CAPITOLATO TECNICO

PERCORSI FORMATIVI E CERTIFICATIVI SANS INSTITUTE

INDICE

1 DEFINIZIONI

Nel corpo del documento, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- CONSIP: la società che, in qualità di stazione appaltante, affida il servizio oggetto del presente Capitolato;
- SOGEI: la Società Generale di Informatica S.p.A. Committente e Beneficiaria;
- Capitolato tecnico: il presente documento che enuncia le specifiche tecniche alle quali dovrà conformarsi il servizio;
- Contratto: il contratto che verrà stipulato tra la SOGEI e l'impresa che enuncia le regole giuridiche alle quali si dovrà conformare il servizio;
- Servizio: il complesso delle attività oggetto del presente Capitolato;
- Società: la società aggiudicataria della fornitura;
- Responsabile delle attività contrattuali o Responsabile SANS: la persona individuata dalla Società come interlocutore di Sogei e responsabile di tutte le attività contrattuali.

2 PREMESSA

Nell'ambito delle proprie attività istituzionali, Sogei ha, tra gli altri, il compito di fornire servizi informatici qualificati alle Pubbliche Amministrazioni italiane.

In relazione al proprio ruolo di centro nodale della informatica pubblica italiana, pertanto, Sogei ha l'esigenza di garantire il più altro livello di consapevolezza e conoscenza riguardo ai rischi di attacchi informatici (cybersecurity) che possono, potenzialmente, provocare danni economici e di immagine ai clienti serviti.

Per tali motivi Sogei deve quindi curare e aggiornare periodicamente la formazione del personale in merito a metodi e tecniche di protezione / intrusione / pentesting a livello di sistemi, reti, applicazioni web e servizi cloud, investendo in formazione di qualità su personale specializzato in modo da

disporre aziendalmente delle conoscenze di cybersecurity necessarie ad affrontare nuovi scenari di servizio e di rischio.

È stata pertanto condotta una indagine di mercato, mirata a identificare un operatore ad altissima qualificazione, riconosciuto internazionalmente, in grado di soddisfare pienamente le esigenze formative sopra descritte, sintetizzabili nella definizione di:

• Percorsi formativi “Security”, vale a dire con focus specifico sulle attività proattive e le nuove frontiere di Cyber & Cloud Security;

• Percorsi formativi “Forensics”, con focus sulle attività reattive, analisi evidenze e gestione avanzata degli incidenti informatici

I due percorsi descritti devono, per Sogei, essere organizzati in set di corsi che consentano di sviluppare una formazione altamente specializzata, interamente orientata alla sicurezza informatica sia dal lato tecnico che da quello manageriale e di pianificazione strategica.

A questo si aggiunge per Sogei la necessità di ottenere strumenti didattici agili, erogati in presenza e/o da remoto.

In dettaglio, l’esigenza di Sogei è quella di ottenere programmi di formazione:

• su tutti gli ambiti necessari per Sogei (web application pentesting, cloud pentesting, cloud devsecops, digital forensics, data science & machine learning for cybersecurity) organizzati in un percorso formativo integrato;

• che siano basati su sessioni hands-on in cui si trattano casi ed evidenze digitali provenienti da casi reali, con docenti di alto livello, esperti del settore provenienti da aziende e enti specializzati;

• acquisire documentazione originale tecnicamente approfondita;

• che possa consentire il conseguimento di una certificazione internazionalmente riconosciuta della formazione ricevuta, in modo da qualificare pienamente le persone di Sogei alle quali sono affidate attività legate alla cybersecurity.

L’analisi di mercato condotta, pertanto, ha identificato il SANS Institute come l’unico fornitore in grado di soddisfare pienamente tutte le esigenze sopra esposte.

Questo istituto di formazione internazionale mette a disposizione una serie di corsi che rispondono pienamente alle esigenze di Sogei.

I corsi erogati da SANS Institute consentono di conseguire la certificazione Global Information Assurance (GIAC).

