



Consip S.p.A.

“Acquisizione di strumenti hw e sw per analisi forense dei dati di supporto del CERT MEF”

CAPITOLATO TECNICO

ACQUISIZIONE DI STRUMENTI HW E SW PER ANALISI FORENSE DEI DATI DI SUPPORTO DEL CERT MEF



INDICE

1	PREMESSA.....	3
1.1	Definizioni	3
1.2	Informazioni generali.....	3
1.3	Contesto tecnologico.....	4
2	OGGETTO DELLA FORNITURA	5
2.1	Dettaglio della fornitura	5
2.2	Consegna e durata	11
2.3	Servizio di manutenzione	11
2.4	Riservatezza	12
2.5	Prescrizioni in materia di Sicurezza	12
3	GESTIONE DELLA FORNITURA.....	13
3.1	Responsabile della Fornitura	13
3.2	Modalità di comunicazione	13
3.3	Verifica di conformità.....	13
3.4	Modalità di fatturazione.....	14
3.5	Livelli di servizio	14
4	PENALI	15



1 PREMESSA

1.1 DEFINIZIONI

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

- Capitolato tecnico: il presente documento che enuncia le specifiche tecniche alle quali si dovrà conformare la fornitura;
- CONSIP: la società che, in qualità di stazione appaltante della presente fornitura, affida la fornitura oggetto del presente Capitolato;
- Contratto: il contratto che verrà stipulato tra la SOGEI e la Società che enuncia le regole giuridiche alle quali si dovrà conformare la fornitura;
- Malfunzionamento: qualsiasi anomalia funzionale che, direttamente o indirettamente, provochi l'interruzione o la non completa disponibilità e funzionalità dei servizi o dei prodotti forniti e, inoltre, ogni difformità dalla relativa documentazione tecnica di funzionalità e utilizzo;
- Prodotto/Servizio: il complesso delle attività oggetto del presente Capitolato;
- SOGEI: la Società Generale di Informatica S.p.A., la Committente;
- DAG: Dipartimento dell'Amministrazione Generale, del Personale e dei Servizi, il beneficiario;
- Amministrazione: indica l'insieme delle strutture del Ministero dell'Economia e delle Finanze e della Corte dei Conti nonché le altre Amministrazioni, compresi gli Enti e le Società pubbliche per cui Sogei svolge e/o svolgerà attività di natura informatica;
- Società: la società aggiudicataria della fornitura;
- Responsabile della fornitura: la persona individuata dalla Società come interlocutore di Sogei e responsabile di tutte le attività contrattuali.

1.2 INFORMAZIONI GENERALI

Il CERT (Computer Emergency Response Team) istituito presso il Ministero dell'Economia e delle Finanze, per l'assolvimento dei propri compiti istituzionali, ha la necessità di disporre di adeguate attrezzature tecnologiche ad uso, in via prioritaria, del personale in servizio presso il Nucleo Tattico Operativo (NTO), struttura operativa di cui si avvale il CERT-MEF per l'esercizio delle sue funzioni.

In particolare, il Nucleo Tattico Operativo:

- fornisce supporto per l'accreditamento alle strutture istituzionali esterne di sicurezza cibernetica;
- gestisce i flussi informativi verso la SdG;



- esegue l'analisi delle minacce cibernetiche;
- si occupa della realizzazione d'iniziative per l'incremento della cultura della sicurezza informatica;
- cura i flussi informativi da e verso SOGEL;
- partecipa ad iniziative istituzionali in ambito sicurezza cibernetica.

1.3 CONTESTO TECNOLOGICO

I prodotti andranno inseriti nel contesto tecnico già predisposto presso il CERT MEF.



