



Consip S.p.A.

“Fornitura Software per l’acquisizione di prove digitali forensi su dispositivi mobili”

CAPITOLATO TECNICO

FORNITURA SOFTWARE PER L’ACQUISIZIONE DI PROVE DIGITALI FORENSI SU DISPOSITIVI MOBILI



Consip S.p.A.

"Fornitura Software per l'acquisizione di prove digitali forensi su dispositivi mobili"

INDICE

1	PREMESSA	3
1.1	Definizioni.....	3
1.2	Descrizione dell'esigenza.....	3
2	OGGETTO DI FORNITURA.....	4
2.1	Caratteristiche Tecniche.....	4
2.2	Acquisizione ed estrazione di prove digitali da dispositivi mobili.....	4
2.3	Analisi delle prove digitali da dispositivi mobili	7
2.4	Formazione del personale	9
2.5	Consegna	9
2.6	durata	10
2.7	Servizio di manutenzione in garanzia	10
3	GESTIONE DELLA FORNITURA.....	12
3.1	Responsabile della Fornitura.....	12
3.2	Modalità di comunicazione	12
3.3	Verifica di conformità.....	12
3.4	Modalità di fatturazione.....	14
3.5	Riservatezza.....	13
4	PENALI	14



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:

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

1.2 DESCRIZIONE DELL’ESIGENZA

L’Agenzia delle Dogane e Monopoli (in avanti anche solo “ADM”), nel corso del 2022, ha espresso la volontà di ampliare l’ambito inerente al supporto agli uffici periferici e centrali dell’Agenzia ed agli organi di polizia giudiziaria per le acquisizioni e analisi forensi inerenti agli accertamenti tecnici su apparati multimediali prevedendo la possibilità di acquisire e analizzare non solo personal computer e totem ma anche dispositivi mobili.

Il nuovo ambito impone a Sogei di ampliare le dotazioni hardware e software, prevedendo anche una formazione del personale specifica nell’attività di perizia informatica forense inerente agli accertamenti tecnici su dispositivi mobili.

A questo fine, quindi, è necessario avere a disposizione una fornitura di software specifici come meglio dettagliato nei successivi paragrafi.



Consip S.p.A.

“Fornitura Software per l’acquisizione di prove digitali forensi su dispositivi mobili”

2 OGGETTO DI FORNITURA

Il presente documento disciplina l’acquisizione e la manutenzione di licenze d'uso di tipo “Subscription” di prodotti "Cellebrite", in particolare:

- a) Acquisizione ed estrazione di prove digitali da dispositivi mobili;
- b) Analisi di prove digitali da dispositivi mobili;
- c) Formazione del personale.

2.1 CARATTERISTICHE TECNICHE

Nella tabella seguente viene riportato il dettaglio dei prodotti e le quantità relativi ad una “Subscription” di 1 anno:

<i>Software</i>	<i>Descrizione</i>	<i>Quantità</i>
<i>UFED Touch3 Standard Ultimate Subscription + kit cavi</i>	Acquisizione Dati da devices mobili	1
<i>Cellebrite Premium Stand Alone + Premium Unlimited iOS</i>	Acquisizione Dati da devices mobili, prodotto Stand Alone (Offline 1 Laptop incluso)	1
<i>Cellebrite Premium Adroid action</i>	Sblocchi mobile devices (brute force)	20
<i>Cellebrite Digital Collector Subscription con dongle 1TB</i>	Acquisizione Dati da mobile devices (live e da cloud)	1
<i>Cellebrite Inspector Subscription</i>	Analisi di prove acquisite da mobile devices	1
<i>Training 5 GG per max 10 discenti</i>	Percorso formativo per SOGEI 10 discenti	1

2.2 ACQUISIZIONE ED ESTRAZIONE DI PROVE DIGITALI DA DISPOSITIVI MOBILI

L’acquisizione ed estrazione di prove digitali da dispositivi mobili deve prevedere la possibilità di estrarre e decodificare dati presenti in supporti digitali quali telefoni cellulari o smartphone anche con chipset cinesi, smartphone su base android, iOS o Windows, tablet, navigatori satellitari, ma anche server in cloud:

- deve prevedere un supporto per i fornitori Android, incluso il supporto esclusivo per Huawei, Xiaomi e altri;



