CAPITOLATO TECNICO

SERVIZIO DI "REPOSITORY MANAGER" PER IL CONTROLLO DI CONFIGURAZIONE E SICUREZZA DELLE LIBRERIE SW E DELLE IMMAGINI CLOUD ADOTTATE NELL'AMBITO DEL PROGETTO CLOUDIFY

INDICE

1 PREMESSA

La mole elevata e in crescita delle librerie gestite (dipendenze dí terze parti e artefatti prodotti dai processi di compilazione) dall'attuale repository manager open source in webo nell'ambito del progetto Coudify NOIPA del DAG e l'esigenza di monitorare la sicurezza delle librerie utilizzate nel software rilasciato per il progetto in termini di presenza di vulnerabilità note e problemi relativi al corretto uso delle licenze di librerie open sources, si è resa auspicabile l'adozione di un Artifact & Library Repository Manager di classe Enterprise che sia integrabile e compatibile con la infrastruttura Openshift del progetto Cloudify.

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 della presente fornitura, affida la fornitura oggetto del presente Capitolato;
- SOGEI: la Società Generale di Informatica S.p.A., Committente; beneficiaria della fornitura;
- DAG: dipartimento dell'Amministrazione generale del personale e dei servizi, beneficiaria del servizio;
- Capitolato tecnico: il presente documento che enuncia le specifiche tecniche alle quali si dovrà conformare la fornitura;
- Contratto: il contratto che verrà stipulato tra la Sogei e la Società che enuncia le regole giuridiche alle quali si dovrà conformare la fornitura;
- Fornitura: il complesso delle attività oggetto del presente Capitolato;
- Società: la società aggiudicataria della fornitura;
- 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 delle attività contrattuali: la persona individuata dalla Società come interlocutore di Sogei e responsabile di tutte le attività contrattuali.

2 DESCRIZIONE DELLA FORNITURA

Il Dipartimento della Amministrazione Generale del Personale e del Servizi del MEF (DAG), si è dotato da tempo di una serie di strumenti atti a garantire il controllo di qualità delle componenti software rilasciate dai suoi fornitori nell'ambito degli sviluppi loro commissionati.

Lo strumento cardine di tali attività è costituto dal sistema Web (Web Orchestrator) che svolge il ruolo di orchestrazione per il funzionamento delle seguenti componenti:

- GITLAB per la gestione del repository GIT delle applicazioni
- Jenkins per l'automazione delle attività di compilazione
- SonarQube per le analisi di qualità del software
- Sonatype NEXUS nella sua versione Open, quale repository manager centralizzato e "library proxy server" verso Internet di tutte le librerie, sia di tipo open source che di terze parti, adottate nelle applicazioni sviluppate per nome e per conto del DAG.

Tutte le suddette componenti sono state adottate nella loro versione Open Source in quanto ritenute adeguate, nelle funzionalità offerte, alle iniziali necessità del DAG.

D'altra parte la crescente necessità di adottare più stringenti strategie di verifica del livello di sicurezza offerto dalle applicazioni e la recente introduzione del regolamento Europeo sulla privacy c.d. GDPR, hanno fatto emergere l'esigenza dí ampliare l'ambito dei controlli di sicurezza anche alle librerie di terze parti referenziate nei progetti. Analoga esigenza riguarda il controllo di sicurezza delle immagini docker dei microservizi realizzati nell'ambito del progetto Cloudify NOIPA, che necessitano di un attento e costante monitoraggio delle vulnerabilità di tutte le componenti run time che le compongono.

Si richiede pertanto la fornitura di un prodotto atto ad operare come repository manager di artefatti, librerie ed immagini docker che sia in grado di soddisfare i seguenti requisiti:

- Dovranno essere resi disponibili i repository per le seguenti tecnologie: Bower, Docker, GitLFS, Maven, .NET/NuGet, npm, PyPi, RubyGems, Yum, Apt, Helm, R, CocoaPods, Go, Gradle, Opkg, Vagrant, Chocolatey. La compatibilità del prodotto va garantita con tutte le ultime versioni dei componenti citati.

- Dovrà essere possibile eseguire il deposito automatizzato degli artefatti mediante build orchestrate dal prodotto Jenkins, per le tecnologie indicate nel precedente punto. A tale scopo dovrà essere oggetto della presente fornitura ogni componente necessario a garantire tale funzionalità mediante opportuni plugin compatibili con Jenkins.

