CAPITOLATO TECNICO

ACQUISIZIONE LICENZE E SERVIZI CYBERARK PER LA GESTIONE DI UTENZE AMMINISTRATIVE DEL DAG

INDICE

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 il servizio oggetto del presente Capitolato;
- SOGEI: la Società Generale di Informatica S.p.A., Committente;
- DAG: Dipartimento Affari Generali del Ministero Economia e Finanze: 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;
- 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;
- Società: la società aggiudicataria del servizio di manutenzione;
- Malfunzionamento: qualsiasi anomalia funzionale dei prodotti software e, in ogni caso, ogni difformità del prodotto in esecuzione rispetto alla relativa documentazione tecnica e manualistica d'uso;
- Responsabile della fornitura: la persona individuata dalla Società come interlocutore di Sogei e responsabile di tutte le attività contrattuali.

1.2 PREMESSA

Il DAG eroga i propri servizi attraverso infrastrutture ospitate prevalentemente nel CED DAG di Via Carucci, all'interno della sede Sogei, e con piccoli contesti IT distribuiti presso i CED della sede MEF di XX settembre e della sede MEF di Piazza Dalmazia.

Le soluzioni infrastrutturali consistono sia in componenti IT tradizionali, sistemi legacy e host virtualizzati X86, sia in soluzioni cloud on premise ad oggi basate su OpenStack.

La conduzione delle infrastrutture è affidata al mercato con contratti di conduzione sistemistica, la cui governance è in capo a Sogei.

Il tema della gestione delle utenze privilegiate per l'accesso amministrativo ai sistemi è diventato estremamente rilevante a seguito dell'entrata in vigore della normativa Europea del GDPR. In particolare per gli aspetti di registrazione e tracciatura di tutti gli accessi e della garanzia del principio del privilegio minimo da assegnare sulla base delle effettive esigenze di accesso ed intervento sui sistemi.

Al fine di assicurare la compliance al Regolamento e a tutte le prescrizioni in tema di gestione della Privacy, il DAG ha manifestato l'esigenza di acquisire una soluzione per la gestione delle utenze privilegiate.

Nel panorama delle soluzioni offerte, sono state identificate come di interesse le soluzioni del catalogo di CyberArk in considerazione dei fattori di seguito elencati:

- i prodotti CyberArk sono prodotti di livello Enterprise, adottati dalle maggiori compagnie a livello internazionale, con una costante evoluzione ed arricchimento delle funzionalità disponibili nel tempo, tipica dei prodotti leader su segmenti di mercato che ne costituiscono core business;

- la grande diffusione di mercato assicura la disponibilità di una vasta rete di partner, anche su territorio nazionale, in grado di offrire servizi sulla tecnologia, sui prodotti e per supporto alla system integration;

- la piattaforma è correntemente in uso nei CED Sogei per la gestione delle credenziali privilegiate non nominative con competenze consolidate sulle funzionalità e caratteristiche tecniche dei prodotti, sulla integrazione con altre componenti tecnologiche IT nonché su tematiche organizzative e metodologiche collegate al deploy della soluzione in ambienti operativi con esigenze di continuità e minimo disservizio;

- l'utilizzo, nei CED DAG, della stessa tecnologia PAM adottata in Sogei consentirebbe infine di sfruttare potenziali sinergie in termini di servizi di conduzione ovvero facilitare eventuali future integrazioni tecnologiche tra il perimetro IT del DAG e il perimetro IT Sogei (aggregazione in unica piattaforma o trusting/federazione, servizi di DR).

Al fine di verificare la copertura dei requisiti primari indicati dal DAG è stata eseguita una POC dei prodotti di interesse a giugno 2018 che ha confermato che le caratteristiche tecnologiche dei prodotti, ed i servizi di supporto forniti dal produttore CyberArk, risultano adeguati alle esigenze del MEF.

1.3 CONTESTO TECNICO-ORGANIZZATIVO

Il mercato delle soluzioni PAM consiste prevalentemente di due tipologie di tool:

- Privileged account and session management (PASM), soluzioni a supporto della protezione e gestione delle credenziali, della registrazione degli accessi;

- Privilege elevation and delegation management (PEDM), che implementano il principio del requisito minimo di accesso con possibilità di elevare i diritti garantiti.