- deve essere in grado di acquisire la più ampia gamma di dispositivi Android, incluso Snapdragon 888;
- deve prevedere il supporto per iOS supersonic incluso iPhone 11;
- deve supportare l’accesso al sistema operativo per più fornitori: Samsung, Huawei, Motorola, Sony, Alcatel, Oppo, Xiaomi, ZTE, Nokia;
- deve prevedere che la versione iOS e lo stato del dispositivo non hanno importanza per l’accesso AFU/BFU;
- deve prevedere un ampio supporto di dispositivi Android da parte del produttore di chipset, MediaTek, Exynos, etc.;
- deve prevedere un ampio supporto del supporto del dispositivo iOS BFU per eliminare il backlog;
- deve prevedere la possibilità di utilizzare la capacità di un attacco di forza bruta per dispositivi Android/iOS;
- deve prevedere il supporto AFU (dopo il primo sblocco) per dispositivi FDE (crittografia completa del disco), Android;
- deve prevedere funzionalità di forza bruta per dispositivi basati su Android come Huawei, Xiaomi, Alcatel, Oppo, Vivo, Blackberry;
- deve prevedere il supporto per sistemi iOS devices A13-A14-A15, iPhone 11, 12 and 13.

L’acquisizione dei dati presenti sul dispositivo analizzato, può essere svolta sia in maniera fisica, ovvero bit a bit sia in maniera logica, prevedendo anche il bypass del blocco di password e PIN ed il recupero dei dati cancellati, tra cui:

- applicazioni;
- chat (WhatsApp, telegram, viber, ecc.);
- Facebook, messenger di Facebook, Instagram, Twitter, etc.;
- Password;
- Email;
- registro delle chiamate in entrata e in uscita;
- sms in entrata e in uscita;
- iMessage (Apple);
- contatti;
- calendari e note;
- immagini;
- file audio;
- file video;



- cartelle sicurezza;
- dati di geolocalizzazione (da telefoni, navigatori satellitari e droni);
- e molto altro (data di prima accensione, aggiornamenti software, programmi di monitoraggio installati abusivamente e ogni altro dato utile);

In Particolare:

- Il software deve fornire funzionalità di accesso avanzate con sblocco ed estrazione dei dati da iOS e telefoni cellulari Android. La soluzione dovrebbe includere il software, l'adattatore e i cavi per eseguire le operazioni supportate su Apple iPhone e telefoni cellulari Android;
- Il software deve fornire funzionalità di accesso avanzate con sblocco. Deve prevedere l'estrazione completa del file system per i dispositivi di crittografia basata su file (FBE) e fisici e l'estrazione per i dispositivi di crittografia dell'intero disco (FDE) da fornitori leader come Samsung, Huawei, Xiaomi, Motorola, LG, Nokia, ZTE, OnePlus, Alcatel, Pixel, Realme, Vivo, Oppo, Pixel e altri;
- Il software deve fornire l'estrazione del file system completo After-First-Unlock (AFU) da bloccato e crittografato anche dispositivi con crittografia dell'intero disco (FDE) e crittografia basata su file (FBE) di fornitori leader come Samsung, Huawei, Xiaomi, Motorola, LG, Nokia, ZTE, OnePlus, Alcatel, Pixel, Realme, Vivo, Oppo, Pixel e altri;
- Il software deve fornire l'accesso tramite forza bruta (BF) da dispositivi Android bloccati e crittografati, con crittografia dell'intero disco (FDE) e crittografia basata su file (FBE), di fornitori leader come Samsung, Huawei, Xiaomi, Motorola, LG, Nokia, ZTE, OnePlus, Alcatel, Pixel, Realme, Vivo, Oppo, Pixel e altri;
- Il software deve fornire l'estrazione del file system completo basata su After-First-Unlock (AFU) dai dispositivi crittografati con crittografia dell'intero disco (FDE) e crittografia basata su file (FBE) di fornitori leader come Samsung, Huawei, Xiaomi, Motorola, LG, Nokia, ZTE, OnePlus, Alcatel, Pixel, Realme, Vivo, Oppo, Pixel e altri;
- Il software deve fornire funzionalità di forza bruta per sbloccare i dispositivi Huawei e Honor con processore Kirin;
- Il software deve fornire funzionalità di forza bruta per i dispositivi basati su Unisoc;
- Il software deve fornire funzionalità di forza bruta per sbloccare Qualcomm Snapdragon di nuova generazione Processore 888, dispositivi 8 Gen1, 8 Gen1+ e Gen2 come Samsung S, modelli Flip & Fold, Xiaomi Mi12, Redmi K50 Pro, OnePlus 10, RedmiA11 e altri;
- Il software deve fornire funzionalità di forza bruta per sbloccare dispositivi Qualcomm FBE a 64 bit come LG Velvet 5G, Moto XT2043, XT2115, TCL REVVL 4, OnePlus DE2118 e altri;
- Il software deve fornire funzionalità di forza bruta per sbloccare la crittografia basata su file Android Qualcomm (FBE) di fornitori leader come Motorola, Nokia, Huawei e altri;