- Dovrà essere possibile verificare in automatico, per artefatti, librerie e immagini docker presenti nei repository, la presenza di eventuali vulnerabilità note e rinvenibili nei principali siti specializzati (almeno CWE, CERT, OWASP). Tale caratteristica dovrà essere garantita almeno per le librerie Java, Javascript, NPM, YUM, APT, .NET, e per le immagini docker residenti nei repository citati nel precedente punto.

- Dovrà essere possibile verificare il corretto impiego delle licenze relative alle librerie di terze parti adottate all'interno delle applicazioni del DAG.

- Dovrà essere possibile produrre dei report e delle dashboard per consentire un efficacie e continuo monitoraggio dello stato delle applicazioni e delle dipendenze rispetto alle vulnerabilità note e poter effettuare una analisi dei trend.

- Dovrà essere possibile segnalare la presenza di nuove vulnerabilità di sicurezza su artefatti e immagini presenti nei repository a fronte della disponibilità di aggiornamenti nei database delle vulnerabilità.

- Dovrà essere resa disponibile la funzione di "proxy repository" quale interfaccia verso i repository public domain disponibili su internet per tutte le tecnologie citate al primo punto.

- Dovrà essere possibile verificare in automatico la tipologia di licenza (open source o proprietaria) delle librerie referenziate dai progetti che accedono ai repository indicati nel primo punto.

- Dovrà essere possibile poter definire delle policies di sicurezza rispetto all'utilizzo di librerie di terze parti contenenti vulnerabilità note e di coretto utilizzo delle licenze nei termini descritti all'interno delle stesse licenze o dalla loro tipologie, le policies sono da intendersi come una serie di regole e soglie con lo scopo di rappresentare lo schema di aderenza di una applicazione da un determinato livello di sicurezza in termini di presenza di vulnerabilità note nelle e di corretto utilizzo delle licenze nell'ambito delle librerie di terze parti inglobate nell'applicazione stessa.

- Dovrà essere possibile impedire l'uso di librerie non aderenti alle policies descritte nel punto precedente bloccando le operazioni di build automatiche gestite dal sistema WebO mediante il componente Jenkins.

- Dovrà essere possibile gestire il versionamento di artefatti e librerie caricate sui repository disponibili nel prodotto. Tale modalità dovrà essere compatibile con quelle offerte dai build manager più diffusi (a titolo esemplificativo e non esaustivo: maven, gradle, etc).

- Il prodotto dovrà consentire la gestione degli accessi e la parzializzazione nella visibilità di artefatti, immagini e librerie sulla base di utenze nominali. Il sistema di autenticazione dovrà essere compatibile con il prodotto Oracle IAM che implementa la funzionalità di "header authentication" trasmettendo sull'header delle richieste http al prodotto, le informazioni identificative degli utenti abilitati.

- Il prodotto dovrà fornire una interfaccia di accesso web sia alle funzioni di amministrazione che alle funzioni di consultazione per tutti gli utenti registrati. Dovrà inoltre essere possibile disporre di accesso http in formato analogo al repository maven2 per le librerie e gli artefatti Java. Tale interfaccia dovrà poter colloquiare in modo nativo con Maven di versioni >= 2.0

- Il prodotto dovrà fornire una serie di metodi basati su REST API al fine di consentire almeno:

  - La creazione, abilitazione o cancellazione di una nuova utenza
  - La profilazione delle utenze create
  - La creazione di un nuovo "hosted repository"

- Dovrà essere possibile definire e garantire accesso ad almeno 500 utenti nominali;

- Il prodotto dovrà garantire l'alta affidabilità almeno contro i guasti di un singolo nodo, il mirroring dei repository su altri nodi e funzionalità di load balancing tra almeno due nodi.

- Il prodotto dovrà garantire piena compatibilità ed integrazione con i principali prodotti di Continuos integration/Continuos Delivery, tra questi almeno Jenkins, docker, Ansible e OpenShift per le ultime versioni disponibili sul mercato.

- Il prodotto dovrà essere disponibile anche nella versione docker image e pertanto installabile come docker container.

- Il prodotto dovrà prevedere la installazione "on premise" ed installato in un ambiente target definito all'interno della infrastruttura del MEF e non esclusivamente su ambienti cloud esterni al MEF.

- Il prodotto non deve presentare limiti relativi all'utilizzo di spazio su disco per l'archiviazione di dati di ogni tipo comprese librerie e immagini.

