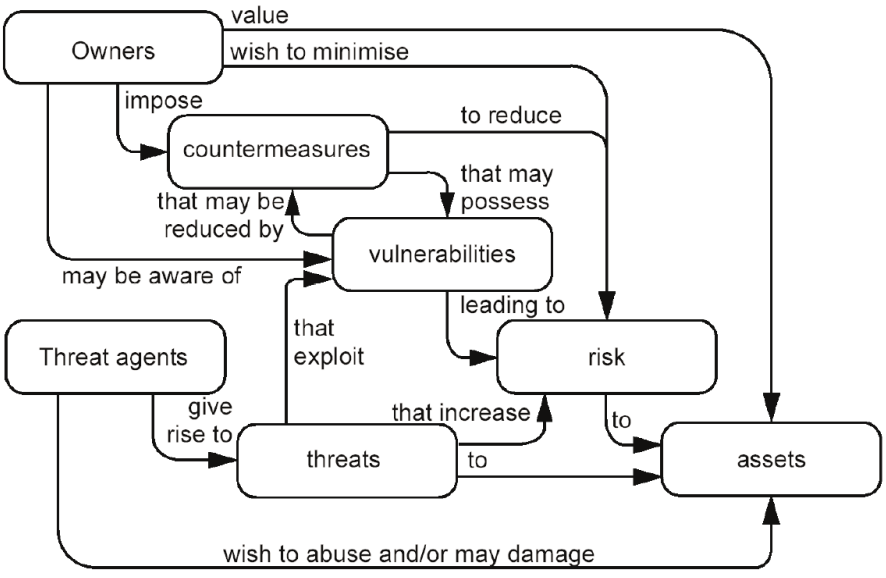

Figura 1 – Relazione tra concetti di sicurezza

In particolare, il servizio di IT Security Audit consiste in una verifica di sicurezza approfondita, mediante diverse tecniche di attacco (*threats*) rivolte alle infrastrutture tecnologiche del Cliente (assets).
Il Team di analisi simula gli agenti di minaccia (*threat agents*) tentando di identificare le vulnerabilità (*vulnerabilities*) e le relative contromisure (*countermeasures*) che portano il Cliente (*owners*) a ridurre il rischio (*risk*) sui propri beni/servizi (*assets*).

Il team di analisi si impegna a ridurre al minimo il rischio di poter causare danni o disservizi agli asset del Cliente seguendo scrupolosamente una prudente modalità di condotta delle attività di Security Auditing, al fine di garantire la continuità operativa dei sistemi, servizi e infrastrutture oggetto di test. In caso di dubbio il Cliente è sempre tempestivamente interpellato prima che siano eseguite operazioni potenzialmente pericolose al fine di richiedere l'autorizzazione per la prosecuzione o meno dell'attacco.
Engineering assicura che il team di analisi utilizza strumenti privi di virus o malware, inoltre garantisce di tenere aggiornati software anti-virus, anti-spyware e simili sugli apparati che collega alla rete del Cliente durante le attività.
Inoltre, Engineering garantisce di tenere costantemente aggiornati anche gli strumenti utilizzati per l'erogazione dei servizi al fine di sanare eventuali bug scoperti e usufruire delle nuove funzionalità implementate nelle versioni più recenti.
Il team di analisi è sempre disponibile a fornire spiegazioni al Cliente circa le motivazioni che lo portano ad eseguire le operazioni sui suoi asset e a descrivere in che modo sono utilizzati gli strumenti di test, garantendo quindi l'assoluta trasparenza delle operazioni.
Il team di analisi, in caso di scoperta di vulnerabilità gravi tali per cui esiste un immediato rischio per il Cliente, provvederà ad informare tempestivamente il referente fornendo tutti i dettagli tecnici del caso.
Engineering inoltre garantisce che tutte le informazioni e i materiali ricevuti dal Cliente sono custoditi, manipolati e trasmessi in modo sicuro (cifrati) al fine di prevenire fughe di informazioni, anche in seguito all'eventuale furto dei supporti tecnologici, prima, durante e dopo le attività svolte.
Engineering garantisce inoltre la riservatezza delle informazioni e si impegna a siglare un NDA con il Cliente per tutte le informazioni di cui dovesse venire in possesso durante l'esecuzione dell'attività.