- Il software deve fornire funzionalità di forza bruta per lo sblocco di dispositivi Android MTK con crittografia completa del disco (FDE) e crittografia basata su file (FBE) di fornitori leader come Samsung, OnePlus, Motorola, Nokia, Huawei e altri;
- Il software deve identificare, eseguire la forza bruta, ovvero decrittograferà ed estrarrà il contenuto di contenitori protetti inclusi Cartella sicura Samsung, spazio privato Huawei, secondo spazio Xiaomi e Realme system cloner;
- Il software deve fornire l'estrazione After-First Unlock (AFU) dagli iPhone 12-13 bloccati;
- Il software deve fornire un'estrazione completa del file system da iPhone 8, X, XS, XR, 11, SE gen2, SE gen 3, 12, 13 e 14 con iOS 16;
- Il software deve fornire funzionalità di forza bruta sui dispositivi BFU (Cold). Deve supportare iPhone 5-11 bloccato con iOS 8 - 16 per determinare il passcode del dispositivo;
- Il software deve fornire Sonic Brute-force sui dispositivi BFU (Cold). La soluzione dovrebbe supportare 3000-5000 tentativi al giorno (APD) per iPhone 6S-11;
- Il software deve fornire la forza bruta e il file system completo da iPad fino a iOS 15.7;
- Il software deve estrarre i Cloud Token da utilizzare per accedere direttamente alle applicazioni sul Cloud da entrambi Dispositivi iOS e Android;
- Il software deve fornire la possibilità di estrarre le chiavi Keystore dai dispositivi Android per consentire la decrittazione delle app sui server di decodifica. Deve supportare Samsung Health, Signal, Proton Mail, Samsung Cloud, Samsung pass, FitBit, Trust wallet e Mew wallet;
- Il software deve fornire un ambiente protetto consentendo la modalità di lavoro offline;
- Il software deve essere sotto password dell'utente e la sicurezza di BitLocker;
- Il software deve supportare l'estrazione selettiva dei dati dell'applicazione consentendo una rapida estrazione di dati specifici sia per iOS che per Android;
- Il software deve consentire l'estrazione in modo legale;
- Il software deve essere regolarmente aggiornato per supportare ulteriori versioni dei sistemi operativi e dispositivi durante la licenza valida e il periodo di supporto;
- Il software deve fornire lo sblocco illimitato e la licenza di estrazione illimitata per iOS ed in numero limitato per Android;
- Il software deve fornire all'esaminatore la schermata dei Dettagli del caso per riempire creare reports.

2.3 ANALISI DELLE PROVE DIGITALI DA DISPOSITIVI MOBILI

L'analisi di prove digitali estratte da dispositivi mobili presuppone l'utilizzo di software commerciale specifico che tenga conto di alcuni principi alla base dell'analisi forense. Tale software deve garantire l'integrità forense del sistema, ovvero:



- nessuna azione intrapresa dalle autorità incaricate dell'applicazione della legge o dal personale Sogei incaricato da tali autorità deve poter modificare dati che successivamente potrebbero essere invocati in tribunale;
- Il personale incaricato di svolgere l'attività di analisi dovrà possedere la competenza necessaria per l'utilizzo del software di analisi ed essere in grado di fornire prove che spieghino la pertinenza e le implicazioni delle sue azioni;
- Il software di analisi deve poter creare e conservare un audit Trail o altro tipo di registrazione di tutti i processi applicati alle prove digitali. Una terza parte indipendente dovrebbe poter essere in grado di esaminare tali processi e raggiungere lo stesso risultato.