- **Inoltre si richiedono 20 giornate di supporto tecnico a consumo.**

2.1 MANUTENZIONE CORRETTIVA E SLA

ll prodotto software dovrà essere oggetto di manutenzione correttiva consistente nella fornitura di quanto necessario (nuove versioni del software, patch o workaround) in grado di risolvere eventuali problemi funzionali o di sicurezza si manifestino nell'uso del prodotto; la Società dovrà fornire inoltre a Sogei, senza ulteriori oneri economici, il software oggetto di aggiornamento comprensivo della manualistica e del supporto professionale necessario alla applicazione delle misure correttive . Dovrà essere inoltre fornito il supporto professionale per la prima installazione del prodotto e per la migrazione di artefatti e librerie dall'attuale repository del sistema WebO, al nuovo prodotto.

Dovranno essere forniti gli aggiornamenti del sistema (es. per patch, nuove release) oltre all'aggiornamento di quanto necessario ad intercettare eventuali vulnerabilità presenti tra gli artefatti e le immagini depositate nel repository . Tutte le attività summenzionate da erogare a partire dalla Data di Accettazione della fornitura per 36 mesi dovranno essere ricomprese nel canone di manutenzione.

Dovranno essere garantiti adeguati SLA al servizio di manutenzione correttiva:

Tab. A

Gravità Malfunzionamento	Tempo di presa in carico del malfunzionamento	Tempo di risoluzione
CRITICA	4 ORE LAVORATIVE	Risoluzione del problema o individuazione di un workaround entro 8 (otto) ore lavorative a partire dal momento in cui ha preso in carico il malfunzionamento.
SEVERE	8 ORE LAVORATIVE	Risoluzione del problema o individuazione di un workaround entro 2 (due) giorni lavorativi a partire dal momento in cui ha preso in carico il malfunzionamento.
MODERATE	16 ORE LAVORATIVE	Risoluzione del problema entro 4(quattro) giorni lavorativi a partire dal momento in cui ha preso in carico il malfunzionamento.
LOW	32 ORE LAVORATIVE	Risoluzione del problema entro 8 (otto) giorni lavorativi a partire dal momento in cui ha preso in carico il malfunzionamento.

Ai fini della individuazione della tipologia di gravità di malfunzionamento in essere, fanno fede le seguenti definizioni:

- Critica: prodotto non più operativo oppure oggetto di un grave malfunzionamento; malfunzionamento con grave impatto sul business e/o su una porzione significativa di utenti; nessun workaround idoneo disponibile;

- Severe: perdita critica di funzionalità del prodotto o degrado significativo delle prestazioni con impatto su un elevato numero di utenti; nessun workaround idoneo disponibile;

- Moderate: perdita moderata di funzionalità del prodotto o problema di prestazioni, con impatto su più utenti; workaround idoneo disponibile;

- Low: richiesta riguardante questione tecnica di routine o domanda di carattere generale; caso afferente a versione di prodotti in end-of-life.

Per quanto riguarda gli aggiornamenti, la Società dovrà fornirli a Sogei entro 30 giorni dalla data di rilascio; sarà cura di Sogei valutarne la applicabilità.

Per servizio di Manutenzione Correttiva si intende la diagnosi e la rimozione delle cause e degli effetti sulle funzionalità, sulle interfacce utente e sulle basi dati dei malfunzionamenti delle procedure e dei programmi facenti parte del prodotto o come componenti a corredo forniti nel pacchetto di installazione in quanto necessari al suo funzionamento. Si precisa che l'intervento di manutenzione correttiva può riguardare anche il disallineamento della documentazione utente.

Più in generale, il servizio di manutenzione correttiva comprende tutte le attività volte ad assicurare la piena operatività del prodotto, sia a fronte di difetti del codice, malfunzionamenti od anomalie, sia in caso di problemi, potenziali o manifesti, derivanti da obsolescenza o incompatibilità tecnologica della soluzione rispetto alla infrastruttura sulla quale è basata.

A fronte di aggiornamenti o a conclusione di interventi di manutenzione, i prodotti aggiornati e la relativa documentazione, se aggiornata, dovranno essere consegnati alla Committente. Sarà cura della Società fornire alla Committente tutti i prodotti attraverso supporti informatici esenti da virus.