Engineering eroga il servizio di Audit nel pieno rispetto delle norme etiche che contraddistinguono gli Ethical Hacker che compongono il gruppo, seguendo standard internazionali e avvalendosi delle più recenti e consolidate metodologie di analisi come ad esempio la metodologia OSSTMM, OWASP, NIST e PTES. Inoltre, il gruppo di lavoro è a conoscenza degli aspetti tecnici e legali inerenti al GDPR, al Codice della Privacy e successivi provvedimenti e può supportare il Cliente nella gestione di eventuali incidenti di sicurezza. Il Cyber Security Team di Engineering si impegna ad avvisare tempestivamente il Cliente nel caso dovesse venire a conoscenza, durante l'erogazione delle attività oggetto dell'offerta, di violazioni che possono avere impatti legali o sul business dell'Azienda.
Di seguito una breve descrizione delle principali metodologie applicate:

La metodologia OSSTMM regolamenta la pianificazione, l'esecuzione e la reportistica dei test.

OWASP è la più collaudata metodologia per la verifica di siti/applicazioni web.

NIST National Institute of Standards and Technology U.S. Department of Commerce	***Il documento SP800-115 rilasciato dal NIST rappresenta una guida di riferimento per gli aspetti tecnici di base sulla conduzione di security assessment.***
PENETRATION TESTING EXECUTION STANDARD PTES Technical Guidelines	***Le linee guida del Penetration Testing Execution Standard coprono tutte le fasi dell'attività di Penetration Test, dove l'esperienza tecnica di sicurezza dei tester si combina con la comprensione del business in modo da fornire il massimo valore per il Cliente.***
OWASP Mobile Security Project	***Il progetto OWASP Mobile Security Project è una risorsa centralizzata destinata a fornire agli sviluppatori e ai team di sicurezza le risorse di cui hanno bisogno per costruire e mantenere sicure le applicazioni mobili.***
OWASP INTERNET OF THINGS	***Il progetto OWASP IOT è stato concepito per aiutare i produttori, gli sviluppatori e i consumatori a comprendere meglio i problemi di sicurezza associati IOT.***

Tabella 1 - Metodologie applicate

La classificazione del livello di rischio viene calcolato in base ad un indice di criticità della vulnerabilità. Tale calcolo viene effettuato considerando alcuni parametri oggettivi ed utilizzando metriche ben definite. Il risultato finale che si ottiene dall'aggregazione di questi valori esprime l'indice reale di rischio della vulnerabilità.

CVSS	***Un noto standard di scoring delle vulnerabilità composto da tre fattori: punteggio base, punteggio in relazione al tempo e quello basato sul contesto in cui le vulnerabilità sono rilevate.***

La metrica RAV si basa sul calcolo bilanciato di Porosity (il grado di esposizione che è necessario mantenere per offrire servizi interattivi), Controls (contromisure che innalzano il livello di sicurezza fornendo protezione da interazioni non valide o inaspettate) e Limitations (criticità di sicurezza). Secondo la metodologia OSSTMM è possibile raggiungere lo stato di Perfect Security, ovvero l'esatto bilanciamento di separazione e controlli con l'esposizione e le criticità (valore di rav pari a 100).

Un noto standard di classificazione delle vulnerabilità che permette di identificarle facilmente in un contesto internazionale. La documentazione prodotta da Engineering, per quanto possibile, riporta per ogni vulnerabilità l'identificativo CVE.

CCWAPSS

Uno standard emergente per ottenere una panoramica dello stato di sicurezza di un sito web secondo 11 criteri base derivati dalla metodologia OWASP.