Questo ente di certificazione, unico nel suo genere, fondato nel 1999 per accreditare la formazione avanzata nella sicurezza informatica, è una garanzia di competenza e professionalità a livello globale.

Infatti, attualmente, le certificazioni di sicurezza “GIAC Security” sono ampiamente riconosciute come la qualifica di più alto livello nel settore della Cyber Security, in quanto prevedono quasi esclusivamente sessioni *hands-on* su casi reali ed evidenze digitali provenienti da incidenti reali, con docenti di alto livello, esperti del settore provenienti da aziende e enti specializzati.

Inoltre le certificazioni di sicurezza “GIAC Security” sono ampiamente riconosciute come la qualifica di più alto livello a livello tecnico nel settore della Cyber Security, in quanto a differenza delle altre certificazioni analogamente riconosciute a livello internazionale (CEH, CISM, CISSP. CISA, CompTIA Security) che hanno carattere più generale e gestionale, le certificazioni GIAC sono le uniche a riguardare più di 40 ambiti tecnici specialistici e sono pertanto le uniche a misurare competenze e aree tecniche di conoscenza specifiche di cybersecurity piuttosto che conoscenze generali di infosec. Il personale di Sogei per cui si richiede l’acquisizione di questi percorsi formativi è infatti impegnato nell’erogazione dei servizi più critici di cybersecurity (CERT, SOC, Red Team) che proteggono dati e servizi del MEF e della PA centrale; alcuni di questi professionisti possiedono già altre certificazioni GIAC, ormai di prossima scadenza, che potranno essere mantenute solo mediante la fruizione dei corsi indicati, in assenza dei quali si perderanno gli investimenti formativi già sostenuti dall’azienda.

Tali metodologia e modalità di preparazione e di certificazione mediante esame finale, insieme al fatto che le sessioni formative e la documentazione fornita sono estremamente approfondite, rappresentano delle unicità non riscontrabili

negli altri corsi presenti sul mercato; in particolare ad oggi non ve ne sono che offrano la stessa ampiezza di offerta come nell'elenco delle esigenze espresse, né tantomeno un modello equivalente di approfondimento pratico.

L'indagine di mercato ha riscontrato che ad oggi fra i corsi di formazione specialistica in ambito cybersecurity, i corsi erogati dal SANS Institute risultano gli unici a soddisfare pienamente le esigenze precedentemente rappresentate.

Stante quanto sopra rappresentato, si evidenzia quindi che l'acquisizione di corsi SANS è infungibile per la Scrivente, in quanto non esistono possibili sostituti dello stesso nel periodo di interesse, non esistendo soluzioni alternative ragionevoli alle esigenze di formazione specialistica oggetto dell'iniziativa. Sogei si impegna a continuare un monitoraggio costante di quanto disponibile sul mercato ed è pronta a valutare tempestivamente tutte le offerte formative alternative che si dovessero rendere disponibili. La durata dell'acquisizione è stata stabilita in relazione all'esigenza sopra descritta, all'indagine di mercato effettuata e all'impegno assunto.

3 OGGETTO

Il presente Capitolato disciplina l'acquisizione di partecipazioni ai corsi e alle certificazioni SANS Institute come di seguito specificate:

Descrizione	**Quantità**
FOR500: Windows Forensic Analysis + certificazione GCFE	1
SEC540: Cloud Security and DevSecOps Automation + certificazione GCSA	4
SEC588: Cloud Penetration Testing Course + certificazione GCPN	2
FOR578: Cyber Threat Intelligence + certificazione GCTI	2
SEC275: Foundations: Computers, Technology, & Security + certificazione GFACT	2

SEC504: Hacker Tools, Techniques, and Incident Handling + certificazione GCIH	3
SEC595: Applied Data Science and Machine Learning for Cybersecurity Professionals	2
SEC522: Application Security: Securing Web Apps, APIs, and Microservices + certificazione GWEB	2

3.1 CARATTERISTICHE DEL SERVIZIO

Indicare:

- I contenuti dei corsi richiesti e dell'esame di certificazione.