In particolare è necessario che il software preveda un'analisi completa di prove acquisite su sistemi Windows, MAC, IOS e Android in un'unica soluzione:

- Il software deve supportare i sistemi basati su Windows: deve prevedere il controllo della history del dispositivo da Microsoft volume shadow copies;
- Il software deve prevedere l'analisi integrata per Windows memory ed il registro di sistema;
- Il software deve prevedere l'analisi automatica delle informazioni account, documenti recenti, download, cestino, Connessioni USB e altro;
- Il software deve prevedere l'analisi delle attività dell'utente e gli artefatti del registro come ad esempio jump lists, shellbags, prefetch, Windows 10 timeline activity, SRUM, e altro ancora;
- Il software deve dare il pieno supporto per Apple fusion drive, APFS, e dispositivi crittografati, incluso chip T2;
- Il software deve prevedere il controllo della cronologia del dispositivo da APFS snapshots and Time Machine backups;
- Il software deve prevedere la ricerca e la visualizzazione di unified log, Spotlight e KnowledgeC data;
- Il software deve prevedere la ricerca e visualizzazione dei download, delle connessioni WI-FI, dei documenti recenti, dell'attività utente ed altro;
- Il software deve prevedere il pieno supporto per IOS, ovvero deve poter visualizzare facilmente le conversazioni ed i messaggi dell'utente;
- Il software deve prevedere l'accesso a dati sulla salute, sul wallet delle transazioni, ed il calendario delle attività;
- Il software deve prevedere l'estrazione dei dati;
- Il software deve prevedere l'accesso a SQLite, Plist ed altro;



- Il software deve includere il supporto per integrazioni con prodotti come Berla iVe, Semantica 21, FotoDNA, Project VIC, APOLLO e altro;
- Il software deve prevedere funzionalità avanzate per produrre export e-Discovery;
- Il software deve prevedere la condivisione dei report con stakeholder esterni prevedendo un sistema di revisioni.

2.4 FORMAZIONE DEL PERSONALE

La fornitura comprende un periodo di formazione del personale della durata minima di 5 giorni erogata in presenza ed in lingua italiana.

In relazione alle caratteristiche peculiari dei software oggetto di fornitura, è necessario prevedere un percorso formativo inerente sia il software per l’acquisizione di dati da dispositivi mobili sia inerente le tecniche investigative anche proprie della Digital Forensic.

In particolare dovranno essere trattati i seguenti argomenti:

- un’introduzione alla mobile forensic ed alla digital forensic, principi, tecniche e contesto normativo Italiano;
- l’installazione e la configurazione dei software;
- le tecniche di acquisizione ed estrazione dei dati su dispositivi mobili;
- le estrazioni di dati logiche e fisiche dei file system in maniera forense;
- best practice per l’identificazione, la raccolta e l’analisi di dati estratti da dispositivi mobili;

Dovranno inoltre essere previste prove pratiche di acquisizione e analisi di dispositivi mobili con l’obiettivo di rendere autonomi i partecipanti nel condurre acquisizioni di dati, indagini ed analisi e nel produrre report forensi.

2.5 CONSEGNA

La consegna delle licenze software e della relativa documentazione dovrà essere effettuata entro 15 (quindici) giorni dalla data di stipula del contratto alla casella di posta del referente Sogei che sarà indicato successivamente al fornitore aggiudicatario, salvo diversi termini indicati dalla Sogei in accordo con il fornitore.

Entro il termine di 10 (dieci) giorni antecedenti la consegna, dovrà essere inviato a Sogei un elenco dei dati identificativi dei prodotti software e di tutte le informazioni necessarie al loro utilizzo, come ad es. il link da cui scaricare la licenza d’uso del prodotto, nonché la chiave di accesso che consente l’utilizzo della licenza stessa e la disponibilità delle nuove versioni del prodotto.



Consip S.p.A.

"Fornitura Software per l'acquisizione di prove digitali forensi su dispositivi mobili"

L'elenco dovrà essere inviato per email all'indirizzo di posta elettronica asset_sw@sogei.it.

L'elenco dovrà essere redatto secondo il seguente tracciato record:

Repertorio Contratto	Produttore	Nome licenza	Quantità	Unità di misura	Versione	Sistema operativo	Part number

Le licenze software dovranno essere corredate della relativa documentazione e manualistica e della documentazione tecnica necessaria per il corretto utilizzo.

Tutte le consegne dovranno risultare da appositi documenti che dovranno riportare:

- la ragione sociale del fornitore,
- il numero di repertorio,
- la descrizione dettagliata dei prodotti consegnati, con i relativi quantitativi, il modello e il numero seriale delle versioni dei prodotti software consegnati,
- la data di consegna.

A tale documentazione dovrà essere anche allegata la documentazione amministrativa.

Effettuata la consegna delle licenze, il fornitore dovrà fornire supporto a Sogei per la loro installazione, attivazione e configurazione presso le sedi Sogei, secondo le modalità e i termini concordati con Sogei.