Di seguito sono indicati gli step di analisi in uno scenario generico. Ove necessario, tali step possono variare per adattarsi a specifiche configurazioni riscontrate nell'infrastruttura di rete oggetto di test. Tale variazione è finalizzata a massimizzare l'efficacia del Security Assessment.

ID	DESCRIZIONE STEP ANALISI
1	Valutazione dell'esposizione su internet attraverso la consultazione di fonti pubbliche di informazione.
2	Analisi esterna del target mirata a mappare la rete mediante interrogazione DNS o servizi accessibili online e non direttamente ospitati presso il Cliente. L'obiettivo è comprovare la solidità del target e l'effettivo livello di tracciabilità in rete.
3	Ricostruzione e mapping della rete al fine di individuare i sistemi raggiungibili ed i servizi esposti.
4	Scansione mirata a censire tutti i sistemi oggetto del Penetration Test, individuando porte/servizi, protocolli supportati e versioni del software installato.
5	Individuazione di fonti e servizi utili per l'IP grabbing. Lo scopo è quello di ottenere informazioni della rete interna ed individuare i possibili anelli deboli non direttamente visibili dall'esterno.
6	Determinare il possibile sfruttamento di tecniche di IPID o TCP SEQ Prediction vagliando le probabilità di un attacco di spoofing/hijacking cieco.
7	Determinare la possibilità di accedere ai suddetti servizi mediante credenziali di

ID	DESCRIZIONE STEP ANALISI
	autenticazione standard o mediante attività di user enumeration e password guessing.
8	Scansioni automatiche e manuali al fine di censire le vulnerabilità esposte dall'infrastruttura ed individuare le problematiche che potrebbero essere sfruttare immediatamente da un ipotetico attaccante.
9	Analisi manuale ed exploting delle vulnerabilità individuare al fine di simulare attività intrusive ed attacchi portati al fine di perseguire obbiettivi specifici (ottenere l'accesso ai dati memorizzati in un database, impersonare altri utenti, compromettere un determinato sistema ecc.).
10	Identificazione dei servizi non hardenizzati e sfruttamento delle relative falle.
11	Individuazione di misconfigurazioni che possono ledere la sicurezza dei sistemi o delle applicazioni.
12	Verifica dello stato di aggiornamento dei sistemi.
13	Identificazione di carenze nella segregazione dei sistemi o delle reti.
14	Verifica della corretta profilazione delle utenze.
15	Determinare la possibilità di accedere a informazioni o risorse in maniera non autorizzata.
16	Valutazione e classificazione delle vulnerabilità individuate secondo le seguenti dimensioni: a) Difficoltà che un ipotetico attaccante deve fronteggiare per sfruttare con successo la vulnerabilità. b) Impatto che si avrebbe sul business aziendale qualora la vulnerabilità venisse effettivamente sfruttata
17	Identificazione di possibili falle di sicurezza dovute al comportamento umano.
18	Fornitura di report finalizzati alla definizione di un piano di intervento utile all'azienda per pianificare azioni medio-lungo termine al fine di innalzare e mantenere il livello globale di sicurezza dell'infrastruttura.
19	Aggiornamenti e supporto sui vari stati di avanzamento durante tutta la fase di analisi.

Tabella 2 -Descrizione step di analisi

Il servizio di Audit è approcciato nei nostri progetti in quattro fasi:

1. **Incontro preliminare con il Cliente** per la determinazione degli asset (target) e delle modalità operative
2. **Firma della liberatoria** da parte del Cliente;
3. **Esecuzione del VA**
4. **Redazione dei risultati tramite un *Test Report***

Durante l'incontro preliminare il GdL collabora con il Cliente per ottenere tutte le informazioni necessarie alla pianificazione dell'attività e concordare le modalità operative.