FOR500: Windows Forensic Analysis + certificazione GCFE. Il corso consta di 6 moduli che affrontano i seguenti argomenti:

1. Digital Forensics and Advanced Data Triage
2. Registry Analysis, Application Execution, and Cloud Storage
3. Shell Items and Removable-Device Profiling
4. Email Analysis, Windows Timeline, SRUM, and Event Logs
5. Web Browser Forensics
6. Windows Forensic Challenge

Il corso prepara al superamento dell'esame di certificazione GCFE (Certified Forensic Examiner) che, fra le altre cose, verifica le seguenti competenze e conoscenze:

1. Windows Forensics and Data Triage
2. Windows Registry Forensics, USB Devices, Shell Items, Email Forensics and Log Analysis
3. Advanced Web Browser Forensics (Chrome, Edge, Firefox, Internet Explorer)

SEC540: Cloud Security and DevSecOps Automation + certificazione GCSA. Il corso consta di 5 moduli che affrontano i seguenti argomenti:

1. DevOps Security Automation
2. Cloud Infrastructure Security
3. Cloud Security Operations
4. Cloud Security as a Service
5. Compliance as Code

Il corso prepara al superamento dell'esame di certificazione GCSA (Cloud Security Automation) che, fra le altre cose, verifica le seguenti competenze e conoscenze:

1. Using cloud services with DevSecOps principles, practices, and tools to build and deliver secure infrastructure and software
2. Automating Configuration Management, Continuous Integration, Continuous Delivery, and Continuous Monitoring
3. Use of open-source tools, the Amazon Web Services toolchain, and Azure services

SEC588: Cloud Penetration Testing Course + certificazione GCPN. Il corso consta di 6 moduli che affrontano i seguenti argomenti:

1. Discovery, Recon, and Architecture at Scale
2. Discovery, Authentication, and Cloud Services
3. Windows in the Cloud with Azure
4. Vulnerabilities and Exploitation of Cloud Native Applications
5. Red Team in the Cloud
6. Capstone (esercizio conclusivo di applicazione delle metodologie trattate)

Il corso prepara al superamento dell'esame di certificazione GCPN (Cloud Penetration Tester) che, fra le altre cose, verifica le seguenti competenze e conoscenze:

1. Cloud Penetration Testing Fundamentals, Environment Mapping, and Service Discovery
2. AWS and Azure Cloud Services and Attacks
3. Cloud Native Applications with Containers and CI/CD Pipelines

FOR578: Cyber Threat Intelligence + certificazione GCTI. Il corso consta di 6 moduli che affrontano i seguenti argomenti:

1. Cyber Threat Intelligence and Requirements
2. The Fundamental Skill Set: Intrusion Analysis
3. Collection Sources
4. Analysis and Production of Intelligence
5. Dissemination and Attribution
6. Capstone (esercizio conclusivo di applicazione delle metodologie trattate)

Il corso prepara al superamento dell'esame di certificazione GCTI (Cyber Threat Intelligence) che, fra le altre cose, verifica le seguenti competenze e conoscenze:

1. Strategic, operational, and tactical cyber threat intelligence application & fundamentals
2. Open source intelligence and campaigns
3. Intelligence applications and intrusion analysis
4. Analysis of intelligence, attribution, collecting and storing data sets
5. Kill chain, diamond model, and courses of action matrix
6. Malware as a collection source, pivoting, and sharing intelligence

SEC275: Foundations: Computers, Technology, & Security + certificazione GFACT. Il corso consta di 4 moduli che affrontano i seguenti argomenti:

1. System Architecture, Operating System and Linux
2. Search, Web and Networking
3. Introduction su Servers and Programming
4. Security Concepts and Advanced Security Concepts