2 OGGETTO DELLA FORNITURA

2.1 DETTAGLIO DELLA FORNITURA

Di seguito l'elenco dei prodotti hardware e software, comprensivi del servizio di consegna, installazione e manutenzione on site per un periodo di 36 (trentasei) mesi:

HARDWARE			
ID	Prodotto	Quantità	Caratteristiche tecniche
1	IDS (Intrusion Detection System) Appliance	1 (copertura fino a 75 asset)	<ul style="list-style-type: none">• Network IDS• Host IDS• File Integrity Monitoring (FIM)• Reporting and Alarms• Cloud intrusion detection for public cloud environments including AWS, Microsoft Azure).• Check Assets and Vulnerabilities• Active Network Scanning• Passive Network Monitoring• Asset Inventory• Services Inventory• Vulnerability Assessment• Netflow Analysis• Service Availability Monitoring• Full Packet Inspection• Log Management• Event Correlation• Incident Response• Reporting and Alarms <p>Prodotto di riferimento: AlienVault Unified Security Management Appliance (max assets=75).</p>
2	Disco SSD interno da 2 TB di tipo PCIe NVMe M.2 2280	12	Da installare sui modelli Ultrabook Lenovo Thinkpad x280 già acquisiti dal MEF
3	Adattatore USB-C 4 in 1 (porta RJ 45 e 3 USB 3.0 da 5 Gbps)	12	
4	Adattatore USB 3.1 tipo C, da USB-C femmina a USB 3.0 maschio	12	
5	Notebook	2	<ul style="list-style-type: none">• Sistema Operativo Windows 10 64 bit• Processore Xeon E-2276 o i9-9880H o superiore• Tastiera retroilluminata



			<ul style="list-style-type: none">• Display UHD 4K 17.3" (in alternativa FHD)• 32GB RAM DDR4• SSD PCIe TLC OPAL2 da 512 GB• DVD-RW• Nvidia Quadro• Connettività Wireless 802.11a/b/g/n• Connettività Bluetooth• Connettività USB 3 Thunderbolt
6	Smartphone	7	<ul style="list-style-type: none">• Display a schermo intero da 6,3"• Processore di ultima generazione di tipo Pixel Neural Core di tipo Octacore Qualcomm SDM855 Snapdragon 855, con modulo di sicurezza Titan M⁵• GPU Adreno 640• Display OLED flessibile QHD+ a 537 ppi, rapporto 19:9, refresh rate 90hz, 1440 x 3040 pixel• Supporto HDR (certificazione UHDA)• Rapporto di super contrasto pari a 100.000:1• Profondità completa a 24 bit o 16,77 milioni di colori• Sistema Operativo Android 10 o superiore;• Aggiornamenti del sistema operativo e della sicurezza per almeno 3 anni garantiti Google• RAM 6 GB LPDDR4x;• Batteria 3700mAh, o superiore;• Ricarica wireless con certificazione Qi Ricarica rapida da 18 W³• Memoria interna di almeno 64 GB• Wi-Fi 2.4 GHz + 5 GHz 802.11 a/b/g/n/ac 2x2 MIMO• Bluetooth 5.0 + LE (codec HD: AptX, AptX HD, LDAC)• Certificazione di protezione da polvere e acqua IP68
7	Pendrive	12	<ul style="list-style-type: none">• Capienza 256GB o superiore• Interfaccia USB 3.0• Velocità di lettura fino a 420MB/s• Velocità di scrittura fino a 380MB/s• Impermeabile• Resistente agli urti• Resistente ai raggi X