I tool consentono di applicare le policy di sicurezza a larga parte di soluzioni IT: sistemi operativi, DB, middleware e software applicativo, apparati di rete e sicurezza, hypervisor, cloud services (IaaS, PaaS and SaaS).

Il mercato delle soluzioni PAM, fonte Gartner Market Guide for Privileged Access Management di agosto 2017, sta sempre più maturando con prevalenza di soluzioni SW on premise, anche se cresce il segmento di mercato di as a service su Cloud, e con acquisizioni mirate al consolidamento di posizioni di mercato da parte dei principali attori quali CyberArk e CA Technologies (tra gli altri).

L'interesse per le soluzioni cresce anche in ragione della richiesta di compliance a normative e dell'esigenza di una strategia globale di "cyber security defense" per infrastrutture critiche che riguarda non solo organizzazioni Enterprise ma anche medio/piccole.

Il mercato è molto competitivo e pertanto i diversi produttori si confrontano con piani di sviluppo delle funzionalità offerte mirati a ampliare le possibilità di deploy e gli automatismi offerti (estendendo funzionalità di discovery e gestione credenziali al maggior numero di contesti IT quali anche Devops, IaaS, PaaS, Container, Etc.).

I principali player del mercato hanno una offerta che comprende sia le funzionalità PASM che le funzionalità PEDM.

L'introduzione di soluzioni PAM all'interno di una organizzazione insiste sia su aspetti organizzativi che su modalità operative consuete, pertanto non è configurabile come un progetto puramente infrastrutturale ma più in generale come una revisione ed evoluzione globale delle politiche di sicurezza e protezione delle risorse critiche presenti (rif. global Cyber security defense approach). Sempre Gartner indica che il conseguimento dei risultati attesi richiede una impostazione in più step del deploy di tali soluzioni, con una iniziale analisi dell'ambito organizzativo/tecnologico e l'attivazione di soluzioni PASM, seguita eventualmente dall'introduzione di funzionalità aggiuntive PEDM e automatismi di integrazione con le soluzioni IT presenti. Si evidenzia infine come sia rilevante anche l'aspetto di formazione sull'uso e gestione di tali soluzioni e sulla sensibilizzazione di tutte le organizzazioni coinvolte dagli obiettivi di sicurezza che hanno determinato l'introduzione degli "strumenti tecnici" a supporto.

La POC eseguita ha riguardato le soluzioni CyberArk:

Enterprise Password Vault™ Protection, modulo per la gestione e l'audit delle credenziali privilegiate che consente di impostare policy di sicurezza e controllo su chi può accedere alle password e in quali condizioni.

Privileged Session Manager™, modulo che realizza funzioni di isolamento e controllo della sessione, registrazione delle azioni eseguite e monitoring real time. Consente di realizzare

un single point di accesso ai target evitando l'accesso diretto e il potenziale jumping su altri sistemi. Supporta inoltre l'integrazione con sistemi SIEM per conservazione dei dati e per invio alerts su attività non usuali.

L'architettura di test predisposta per la POC ha previsto i seguenti moduli:

Vault – sistema per la gestione e protezione degli account (con meccanismi crittografici certificati FIPS140-2);

CPM - Central Policy Manager, motore per la gestione degli account privilegiati attraverso il quale è possibile impostare le policy di rinnovo/modifica delle credenziali su sistemi distribuiti sia su reti locali che remote;

PVWA - CyberArk Portal, noto come Password Vault Web Access (PVWA), interfaccia multi - lingua e web-based per la gestione e definizione delle policy di account condivisi e applicativi. Permette la ricerca di sessioni registrate e l'impostazione di permessi di root per esecuzione di specifiche attività on demand. Il portale supporta anche accessi via mobile;

PSM - Privileged Session Manager è la soluzione per il monitoraggio e controllo degli accessi privilegiati a sistemi e apparati critici. Svolgendo funzioni di nodo di accesso consente la gestione dell'accesso al sistema target senza rendere visibile le credenziali di sistema all'utente.