Il corso prepara al superamento dell'esame di certificazione GFACT (Foundational Cybersecurity Technologies) che, fra le altre cose, verifica le seguenti competenze e conoscenze:

1. Core Computing Components: Hardware and Virtualization, Networking, Operating Systems, Web, Cloud, and Data Storage
2. IT Fundamentals and Concepts: Logic and Programming, Windows, and Linux
3. Security Foundations and Threat Landscape: Concepts, Exploitation and Mitigation, Forensics and Post Exploitation

SEC504: Hacker Tools, Techniques, and Incident Handling + certificazione GCIH. Il corso consta di 6 moduli che affrontano I seguenti argomenti:

1. Incident Handling Step-by-Step and Computer Crime Investigation
2. Computer and Network Hacker Exploits – Part 1
3. Computer and Network Hacker Exploits – Part 2
4. Computer and Network Hacker Exploits – Part 3
5. Computer and Network Hacker Exploits – Part 4
6. Hacker Tools Workshop

Il corso prepara al superamento dell'esame di certificazione GCIH (Certified Incident Handler) che, fra le altre cose, verifica le seguenti competenze e conoscenze:

1. Incident Handling and Computer Crime Investigation
2. Computer and Network Hacker Exploits
3. Hacker Tools (Nmap, Metasploit and Netcat)

SEC595: Applied Data Science and Machine Learning for Cybersecurity Professionals. Il corso consta di 6 moduli che affrontano I seguenti argomenti:

1. Data Acquisition, Cleaning, and Manipulation
2. Data Exploration and Statistic
3. Essentials of Machine Learning – Part I
4. Essentials of Machine Learning – Part II
5. Essentials of Machine Learning – Part III
6. Essentials of Machine Learning – Part IV

Al corso non corrisponde una certificazione GIAC alla data del contratto.

SEC522: Application Security: Securing Web Apps, APIs, and Microservices + certificazione GWEB. Il corso consta di 6 moduli che affrontano I seguenti argomenti:

1. Web Fundamentals and Security Configurations
2. Input-Related Defenses
3. Authentication and Authorization
4. Web Services and Front-End Security
5. APIs and Microservices
6. DevSecOps and Defending the Flag

Il corso prepara al superamento dell'esame di certificazione GWEB (Web Application Defender) che, fra le altre cose, verifica le seguenti competenze e conoscenze:

1. Access Control, AJAX Technologies and Security Strategies, Security Testing, and Authentication
2. Cross Origin Policy Attacks and Mitigation, CSRF, and Encryption and Protecting Sensitive Data
3. File Upload, Response Readiness, Proactive Defense, Input Related Flaws and Input Validation
4. Modern Application Framework Issues and Serialization, Session Security & Business Logic, Web
5. Application and HTTP Basics, Web Architecture, Configuration, and Security

3.2 MODALITÀ DI ISCRIZIONE AL CORSO E ALL'ESAME DI CERTIFICAZIONE

Sogei avrà cura di trasmettere al Responsabile SANS la lista dei discenti ed i rispettivi corsi ed esami di certificazione ai quali intendono iscriversi. Resta inteso che le condizioni di questo contratto si applicano e saranno valide soltanto per i soggetti individuati da Sogei e comunicati al Responsabile SANS.

Le iscrizioni ai corsi avvengono tramite il sito della Società web www.sans.org previa creazione di un account da parte del discente. Tramite il medesimo sito sarà possibile consultare il calendario dei corsi, siano essi in presenza o Live Online.

All'atto dell'iscrizione al corso il discente dovrà selezionare il cd. GIAC Bundle per iscriversi al tentativo di esame di certificazione associato al corso. In questo modo avrà a disposizione 120 giorni a partire dalla conclusione del corso per sostenere l'esame, che potrà essere svolto o presso un centro Pearson Vue oppure da remoto nella cd. modalità "proctored". Anche in questo caso il calendario degli esami sarà visionabile dal medesimo account con il quale il discente ha concluso l'iscrizione al corso.