8	Hdd Esterni	12	<ul style="list-style-type: none">• Formato 2,5”• Capacienza almeno 2TB SSD• Peso inferiore ai 50 grammi• Interfaccia USB 3.1• Alta resistenza agli urti ed alle vibrazioni• Crittografia AES a 256 bit integrata• Certificazioni CE, BSMI, KC, VCCI, C-tick, FCC, IC, UL, TUV, CB
9	Stampante Multifunzione di Rete a colonna	1	<ul style="list-style-type: none">• Stampante a getto d’inchiostro da inserire in ambiente non arieggiato, eliminando il problema delle polveri sottili nocive (impossibile predisporre eventuali cappe aspiranti nei locali adibiti)• Testina di stampa PrecisionCore™• 4,6 pl, con tecnologia Variable-sized Droplet• 800 ugelli per il nero, 800 ugelli per ciascun colore• Fax, CCITU/ITU Group3 con modalità di correzione errore• Stampa B/N e Colori fronte/retro• Gigabit Ethernet• Wireless LAN (IEEE 802.11a/b/g/n)• Velocità di stampa 24 pag/min• Velocità di stampa fronte/retro 16 pag/min• Protocolli di rete IPP, LPD, Port 9100, WSDProtocolli di gestione SNMP, HTTP, DHCP, BOOTP, APIPA, DDNS, mDNS, Sntp, SLP, WSD, LLTD, Ping• Interfacce USB 3.0 Type B, Interfaccia Ethernet (1000Base-T/100Base-TX/10Base-T), LAN IEEE 802.11a/b/g/n/ac (WiFi 5) wireless, Wi-Fi Direct, Host USB, Near Field Communication (NFC), USB 2.0 tipo A (2x)• Formato carta cassetti: A4, A5, A6, B5, C6 (busta), C4 (busta), N. 10 (busta), Letter, 10x15 cm, 13x18 cm, 20x25 cm, 16:09, Legal, A3, A3+• Protezione memoria interna tramite crittografia• Protezione utilizzo tramite codice PIN



10	Accessori per backup dati	50	DVD±R vergini (marchi noti)
		50	DVD±RW vergini (marchi noti)
		50	CD±R vergini (marchi noti)
		50	CD±RW vergini (marchi noti)
		20	pendrive USB 16 GB USB 3.1 (marchi noti)
		20	pendrive USB 16 GB USB 2.0 (marchi noti)
11	UltraDock	1	<ul style="list-style-type: none">• Compatibilità con sistemi• Windows Xp e superiori• Compatibilità con sistemi Mac OS X 10.6 e superiori• Compatibilità con le principali distribuzioni Linux• Drive supportati:<ul style="list-style-type: none">o PATA/IDE 2.5"o PATA/IDE 3.5"o SATA 2.5"o SATA 3.5"o MSATAo PCIe PATAo PCIe SATAo PCIe USB• Connettività:<ul style="list-style-type: none">o USB 3.0o eSatao Firewire 800
12	USB WriteBlocker	1	Usb 2.0 e/o 3.0
13	Forensic FieldStation, con espansioni USB e SAS	1	<ul style="list-style-type: none">• Interfaccia di collegamento USB 3.0 e Ethernet• Interfaccia di output Sata e/o eSata• Interfaccia Web capace di visualizzare/filtrare i file• Compatibilità S.O.:<ul style="list-style-type: none">- Windows, MacOSXLinux- iOS Tablet/smartphone- Android Tablet/smartphone• Write Blocker con interfacce in input:<ul style="list-style-type: none">o SATA, eSATA, PATA, USB 3.0• Funzionalità di acquisizione dati:<ul style="list-style-type: none">o Cloneo DDo E01o L01 con MD5 o SHA-1 Hashing• Funzione di cancellazione completa e sicura• Funzioni di clonazione• Impermeabile



14	valigetta che contenga tutto il materiale per l'analisi forense.	1	Prodotto di riferimento: Ditto Field Kit “D” o “K”
----	--	---	---