Il fornitore del prodotto dovrà eseguire la migrazione della soluzione in essere alla nuova, comprensiva di configurazioni utente, profilazioni e librerie, in un tempo massimo di 10gg dall'accettazione del prodotto stesso.

3 MODALITÀ DI ESECUZIONE DEL SERVIZIO / FORNITURA

Il contratto, di durata di 36 Mesi, dovrà prevedere la fornitura della licenza ed il supporto in garanzia del prodotto selezionato oltre al supporto per la prima installazione e la migrazione dalla soluzione in essere.

Le licenze dovranno essere consegnate presso la Sogei SpA di via Atanasio Soldati, 80 00155 Roma e/o via Mario Carucci 99

4 RESPONSABILE DELLA FORNITURA

La Società aggiudicataria dovrà comunicare alla Consip , congiuntamente alla compilazione della documentazione di gara , il nominativo e i riferimenti del proprio Responsabile della Fornitura.

La Società aggiudicataria si impegna a comunicare, contestualmente alla stipula del contratto, un numero di fax, un indirizzo e-mail, un numero di telefono e/o un sito Web al quale rivolgersi, per ogni comunicazione relativa alla fornitura.

Il Responsabile della Società aggiudicataria sarà l'interlocutore unico della Sogei per gli aspetti amministrativi, per l'organizzazione ed il coordinamento delle attività contrattuali. Sarà cura del responsabile verificare il rispetto di tutti gli adempimenti contrattuali.

Per facilitare e velocizzare l'attività amministrativa di entrambe le parti, ogni comunicazione riguardante aspetti contrattuali dovrà essere scambiata, sia in formato cartaceo che elettronico, tra il responsabile Sogei e quello della Società aggiudicataria.

5 MODALITÀ DI COMUNICAZIONE

Resta inteso che, per tutta la durata contrattuale, la Società aggiudicataria dovrà garantire la piena funzionalità dei mezzi di comunicazione di cui al par. 4 comunicando tempestivamente a Sogei eventuali modifiche.

6 VERIFICA DI CONFORMITÀ

La verifica di conformità verrà eseguita una volta che siano state ultimate le attività di consegna, attivazione o configurazione del bene oggetto del contratto.

La verifica di conformità verrà eseguita direttamente dal Responsabile della Fornitura Sogei in contraddittorio con il Responsabile della fornitura della Società aggiudicataria.

La verifica di conformità si intende positivamente superata solo se tutte le prestazioni contrattuali siano state eseguite a perfetta regola d'arte e secondo la documentazione tecnica e d'uso fornita dall'Impresa.

Solo a seguito della positiva verifica di conformità verrà emesso il relativo verbale.

7 FATTURAZIONE E MODALITÀ DI PAGAMENTO

Il pagamento del corrispettivo verrà effettuato dalla Sogei previa presentazione di apposita fattura, che dovrà essere emessa successivamente al verbale di positiva verifica di conformità in coerenza con quanto previsto nello Schema di contratto.

Il fornitore potrà emettere tre fatture, una per ogni anno di fornitura.

Per le giornate di supporto il fornitore potrà emettere fattura alla fine del mese per le giornate utilizzate nel mese di riferimento.

In particolare, nel caso di specie, si applica la disciplina prevista per l'acquisto di beni, come disciplinata dall'art. 15 comma 1 dello Schema di contratto e di seguito riportata:

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.

8 CONSEGNA

La consegna della fornitura dovrà avvenire entro 10 (dieci) giorni solari dalla stipula del contratto pena l'applicazione delle penali.

9 PRESCRIZIONI DI SICUREZZA

La Società aggiudicataria si impegna a porre in essere quanto necessario per 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, ai fini degli adempimenti di cui al comma 2 dell'art. 26 del citato decreto.

10 PENALI

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

- ritardo nei tempi previsti per la consegna dei prodotti di cui al precedente paragrafo 8, penale di € 50,00 (cinquanta/00) per ogni giorno di ritardo.
- Ritardo per Gravità del Malfunzionamento "CRITICA", per ogni ora di ritardo sul "Tempo di risoluzione" (vedi tab. A) di cui al paragrafo 2.1, penale di 0,001% del valore contrattuale.
- Ritardo per Gravità del Malfunzionamento "SEVERE", per ogni giorno di ritardo sul "Tempo di risoluzione" (vedi tab. A) di cui al paragrafo 2.1, penale di 0,001% del valore contrattuale.