Scaduti i 120 giorni di tempo previsti per sostenere l'esame di certificazione, il discente potrà eventualmente acquistare un'estensione dei termini tramite il sito ed ai prezzi pubblicati sul sito ww.giac.org. Resta inteso che tale estensione non è compresa nei servizi oggetto di questa fornitura, né potrà essere fatturata a Sogei in alcun modo.

3.3 LE MODALITÀ DI FRUIZIONE DEL CORSO E DETTAGLI CIRCA LO SVOLGIMENTO DEGLI ESAMI DI CERTIFICAZIONE

I prezzi concordati sono da intendersi per i corsi In Presenza o LiveOnline.

I corsi In presenza si frequentano presso una delle sedi elencate dalla Società nel calendario pubblicato sul sito www.sans.org. I corsi In Presenza iniziano di norma il lunedì e si concludono il sabato mattina. La Società si impegna a pubblicare il calendario dei corsi al fine di dare una vista non inferiore ai sei (6) mesi sulla pianificazione a calendario di ogni corso.

I corsi LiveOnLine si frequentano da remoto, in collegamento virtuale con una delle classi che si svolgono presso una delle sedi elencate dalla Società nel calendario pubblicato sul sito www.sans.org. Hanno medesima durata dei corsi In Presenza ed al discente è consentito di interagire con la classe e il docente tramite sistemi di videoconferenza e messaggistica virtuale.

L'esame di certificazione GIAC si sostiene in modalità virtuale, a prescindere che lo si svolga presso un centro Pearson Vue o da remoto. Consta di una serie di domande a risposta multipla alle quali rispondere entro un tempo massimo. Trattasi di esame "open book" ovvero al discente è consentito di poter consultare i libri durante lo svolgimento dell'esame. Per tutte le regole si rimanda al sito www.giac.org.

3.4 MATERIALE DIDATTICO

Nell'ambito del corso, la Società concede, senza alcun costo aggiuntivo, una licenza mondiale, perpetua, irrevocabile e non esclusiva direttamente a ogni singola persona il cui nome è indicato dalla Committente e/o Amministrazione come studente ("Utente") iscritto al corso, per utilizzare il materiale didattico preesistente della Società, compresi i materiali online, scritti e visivi (Courseware). I discenti non potranno copiare, riprodurre, distribuire, visualizzare, modificare o creare opere derivate basate su tutto o parte del Courseware in qualsiasi supporto, sia esso cartaceo, elettronico o di altro tipo, senza l'espresso consenso scritto della Società.

4 DURATA

Il contratto avrà efficacia dalla data della sua stipula, per 24 (ventiquattro) mesi e, comunque, sino al completo adempimento di tutte le obbligazioni contrattuali.

5 GESTIONE DELLA FORNITURA

5.1 RESPONSABILE DELLE ATTIVITÀ CONTRATTUALI

La Società dovrà comunicare a Consip, mediante compilazione del facsimile "*Scheda anagrafica e tracciabilità dei flussi*", contestualmente alla presentazione dell'offerta, il nominativo del Responsabile delle attività contrattuali, nonché un numero di telefono e un indirizzo e-mail al quale indirizzare eventuali comunicazioni. La Società deve provvedere in piena autonomia al coordinamento e all'organizzazione delle attività nel rispetto delle specifiche e dei tempi forniti da Sogei.

Sarà compito del Responsabile curare la gestione amministrativa del contratto e delle attività legate alla fatturazione e verificare il rispetto di tutti gli adempimenti contrattuali.

5.2 MODALITÀ DI COMUNICAZIONE

La Società si impegna a comunicare un numero di fax, un indirizzo e-mail, un indirizzo pec e un numero di telefono al quale rivolgersi, senza alcun limite sul numero di chiamate, per ogni comunicazione relativa al servizio.