SOFTWARE			
ID	Prodotto	n. licenze	Caratteristiche tecniche
15	Manipolatore PDF	5	Prodotto di riferimento: Acrobat Pro DC
16	Tool backup centralizzato delle postazioni di lavoro	12 Workstation + 4 (LAB) 1 Server 1 host virtuale	<ul style="list-style-type: none">• Tecnologia di immagine del disco brevettata• Storage – dischi, NAS, SAN, Cloud Storage• Console web touch centralizzata e console di gestione remota• Active Protection• Backup application-aware• Deduplicazione archiviazione centralizzata su disco• Accesso amministrativo basato su ruoli• Report avanzati• Operazioni di gestione dei backup esterne all'host Prodotto di riferimento: Acronis Backup Advanced
17	Software per l'analisi sicura delle evidenze	1 licenza lifetime da 5 PC	Esecuzione del software in uno spazio di memoria isolato e controllato, in modo da prevenire infezioni e/o modifiche del sistema sul quale è eseguito. Prodotto di riferimento: Sandboxie - Home Use
18	Decompiler per analisi forense	1	Disassemblatore e debugger interattivo, programmabile, estendibile, multiprocessore (piattaforma) installabile sui principali sistemi operativi (Windows, Linux, MacOS). Prodotto di riferimento: IDA PRO 7.3 for MS Windows
19	Immagini Disco	3	<ul style="list-style-type: none">• Backup incrementali e differenziali• Backup in background• Backup di file e cartelle• Immagine completa del disco• Backup basato su eventi• Backup wireless



			<ul style="list-style-type: none">• Backup delle schede di memoria• Gestione remota dei backup• Crittografia end-to-end• abbonamento per 36 mesi <p>Compatibile con la famiglia di SW in questo documento</p> <p>Prodotto di riferimento: Acronis True Image 2020</p>
20	Data Recovery	1	<p>Recupero di qualità professionale per file persi e cancellati, cartelle, documenti, foto e altro ancora. Recuperare file persi a causa di diversi eventi come cancellazione accidentale e formattazione, compresi i casi di corruzione del disco rigido.</p> <p>Prodotto di riferimento: Ontrack EasyRecovery Professional for Windows</p>
21	Tool forense	1	<ul style="list-style-type: none">• Bootable (USB Flash Drive)• Boot di un'immagine come VM• OCR su file pdf• Ricerca di Criptocurrency, vpn, keyloggers• Ricerca di archivi email• Ricerca di file cancellati• Ricostruzione di password cancellate• Shadow copies di volumi• Verifica e match di file tramite hash• Verifica delle firme driver• Possibilità di creazione di una timeline• Analisi del registro di sistema• Analisi della thumb cache, dei dati prefetch e dei dati plist (macos).• Creazione di casi e di reportistica di fine analisi <p>Prodotto di riferimento: Passmark OSForensics V7</p>
22	Sanitizzazione	1	<p>Sanitizzazione delle memorie: Hard Disks, Solid State Drives, Memory Cards & USB disks, SCSI storage & RAID disk. Compatibile Windows e Linux, e con la possibilità di creare supporti bootabili. Creazione di report finali di sanitizzazione in PDF e XML.</p> <p>Prodotto di riferimento: Active KillDisk Ultimate</p>



23	Analisi dei malware	1 licenza	<p>Sandbox per l'analisi dei malware e la creazione di report dettagliati contenenti informazioni relative a campagne, analisi del codice, decompilazione del codice eseguito ed IOC.</p> <p>Possibilità di esecuzione sandbox Windows 7 x86 e x64, windows 10 x86 e x64, analizzatore di pacchetti android APK.</p> <p>Deve contenere strumenti per l'analisi dettagliata dei VBA, dei JS, dei JAR e deve avere l'integrazione con il software di disassemblamento IDA.</p> <p>Prodotto di riferimento: Joe Sandbox PRO: Ultimate</p>
----	---------------------	-----------	---

2.2 CONSEGNA E DURATA

La Società dovrà effettuare la consegna completa di tutti i prodotti oggetto di fornitura, **entro e non oltre 20 (venti) giorni solari** dalla data di stipula del contratto, presso il CERT MEF in via XX Settembre, n. 97 00187 Roma, rispettando l'orario di ricezione merci dalle 08,30 alle 16,30 dal lunedì al venerdì.