PSMP - PSM SSH Proxy consente all'utente di connettersi a sistemi target UNIX dalla loro workstation e secondo modalità SSH consuete.

EPM - CyberArk Endpoint Privilege Manager per la rimozione di privilegi locali di amministrazione attribuiti a singole utenze e per gestire gli accessi amministrativi secondo il principio del minimo privilegio su sistemi Windows. È possibile inoltre controllare anche le applicazioni abilitate alla esecuzione sulla rete.

I sistemi target che sono stati considerati per la POC sono stati scelti considerando le tecnologie presenti all'interno del CED DAG.

Sono state realizzate integrazioni con infrastrutture di dominio per abilitare Account Discovery e Active Directory authentication.

I test hanno verificato la corretta interoperabilità in tutti gli ambiti identificati per l'utilizzo delle soluzioni all'interno dell'architettura tecnologica di riferimento per l'iniziativa e per i seguenti ambiti funzionali:

- Password Management;
- Session recording.

Per tutti gli accessi sono state verificare le funzionalità offerte in termini di audit e registrazione.

L'architettura di deploy della soluzione CyberArk è risultata inoltre rispondente ai requisiti di segmentazione logica e fisica delle zone di sicurezza presenti nel CED DAG.

Il prodotto permette inoltre la gestione dei requisiti minimi di accesso tramite installazione di agent su workstation operatore o server target.

1.4 REQUISITI TECNICO QUALITATIVI

Si precisano di seguito i requisiti posti dall'Amministrazione per la soluzione di Privileged Account Management da acquisire e che hanno guidato anche la POC eseguita sui prodotti CyberArk.

1.4.1 Requisiti qualitativi

Le soluzioni di interesse devono assicurare i requisiti minimi di seguito riportati:

- Robustezza certificata delle soluzioni proposte per la protezione e conservazione delle credenziali;
- Ampia copertura funzionale in ambito sia PASM che PEDM;
- Compliance con normative GDPR e per Gestione privacy.

In ragione della criticità dei servizi erogati dall'Amministrazione è importante che la soluzione identificata possa essere supportata da una rete certificata di partner su territorio nazionale e siano assicurati livelli di servizio adeguati ad un contesto Enterprise.

1.4.2 Requisiti tecnici

Per quanto riguarda i requisiti tecnici che la soluzione deve soddisfare si elencano di seguito alcune caratteristiche generali:

- Possibilità di creare isole di rete protette singolarmente da nodi di accesso e policy personalizzate;
- Gestione delle credenziali con soluzioni dedicate e isolabili, in termini di networking e responsabilità operativa, dal contesto IT circostante, protette a livello hardware o comunque con meccanismi di crittografia software robusta e certificata;
- Supporto di alta affidabilità e integrabilità con soluzioni in DR;
- Disponibilità di moduli/soluzioni di integrazione con le principali tecnologie IT sia on premise che su cloud (server, networking, security, strumenti di service management, middleware, soluzioni cloud IaaS/PaaS/CaaS) e per A2A password management.

Per i requisiti funzionali specifici per la gestione degli account con privilegi amministrativi sono stati indicate le seguenti aree di copertura da assicurare:

- Privileged account discovery – per domini Windows, server stand alone sia Windows che UNIX;
- Discovery and mapping of SSH-Keys in ambienti Unix/Linux;
- Gestione automatizzata delle password per piattaforme Windows, Microsoft Active Directory, Unix/Linux (possibilità di impostare policy di modifica periodica, per singolo accesso, da amministratore);
- Privileged session isolation (via proxy e senza accesso diretto a target) e registrazione supportata almeno per le piattaforme e protocolli Microsoft Windows RDP, Unix/Linux SSH. Sono di interesse la disponibilità di work flow di approvazione on demand oppure collegata alla gestione di ticket di richiesta;
- Least Privileged session, possibilità di gestire accessi utente (anche nominale) con diritto di esecuzione di un set determinato di comandi root registrati e monitorati;
- Disponibilità di moduli out of the box e di SDK per A2A password management e per il provisioning degli account su target creati on demand su soluzioni cloud IaaS, PaaS e CaaS on premise ed eventualmente anche in cloud esterno (pubblico/community).