In particolare, l'incontro verte su:

- identificazione delle modalità operative e determinazione degli scenari di verifica;
- reperimento della documentazione esistente relativa a politiche di sicurezza, specifiche di progetto, ecc. (opzionale);
- accordo logistico per l'esecuzione del VA e in particolare identificazione dei referenti che seguiranno l'attività;

Dopo aver definito il perimetro di analisi, il periodo dell'attività e l'attestazione della sorgente dell'attacco, verrà inviato al Cliente il documento di liberatoria che dovrà essere firmato dal legale rappresentante della Società richiedente il servizio per autorizzare il GdL allo svolgimento dell'attività. **La firma della liberatoria è mandatoria per l'inizio dell'attività**. Solo dopo aver ricevuto il documento firmato si potrà procedere alla fase successiva.

Dopo la convalida del *Test Plan* da parte del Cliente, il GdL inizierà l'esecuzione materiale del test. Durante la verifica, il GdL svolge le seguenti attività:

- tiene traccia di tutte le azioni eseguite sugli asset del Cliente per fornire l'evidenza di quanto è stato fatto;
- concorda di volta in volta con il referente, nel caso la situazione lo richieda, il consenso esplicito per l'esecuzione di azioni il cui risultato potrebbe essere incerto o influire sull'attività del Cliente;

è disponibile alla collaborazione diretta e continuativa con il referente (in caso di scenari "Crystal Box") per quanto riguarda la scelta della logica di attacco o eventuali accorgimenti da seguire durante la verifica di asset particolari. Eventuali richieste di modifiche sostanziali al *Test Plan* da parte del Cliente che includono ad esempio ulteriori asset o modificano profondamente le condizioni del test dovranno essere programmate in sessioni di aggiuntive i cui dettagli dovranno essere concordati.

Al termine dell'Audit, il GdL provvede alla redazione del *Test Report,* che potrà essere composto da uno o più documenti e allegati che esplicano in modo chiaro ed esaustivo i risultati delle attività.

La fase sarà erogata in modalità a corpo con un massimo di giornate pari a 80.

Il **Vulnerability Assessment** effettua una fotografia della infrastruttura e verifica eventuali falle nella sua configurazione, ciò consente una valutazione della situazione dei sistemi di sicurezza implementati su reti, macchine o applicazioni aziendali, con l'obiettivo di rilevare eventuali carenze di protezione rispetto ad elenchi di vulnerabilità tecnologiche note.
Gli Assessment vengono condotti tramite l'utilizzo dei migliori tool di scansione attualmente sul mercato, che forniscono una profondità di rilevazione ed una granularità di scansione completamente configurabili, in base alle esigenze del sistema informatico oggetto di analisi.
I principali obiettivi di un Vulnerability Assessment sono quelli di:

- Ridurre i rischi di compromissione dell'infrastruttura
- Identificare i server attivi sulla rete e i relativi servizi esposti
- Individuare velocemente le superfici d'attacco più critiche
- Scoprire eventuali misconfigurazioni di sicurezza
- Controllare lo stato di aggiornamento del software
- Verificare l'hardening dei sistemi
- Segnalare l'uso di credenziali di default
- Mantenere uno storico sullo stato dell'arte della propria infrastruttura

L'attività può essere svolta nelle seguenti modalità:

- **Autenticata**: Vengono fornite le credenziali per eseguire anche dei check interni al sistema (hardening, corretta implementazione delle policy di sicurezza, stato dell'aggiornamento dei programmi installati, etc.).
- **Non autenticata**: Non vengono fornite credenziali d'accesso al sistema e viene eseguita una scansione esterna sui servizi esposti.