Resta inteso che, qualora, a seguito di successive verifiche, Sogei rilevasse che il fornitore ha consegnato dei beni non conformi ai quantitativi e/o alle caratteristiche tecniche e qualitative indicate nel contratto, la Sogei si riserva il diritto di respingere i prodotti in consegna, senza alcun addebito per la stessa.

2.6 DURATA

Il contratto avrà una durata di 12 (dodici) mesi a partire dalla data di positiva verifica di conformità.

2.7 SERVIZIO DI MANUTENZIONE IN GARANZIA

La Società dovrà garantire il servizio di manutenzione della sottoscrizione software di cui al paragrafo 2, nelle modalità di seguito riportate.

Il servizio di manutenzione dovrà essere comprensivo dell'aggiornamento all'ultima release software disponibile sul mercato.



Consip S.p.A.

“Fornitura Software per l’acquisizione di prove digitali forensi su dispositivi mobili”

In particolare il servizio di manutenzione dovrà garantire:

- Il supporto on-line sia sui prodotti oggetto di manutenzione che sugli aggiornamenti software del prodotto;
- la risoluzione di malfunzionamento quali correzione di bug, patch e nuove Versioni principali o Versioni secondarie messe a disposizione dal produttore;
- la fornitura delle nuove release o “update” dei prodotti software entro 15 (quindici) giorni dalla loro immissione sul mercato italiano;

Per ogni malfunzionamento segnalato, la Società dovrà associare un numero identificativo di ticket e dovrà comunicare alla Sogei tale identificativo.

Ogni nuova versione e aggiornamento di cui sopra, dovrà essere consegnata alla Sogei tramite e-mail alla casella di posta asset_sw@sogei.it indicando il link o la chiave di accesso che permetta lo scaricamento tramite il sito del fornitore/produttore o qualsiasi altro mezzo che la renda disponibile alla Sogei.



3 GESTIONE DELLA FORNITURA

Di seguito vengono specificate le modalità di gestione 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 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 ai par. 3.1. e 3.2 attraverso la compilazione del documento denominato “Scheda anagrafica e tracciabilità”.

3.3 VERIFICA DI CONFORMITÀ

Sogei, effettuerà la verifica di conformità entro 15 (quindici) giorni dalla data di positiva installazione dei prodotti software e 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, in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente Capitolato tecnico.

Al termine delle attività sopra indicate sarà prodotto il “Verbale di conformità” che dovrà essere sottoscritto dal Responsabile della Fornitura e dal Responsabile Sogei.

Tale Verbale dovrà essere allegato alle fatture al fine del pagamento dei corrispettivi alla Società.

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



Consip S.p.A.

“Fornitura Software per l’acquisizione di prove digitali forensi su dispositivi mobili”

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.

3.4 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 e i moduli software forniti da Sogei o realizzati per il servizio, al di fuori delle attività oggetto del presente capitolato.



Consip S.p.A.

"Fornitura Software per l'acquisizione di prove digitali forensi su dispositivi mobili"

4 MODALITÀ DI FATTURAZIONE

Per quanto concerne la fornitura della sottoscrizione Sw del paragrafo 2, si applica quanto previsto nel documento "Condizioni contrattuali" - 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".

Per quanto concerne la fornitura dei servizi di formazione del par. 2.4, si applica quanto previsto nel documento "Condizioni contrattuali" - caso di servizi a consumo:

"Ai fini del pagamento del corrispettivo indicato nel presente contratto, il Fornitore potrà emettere fattura successivamente alla approvazione da parte della Committente del "consuntivo attività", contenente il dettaglio delle prestazioni professionali erogate nel periodo di riferimento, nonché della verifica di conformità positiva. Nella fattura dovrà essere indicato il periodo temporale di riferimento".



5 PENALI

In caso di ritardi rispetto agli obiettivi di intervento o di ripristino verranno applicate le seguenti penali:

- per ogni giorno di ritardo rispetto ai termini previsti per la consegna di cui al paragrafo 2.5, Sogei applicherà una penale pari a 0,1% (zerovirgolaunopercento) dell'importo totale del contratto;
- per ogni giorno di ritardo rispetto ai termini previsti per il rilascio degli aggiornamenti di cui al paragrafo 2.7, Sogei applicherà una penale pari a 0,1% (zerovirgolaunopercento) dell'importo totale del contratto;
- in caso di esito negativo della verifica di conformità di cui al paragrafo 3.3, si applicherà una penale pari allo 0,1 % (zerovirgolaunopercento) dell'importo totale del contratto, per ogni giorno lavorativo intercorrente tra la data del verbale negativo e quello positivo.