2 OGGETTO DEL CAPITOLATO

2.1 INFORMAZIONI GENERALI

Come detto in premessa la presente iniziativa nasce dalla esigenza del DAG di dotarsi di una soluzione PAM per la gestione delle utenze amministrative privilegiate che consenta di rispondere alle previsioni indicate dalle normative di Gestione Privacy (in particolare, requisiti minimi di sicurezza) e dal Regolamento GDPR (in particolare, privilegio minimo di accesso) il cui rispetto è obbligatorio dal 1 Maggio 2017. Le tempistiche da assicurare per la fornitura sono quindi stringenti.

In ragione della conoscenza acquisita nel corso della POC per la predisposizione di una soluzione PAM che implementi i requisiti identificati per il DAG sono state identificate le seguenti esigenze:

Requisiti minimi soluzione PAS CyberArk

Descrizione Componente	Esigenza	Caratteristiche richieste
CyberArk Digital Vault	n°1 istanza per sito primario	Per installazione in HA su server fisici
CyberArk Digital Vault	n° 1 istanza per sito DR	Per installazione in HA su virtual server
CyberArk Web Interface -PVWA	n° 1 istanza per sito primario	Per installazione in HA su server virtuali
CyberArk Web Interface -PVWA	n° 1 istanza per sito DR	Per installazione in HA su server virtuali
Central Policy Manager - CPM	n°10 istanze	Per installazione su server virtuali
Privileged Session Manager - PSM	n°10 istanze	Per installazione su server virtuali
Privileged Session Manager - PSM SSH Proxy	n°10 istanze	Per installazione su server virtuali
Licenze utenti	n°50	50 utenti
Licenza per ambiente di test	1	Ambiente per test e verifiche di configurazioni di prodotto e di funzionalità di integrazione con componenti IT
SDK	Enabled	Possibilità di utilizzo API esposte dal prodotto

2.2 DESCRIZIONE

Il presente Capitolato prevede l'acquisizione di quanto di seguito riportato:

A. N. 1 Bundle PAS-USER-T2 - Named user licenses. Including Credential Protection, Session Isolation and Recording, and Privileged Attack Detection tier 2 [25-99] con licensing per 50 utenti;

B. N°5 licenze PAS-INF-CPM per il modulo CPM;

C. N. 1 MAINT-EU24X 7x3, servizio di manutenzione di 36 mesi per le licenze acquisite.

D. N. 22 Professional service Day - PS-EU (servizi specialistici, per supporto tecnico specializzato in affiancamento per attività di deploy complesse e per l’analisi di contesti con segnalazioni di criticità.

   I servizi professionali dovranno essere assicurati on site a chiamata per tutta la durata del contratto, impegnandosi a garantire nei giorni stabiliti la presenza delle risorse professionali richieste. Le prestazioni dovranno essere svolte, indicativamente, dalle ore 8:00 alle ore 17:00 dal lunedì al venerdì con esclusione delle festività fatto salvo differente accordo con Sogei e/o MEF.

Si considerano inoltre inclusi nella fornitura richiesta

- la partecipazione alle verifiche di conformità di quanto rilasciato e dei servizi erogati in modalità continuativa, la correzione di anomalie che impediscono la chiusura di verifiche di conformità;
- l’obbligo di fornire l‘ultima versione dei prodotti HW e SW richiesti;
- la possibilità di sostituire, a seguito di evoluzioni tecnologiche intervenute durante l’esecuzione del procedimento di acquisto e in fase di esecuzione contrattuale, i prodotti HW e SW oggetto dell’acquisizione con prodotti funzionalmente equivalenti o superiori rilasciati in sostituzione di quanto acquisito.

2.3 DURATA E CONSEGNA

I prodotti saranno inseriti nel contesto delle infrastrutture del DAG ovunque ospitate, CED ubicato nella sede di Sogei in via Mario Carucci (Roma) ovvero diverso site identificato da Sogei e/o MEF.