Le fasi che comprendono il servizio di Vulnerability Assessment sono mostrate in figura:

Figura 2 - Fasi operative del Vulnerability Assessment

Operativamente, l'attività viene svolta con l'ausilio di tool automatizzati e comporta:

- la scansione su tutte le 65535 porte TCP e UDP per ogni host attivo sulla rete
- l'utilizzo di vulnerability scanner configurati nel modo seguente:
  - elenco dei soli host nel perimetro d'analisi
  - inserimento dei soli servizi che risultano attivi dalle due scansioni precedenti
  - disabilitazione dei moduli potenzialmente dannosi (p. es. attacchi DDoS)

Parametri: massimo 500 ip interni

Il **Penetration Test** è un'indagine sperimentale sulla sicurezza di un computer o di una rete, volta a individuare vulnerabilità che potrebbero essere sfruttate in caso di tentativo di accesso non autorizzato e volta a testare i controlli che dovrebbero proteggere i computer e le reti da tali tentativi.
Il test è articolato sostanzialmente in due fasi:

- l'esplorazione dei presidi di sicurezza del sistema oggetto di verifica;
- tentativo di violare quei presidi e di penetrare il sistema stesso (c.d. attacco).

Al termine dell'investigazione viene presentato un rapporto sulle vulnerabilità individuate e sulle contromisure consigliate per rendere il sistema e la rete più sicuri. Il Penetration Test è pertanto un'attività volta ad ottenere informazioni, privilegi o a simulare il danneggiamento di sistemi informatici.
L'attività è svolta utilizzando tecniche generalmente più sofisticate di quelle comunemente in uso all'utente medio, con l'obiettivo di contribuire al miglioramento del livello di sicurezza dei sistemi esaminati.
Lo scopo principale è quello di fare emergere le falle del network o dei sistemi informatici oggetto del test, con particolare riguardo alla confidenzialità, all'integrità ed alla sicurezza dei dati e delle informazioni che vi risiedono.
Alcune delle possibili mancanze di sicurezza, nell'accesso ai sistemi informativi e alle reti del committente, possono riguardare:

- La rete Internet e gli altri punti di accesso elettronico, partendo da tecnologie implementate quali Firewall, Virtual Private Networks, Web Application Server, Web Application, ecc.;
- I modelli procedurali, inclusa l'interazione umana (Social Engineering, Physical Intrusion, ecc.);

I tipi di Penetration test erogati dal GdL sono normalmente classificati in:

1) **PT esterni** (internet/vpn/dialup): sono eseguiti presso la sede del Cliente o da remoto verso servizi erogati dalle infrastrutture del Cliente accessibili ai suoi partner o al pubblico;
2) **PT interni** (intranet): sono eseguiti quasi esclusivamente presso la sede del Cliente verso le infrastrutture e i servizi interni del Cliente;
3) **PT misti** (internet/intranet/extranet/vpn/dialup): sono eseguiti a seconda delle necessità presso il Cliente o da remoto; sono rivolti a servizi interni e/o esterni e coinvolgono potenzialmente anche asset di clienti o fornitori del Cliente.

I principali obiettivi di un Penetration Test sono quelli di:

- Andare in profondità
- Sfruttare le vulnerabilità (o misconfigurazioni) trovate
- Identificare i reali rischi a cui si è esposti
- Rilevare possibili vie d'accesso non autorizzate
- Abusare di funzionalità predisposte per scopi diversi
- Valutare la corretta segregazione dell'infrastruttura
- Verifica password policy
- Eliminare i falsi positivi derivati dall'attività di Vulnerability Assessment
- Verificare la corrispondenza ai domini di sicurezza delineati dalle best practice/standard di sicurezza adottati dalla Società Cliente (es. ISO 27001).

Parametri: Massimo 10 IP perimetro esterno, black box

3.3 TEMPI E PIANIFICAZIONE

In fase di kick-off ed avvio del progetto verrà concordato un piano operativo e verrà definita l'agenda dei colloqui in termini di referenti da coinvolgere, durata degli stessi e modalità; si prevede che l'attività verrà svolta principalmente da remoto. A seguito dell'acquisizione di tutte le informazioni, verrà effettuata l'analisi e la produzione dei deliverables, che verranno condivisi con il Cliente e presentati alla Direzione a conclusione dei lavori.