La data e le modalità di consegna dovranno comunque essere concordate, con adeguato anticipo, con i responsabili della SOGEI/Amministrazione

Unitamente alla fornitura vanno inclusi i seguenti servizi:

- Consegna e installazione;
- assistenza e manutenzione on site per 36 (trentasei) mesi.

Il contratto avrà una durata di 36 (trentasei) mesi a partire dalla data di positiva verifica di conformità della fornitura.

2.3 SERVIZIO DI MANUTENZIONE

La Società dovrà disporre di una struttura di assistenza tecnica, collocata sul territorio italiano, per erogare i servizi di manutenzione per tutta la durata e nei tempi previsti dal contratto, al fine di garantire la piena funzionalità di tutti i prodotti hardware e software oggetto di fornitura, nonché un intervento tempestivo e tracciabile per l'espletamento dei servizi nei tempi previsti.

La struttura di assistenza tecnica dovrà essere operativa nell'arco dell'anno solare, in orario di ufficio (giorni feriali: lun-ven 09.30 – 17.30).

A fronte di una segnalazione, infatti, la Società è tenuta a coordinare ed eventualmente, se richiesto dall'Amministrazione, ad effettuare un intervento di assistenza tecnica.



2.4 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.

2.5 PRESCRIZIONI IN MATERIA DI SICUREZZA

Tutte le apparecchiature fornite devono essere conformi alla normativa vigente che regola la loro produzione, commercializzazione ed utilizzazione; devono inoltre rispettare, ciascuna per le singole specifiche caratteristiche, le seguenti prescrizioni in materia di sicurezza:

- **Legge 1 marzo 1968, n. 186**, *“disposizioni concernenti la produzione di materiali, apparecchiature, installazioni e impianti elettrici ed elettronici”*;
- **Legge 18 ottobre 1977, n. 791**, così come modificata dal D. Lgs. 25 novembre 1996 n. 626, *“attuazione della direttiva 93/68/CEE in materia di marcatura CE del materiale elettrico destinato ad essere utilizzato entro alcuni limiti di tensione”*;
- **D. Lgs. 25 luglio 2005, n. 151**, *“attuazione delle direttive 2002/95/CE, 2002/96/CE e 2003/108/CE, relative alla riduzione dell’uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti”*;
- **D. Lgs. 3 aprile 2006, n. 152**, *“Norme in materia ambientale”*;
- **D. Lgs. 9 aprile 2008, n. 81**, *“attuazione dell’art.1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro”*;
- **Norme Tecniche** di riferimento.

Le apparecchiature fornite devono essere marcate CE e devono essere corredate di informazioni utili al loro smaltimento integrale o parziale, in conformità con la vigente normativa in materia.

La Società dovrà fornire idonea documentazione in merito alla sicurezza di quanto fornito; in particolare, dovrà documentare l’eventuale presenza di sostanze nocive o cancerogene.

La Società dovrà eseguire le attività in piena aderenza con le disposizioni del D. Lgs. 81/2008 “Testo Unico sulla sicurezza durante il lavoro”, cooperando e coordinandosi con i referenti della Committente, ai fini degli adempimenti di cui al comma 2 dell’art. 26 del citato decreto.



3 GESTIONE DELLA FORNITURA

Di seguito vengono specificate le modalità di erogazione della fornitura.

3.1 RESPONSABILE DELLA FORNITURA

La Società dovrà comunicare alla Consip, congiuntamente alla presentazione della documentazione per la stipula, il nominativo del Responsabile della Fornitura, 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.

3.2 MODALITÀ DI COMUNICAZIONE

La Società si impegna a comunicare a Consip, **contestualmente alla presentazione della documentazione per la stipula, 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 alla fornitura.

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.

La Società, dovrà rilasciare le informazioni richieste di cui ai paragrafi 3.1 e 3.2 attraverso la compilazione del documento denominato **“Scheda anagrafica e tracciabilità Sogei”**.