Resta inteso che, per tutta la durata contrattuale, la Società dovrà garantire la piena funzionalità dei suddetti mezzi di comunicazione comunicando tempestivamente a Sogei eventuali modifiche.

Tutte le comunicazioni della Società devono essere inviate all'indirizzo mail formazione@sogei.it .

5.3 ADEMPIMENTI PER LA SICUREZZA

La Società s'impegna a porre in essere quanto necessario a garantire l'esecuzione delle attività in piena aderenza con le disposizioni del D. Lgs. 81/2008 "Testo Unico sulla sicurezza durante il lavoro" e con le ulteriori disposizioni di legge in materia di salute e sicurezza vigenti alla data di erogazione dei corsi, cooperando e coordinandosi, in particolare, con i referenti della Committente e degli uffici dell'Amministrazione Finanziaria presso cui dovranno essere svolte le attività contrattuali, ai fini degli adempimenti di cui al comma 2 dell'art. 26 del citato decreto.

Si evidenzia che le attività di cui al presente capitolato rientrano nelle fattispecie di cui al comma 3-bis del suddetto articolo, per le quali non sussiste l'obbligo di redigere il DUVRI (Documento Unico di Valutazione dei Rischi da Interferenze).

5.4 RISERVATEZZA

Tutte le informazioni trattate e tutti i documenti, anche parziali, scambiati tra la Società e Sogei sono riservati, pertanto è richiesta la massima attenzione per il loro utilizzo, in particolare se questo avviene al di fuori delle sedi Sogei.

La Società non potrà utilizzare, a nessun titolo, la documentazione ricevuta o prodotta, al di fuori delle attività oggetto del presente capitolato.

La Società non potrà utilizzare, a nessun titolo, la documentazione e i moduli software forniti da Sogei o realizzati per il servizio, al di fuori delle attività oggetto del presente capitolato.

5.5 VERIFICA DI CONFORMITÀ

La verifica di conformità verrà effettuata entro 5 giorni lavorativi dalla data di inizio del corso.

La verifica di conformità si intende positivamente superata solo nel caso in cui le prestazioni contrattuali siano state eseguite in conformità e nel rispetto di condizioni, modalità, termini e prescrizioni espresse nel presente Capitolato tecnico.

Il documento attestante la verifica di conformità dovrà essere allegato alle fatture al fine del pagamento dei corrispettivi alla Società.

6 MODALITÀ DI FATTURAZIONE E TERMINI DI PAGAMENTO

Ai fini del pagamento del corrispettivo indicato nel contratto, le parti concordano che il pagamento avverrà entro 30 giorni dalla data di ricezione della fattura.

Per procedere alla fatturazione sarà necessario che:

1. il discente abbia avuto accesso al servizio;
2. la fattura rechi gli elementi necessari richiesti da Sogei per la sua validità;
3. alla fattura venga allegato il verbale di conformità positiva, prodotto da Sogei e inviato al Responsabile SANS entro 5 (cinque) giorni lavorativi dalla data di inizio del corso;
4. la data della fattura che verrà inviata a Sogei sia successiva a quella riportata nel verbale di conformità positiva.

La fattura verrà inviata via mail agli indirizzi specificati da Sogei.

Il Responsabile SANS aggiornerà Sogei sul budget residuo, che dovrà essere utilizzato in un periodo massimo di 24 mesi dalla data di stipula del presente contratto.

7 PENALI

SOGEI applicherà le penali, secondo i seguenti casi:

- In caso di esito negativo della verifica di conformità, si applicherà una penale pari allo all'1‰ (uno per mille) dell'importo contrattuale complessivo, per ogni giorno lavorativo intercorrente tra la data del verbale negativo e quello positivo;

Nell'ipotesi in cui l'importo delle penali applicabili superi l'ammontare del 10% (diecipercento) dell'importo contrattuale complessivo, la Sogei avrà il diritto di risolvere, totalmente o parzialmente, il contratto in danno della Società, salvo il diritto dell'eventuale maggior danno.