4 ORGANIZZAZIONE DEI SERVIZI OGGETTO DI FORNITURA

4.1 RESPONSABILI DELLA GESTIONE DELLA FORNITURA

Entro la data di attivazione della Fornitura, ciascuna delle parti nominerà con lettera a sé stante un proprio Responsabile che dovrà mantenere i collegamenti con l'altra parte in merito alla gestione della Fornitura. Il Cliente, inoltre, comunicherà per iscritto al Responsabile della Fornitura l'elenco nominativo dei Referenti Applicativi di Processo che interfacceranno il Customer Care Service nello svolgimento della Fornitura, completo di numeri telefonici, fax, indirizzo e-mail.

Il Responsabile della Gestione della Fornitura del Cliente è il rappresentante ufficiale del Cliente nella gestione della Fornitura ed ha i seguenti compiti:

- controlla la qualità del servizio ed il grado di soddisfazione degli utenti;
- gestisce, in collaborazione con il Responsabile della Gestione della Fornitura di Engineering, la verifica periodica dell'andamento qualitativo del contratto.

4.2 OBBLIGHI E RESPONSABILITÀ DEL FORNITORE

Il Fornitore s'impegna a:

- operare con diligenza nello svolgimento di tutte le attività connesse alla Fornitura, mettendo a disposizione personale qualificato all'esecuzione autonoma degli interventi di sua competenza, nel rispetto delle procedure specificate nel presente contratto;
- operare nel rispetto delle norme particolari di sicurezza e/o riservatezza concordate con il Cliente;
- garantire il rispetto di dette norme di sicurezza e/o riservatezza da parte di terze parti coinvolte nell'espletamento della Fornitura;
- garantire la corretta esecuzione di quanto previsto nel presente contratto, ritenendosi in ogni caso sollevato da ogni responsabilità per eventuali ritardi dovuti a cause di forza maggiore;
- farsi carico di tutti gli oneri sociali ed assicurativi per il personale impiegato nello svolgimento della Fornitura, con particolare riguardo all'assicurazione contro gli infortuni sul lavoro.

4.3 OBBLIGHI E RESPONSABILITÀ DEL CLIENTE

Il Cliente s'impegna a:

- rendere disponibili tutte le informazioni necessarie per il corretto svolgimento della Fornitura;
- consentire l'accesso alle proprie sedi da parte delle persone del Fornitore preposte all'erogazione della Fornitura, come pure ai sistemi sui quali sono installati i programmi assistiti, fornendo loro le necessarie credenziali di accesso;
- garantire al personale del Fornitore l'accesso alla documentazione di servizio, sia in lettura sia in aggiornamento, anche con accesso remoto;
- garantire il trattamento dei dati secondo quanto previsto dallo specifico accordo per il trattamento dei dati allegato al presente;

Il Cliente deve inoltre assicurare, a proprio carico:

- la predisposizione di adeguati strumenti per l'accesso remoto per lo svolgimento di tutte le fasi progettuali.

4.4 RUOLI DEL CLIENTE

Con riferimento alla gestione della Fornitura, i ruoli d'interfaccia con il Fornitore saranno i seguenti:

Service Manager

È il rappresentante ufficiale del Cliente nella gestione della Fornitura ed ha i seguenti compiti:

- controlla la qualità del servizio ed il grado di soddisfazione degli utenti
- gestisce, in collaborazione con il Responsabile CCS del Fornitore, la verifica periodica dell'andamento qualitativo del contratto

Referenti di Processo

Sono le figure responsabili, lato Cliente, del controllo della qualità complessiva della Fornitura, relativamente al processo di competenza.

In particolare queste figure hanno i seguenti compiti:

- controllano la qualità del servizio relativamente al processo di competenza
- forniscono il necessario supporto informativo ai consulenti del Fornitore
- eseguono e/o controllano l'esecuzione delle fasi progettuali.