3.3 VERIFICA DI CONFORMITÀ

La verifica di conformità verrà effettuata ai sensi dell'art. 314 del DPR 207/2010 e verrà avviata, **entro 15 (quindici) giorni** dalla data di consegna per quanto riguarda la fornitura dei prodotti Hardware e Software, **entro il mese successivo al trimestre di riferimento**, per quanto riguarda il servizio di manutenzione.

A completamento di ogni singola verifica positiva sarà prodotto il “Verbale di conformità” che dovrà essere sottoscritto dal Responsabile della Fornitura e dal Responsabile Sogei.

La Verifica di conformità si intende positivamente superata solo nel caso in cui le prestazioni contrattuali siano state eseguite a regola d'arte sotto il profilo tecnico e funzionale e i prodotti forniti siano corrispondenti con quanto richiesto, in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente Capitolato tecnico.

In caso di esito negativo della verifica, la Società dovrà provvedere, a propria cura e spese, entro il termine che verrà concordato con il direttore dell'esecuzione di Sogei, all'eliminazione dei difetti e/o delle carenze riscontrati e/o alla sostituzione del prodotto.



Dopo la comunicazione, da parte della Società, dell'avvenuta eliminazione dei difetti e/o delle carenze e/o dopo la sostituzione del prodotto, Sogei procederà a una nuova verifica nei termini e con le modalità precedentemente indicate. In caso di ulteriore esito negativo della verifica, Sogei avrà facoltà di risolvere il contratto e di fare eseguire tutta o in parte la fornitura a terzi in danno della Società, fatto salvo in ogni caso il diritto al risarcimento di tutti i danni.

Tali Verbalì dovranno essere allegati alle fatture al fine del pagamento dei corrispettivi alla Società.

3.4 MODALITÀ DI FATTURAZIONE

Per quanto concerne la fornitura dei prodotti Hardware e Software si applica quanto previsto nel documento “Schema di contratto Sogei” all’art. 15 comma 1 - caso di acquisto di beni:

“Ai fini del pagamento del corrispettivo indicato nel presente contratto per la fornitura di beni, da intendersi inclusivo del servizio di manutenzione in garanzia, il Fornitore potrà emettere fattura successivamente al certificato di verifica di conformità positivo”.

Relativamente al servizio di manutenzione si applica quanto previsto nel documento “Schema di contratto Sogei” all’art. 15 comma 3 - caso di servizi a canone:

“Ai fini del pagamento del corrispettivo indicato nel contratto, inerente l'erogazione di servizi a canone, il Fornitore dovrà emettere fattura con periodicità trimestrale posticipata successivamente alla relativa verifica di conformità positiva. Nella fattura dovrà essere indicato il periodo temporale di riferimento”.

3.5 LIVELLI DI SERVIZIO

Di seguito sono indicati i livelli temporali ammessi per l'espletamento dei servizi di manutenzione.

Per ogni tipo di malfunzionamento hw e sw, la Società si impegna a completare il ripristino, con eventuale sostituzione integrale o parziale, al massimo **entro 8 (otto) ore solari** dall'apertura della chiamata.



4 PENALI

Sogei applicherà le penali, secondo le modalità previste in contratto, nei seguenti casi:

- per ogni giorno lavorativo di ritardo rispetto al termine previsto per la consegna dei prodotti hw e sw di cui al paragrafo 2.2, Sogei applicherà una penale pari allo 0,1 % (zerovirgolaunopercento) dell'importo totale del contratto;
- per ogni giorno di ritardo nell'eliminazione dei vizi accertati a seguito di esito negativo della verifica di conformità come disciplinato al paragrafo 3.3, si applicherà alla Società una penale pari allo 0,1 % (zerovirgolaunopercento) dell'importo totale del contratto;
- per ogni giorno di ritardo rispetto ai termini previsti per la risoluzione del malfunzionamento si hw che sw di cui al paragrafo 3.5, Sogei applicherà una penale pari a 0,1 % (zerovirgolaunopercento) dell'importo totale del contratto.