Per tutti i servizi richiesti, si considera di riferimento primariamente la sede Sogei di Via Carucci e, in maniera residuale, la sede MEF di Piazza Dalmazia o altra sede MEF nella città di Roma.

Il presente contratto, che verrà stipulato con Sogei, avrà una durata **di 36 (trentasei) mesi** a decorrere dalla data di stipula.

Almeno 10 (dieci) giorni prima dell‘avvio della fornitura, la Società dovrà comunicare alla SOGEI gli elenchi dettagliati delle licenze oggetto del contratto, al fine di poterne predisporre la ricezione, nonché verificarne la rispondenza ai requisiti richiesti.

In particolare dovranno essere forniti i dati di tutte le licenze software che dovranno essere inviate in formato elettronico (ad indirizzi e-mail comunicati successivamente) e dovranno contenere i dati indicati nella tabella che segue:

PRODUTTORE	NOME LICENZA	UNITA' DI MISURA	QUANTITA'	VERSIONE

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 20 (venti) giorni lavorativi dalla data di consegna per quanto riguarda la fornitura delle licenze di cui alle lettere A) e B) del paragrafo 2.2, entro il mese successivo al trimestre di riferimento, per quanto riguarda i servizi di manutenzione di cui alla lettera C) del paragrafo 2.2 ed entro il mese successivo al mese di riferimento, per quanto riguarda le giornate di supporto specialistico di cui alla lettera D) del paragrafo 2.2.

A completamento della 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 Verbali dovranno essere allegati alle fatture al fine del pagamento dei corrispettivi alla Società.

3.4 MODALITÀ DI FATTURAZIONE

Per quanto concerne la fornitura di nuove licenze di cui al paragrafo 2.2 lettere A) e B), 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 di cui al paragrafo 2.2 lettera C), 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”.

Relativamente all’acquisto dei servizi professionali di cui al paragrafo 2.2 lettera D), si applica quanto previsto nel documento “Schema di contratto Sogei” all’art. 15 comma 2 - 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”.

3.5 LIVELLI DI SERVIZIO

Il servizio dovrà essere assicurato con orario 24x7 e dovrà comprendere:

- accesso completo alla Knowledge Base di CyberArk;

- supporto telefonico / email.

Gli aggiornamenti software dovranno essere disponibili **entro 60 (sessanta) giorni** dal loro rilascio.

La presa in carico del problema/malfunzionamento dovrà avvenire **entro e non oltre 8 (otto) ore solari dalla segnalazione**.

La risoluzione del problema/malfunzionamento e ripristino della completa funzionalità dell'apparecchiatura dovrà avvenire entro e non oltre **3 (tre) giorni lavorativi** dalla presa in carico del malfunzionamento.

Nel caso in cui la Società riscontri un malfunzionamento che richiede un periodo di ripristino superiore ai tre giorni lavorativi, la Società dovrà entro la scadenza dei termini, concordare con Sogei il tempo necessario alla risoluzione del malfunzionamento.

3.6 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.

3.7 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", 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).

4 PENALI

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

- in caso di esito negativo della verifica di conformità di cui a paragrafo 3.3, si applicherà una penale pari a 0,1 % (zerovirgolaunopercento) dell'importo totale del contratto, per ogni giorno intercorrente tra la data del verbale negativo e quello positivo;
- per ogni giorno di ritardo rispetto ai termini di rilascio di nuove release di cui al paragrafo 3.5, Sogei applicherà una penale pari a 0,1 % (zerovirgolaunopercento) dell'importo totale del contratto;
- per ogni giorno di ritardo rispetto ai termini previsti per la presa in carico della segnalazione di malfunzionamento di cui al paragrafo 3.5, Sogei applicherà una penale pari a 0,1 % (zerovirgolaunopercento) dell'importo totale del contratto;
- per ogni giorno di ritardo rispetto ai termini previsti per la risoluzione del malfunzionamento di cui al paragrafo 3.5, Sogei applicherà una penale pari a 0,1 % (zerovirgolaunopercento) dell'importo totale del contratto.