4.5 CONFORMITÀ ALLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DAI PERSONALI

Per l'erogazione del servizio/fornitura, il Fornitore tratterà dati personali per conto del Titolare.
A tale scopo sarà necessario formalizzare apposito accordo per il trattamento dei dati, ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati (Rif. Reg. EU 2016/679).
Il Fornitore si impegna a fornire e mantenere aggiornato, ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al Provvedimento del 25 giugno 2009 ss.mm.ii. l'elenco dei soggetti autorizzati al trattamento ai sensi dell'art 29 del GDPR con funzioni di Amministratore di Sistema, se presenti, al fine di permettere al Titolare d riportare tali informazioni in un documento interno e renderlo disponibile in caso di accertamenti da parte delle Autorità.

4.6 LUOGO DI ESECUZIONE DELLA FORNITURA

Tutti i servizi previsti dalla presente Fornitura saranno erogati in modalità remota dalle sedi/ strutture del Service Provider Engineering Ingegneria Informatica S.p.A.

5 PREZZO

L'importo originario per la fornitura oggetto della presente offerta è pari ad **€ 65.000,00 + IVA**.
Alla luce però del rapporto di partnership intercorrente con la Vostra Amministrazione e considerata la tematica di particolare attualità e delicatezza, Engineering ha deciso di accordare un significativo sconto di **€ 17.500,00**, fissando in questo modo il prezzo finale in **€ 48.500,00** (*quarantottomilacinquecento/00*) esclusa IVA.
Tutti i prezzi indicati sono da intendersi IVA esclusa.

Oggetto di fornitura	Tipologia di Servizio/Quantità	Importo Totale IVA esclusa	Importo Totale Scontato IVA esclusa
Service Management	A corpo	~~**€ 7.000,00**~~	**€ 6.000,00**
Security Assessment	A corpo	~~**€ 38.000,00**~~	**€ 33.000,00**
Vulnerability Assessment	Fino a 500 IP Interni	~~**€ 12.000,00**~~	**€ 6.000,00**
Penetration Test	Max 10 IP perimetro esterno, black box	~~**€ 8.000,00**~~	**€ 3.500,00**
Totale		~~**€ 65.000,00**~~	**€ 48.500,00**

GERMOLE' ANTONINO
ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI ROMA
INGEGNERE
29.11.2021 08:44:05 UTC

6 MODALITÀ DI FATTURAZIONE

I servizi descritti saranno fatturati secondo il Piano di Fatturazione descritto nel seguito:

- Service Management: in base allo stato avanzamento lavori;
- Security Assessment: in base allo stato avanzamento lavori;
- Vulnerability Assessment: in base allo stato avanzamento lavori;
- Penetration Test: in base allo stato avanzamento lavori.

7 MODALITÀ DI PAGAMENTO

Tutti i corrispettivi verranno regolati tramite rimessa diretta a 60 (sessanta) giorni data fattura, facendo riferimento al D.L. del 9 novembre 2012 n.192 modifiche al D.L. del 09 ottobre 2002 n. 231; mediante bonifico bancario con valuta fissa al beneficiario sul conto corrente bancario indicato dal Fornitore, fatto salvo quanto stabilito dall'Accordo Pagamenti promosso dalla Regione Lazio (Decreto n. U00351 del 27 novembre 2012).

Il ritardo nei pagamenti da parte del Cliente comporterà a suo carico l'obbligo di pagare gli interessi moratori.

Il Cliente non potrà far valere alcuna azione o eccezione nei confronti di Engineering Ingegneria Informatica S.p.A. se non dopo il pagamento delle fatture scadute.

8 ORDINE DI PREVALENZA

In caso di conflitto tra le disposizioni contenute nei diversi documenti che costituiscono la proposta al Cliente, si osserverà il seguente ordine di prevalenza:

1. Condizioni Generali di Vendita;
2. Proposta Tecnico-Economica;
3. Lettera di accompagnamento.

Roma, 30/09/2021

Engineering Ingegneria Informatica S.p.A.

Il Procuratore Speciale

Antonio Delli Gatti