



REGIONE BASILICATA

**DIREZIONE GENERALE
AMMINISTRAZIONE DIGITALE**

**UFFICIO AMMINISTRAZIONE
DIGITALE**

Via Vincenzo Verrastro, 6 - 85100 Potenza (PZ)

Tel. 0971.668335

ufficio.amministrazione.digitale@regione.basilicata.it

ufficio.amministrazione.digitale@cert.regione.basilicata.it



REGIONE BASILICATA

Direzione Generale Amministrazione Digitale

Ufficio Amministrazione Digitale

Affidamento dei servizi di manutenzione, aggiornamento e supporto tecnico triennale della piattaforma CAST, comprensivi di integrazione con il cloud regionale e formazione specialistica

CAPITOLATO TECNICO

CUP: G31F25000460009



SOMMARIO

1. Contesto tecnologico	3
2. Finalità e obiettivi dell'iniziativa	3
3. Oggetto	4
4. Descrizione di dettaglio dei servizi richiesti	5
5. Durata	10
6. Tempi e modalità di esecuzione	10
7. Documentazione tecnica richiesta	11
8. Passaggio di consegna	11
9. Revisione dei prezzi	12
10. Verifica, collaudo e penali	12
11. Norme finali	12



1. CONTESTO TECNOLOGICO

Il Data Center Unico Regionale della Regione Basilicata, conforme agli standard ANSI/TIA 942-B-2017 (Tier III), eroga servizi cloud in favore delle PAL e delle Società pubbliche del territorio regionale, con lo scopo di garantire a cittadini, imprese ed altre Amministrazioni l'accesso a servizi applicativi in linea con gli standard di sicurezza e protezione definiti a livello nazionale.

Il cloud regionale è basato su VMware Cloud Foundation e Tanzu Kubernetes Grid, mentre per le attività di sviluppo e rilascio software viene utilizzato GitLab, implementando pipeline CI/CD per la gestione del ciclo di vita applicativo. Al link <https://www.regione.basilicata.it/?temi-dgad=cybersicurezza> sono indicati tutti gli standard tecnologici adottati dalla Regione Basilicata.

Nel 2021 la Regione ha acquisito le piattaforme CAST Application Intelligence Platform (AIP) e CAST Highlight per la misurazione della qualità del software, il calcolo degli AFP, la verifica della presenza di violazioni di sicurezza e della robustezza del software, nonché la valutazione del grado di sostenibilità digitale del proprio portfolio applicativo.

Attualmente il patrimonio software applicativo sviluppato è costituito da circa 800 macchine virtuali nella quale sono implementati circa 300 servizi.

2. FINALITÀ E OBIETTIVI DELL'INIZIATIVA

L'obiettivo della fornitura è quello di assicurare la continuità operativa degli strumenti e dei processi già in uso presso l'Amministrazione e di integrare la piattaforma di Software Intelligence nei processi di sviluppo, test, rilascio e gestione applicativa, al fine di:

- garantire la cybersicurezza by design delle applicazioni ospitate sul Data Center Unico Regionale e assicurare i livelli minimi di sicurezza necessari a preservare la riservatezza, la disponibilità e l'integrità delle informazioni e degli applicativi gestiti;
- supportare le attività di assessment degli applicativi, automatizzando le verifiche di qualità e sicurezza del codice durante il ciclo di vita del software;
- confermare le metriche di valutazione già adottate per tutti gli applicativi sviluppati o ospitati;



- facilitare la modernizzazione e l'adeguamento degli applicativi ai più recenti standard di sicurezza informatica;
- migliorare la continuità operativa e la governance del portfolio applicativo regionale;
- preservare il patrimonio storico di analisi, metriche e baseline evolutive sino ad oggi sviluppato con le attuali piattaforme CAST in uso;
- valorizzare gli investimenti già effettuati nel prodotto CAST.

3. OGGETTO

La presente iniziativa ha per oggetto l'acquisizione delle seguenti soluzioni software e dei servizi professionali connessi:

- aggiornamento della piattaforma CAST AIP verso la nuova soluzione CAST Gatekeeper (100 applicazioni), comprensiva di manutenzione e supporto tecnico triennale;
- rinnovo della sottoscrizione della piattaforma CAST Highlight SCA (100 applicazioni) comprensivo di manutenzione e supporto tecnico triennale;
- servizi professionali per l'integrazione delle soluzioni nel processo DevSecOps del Data Center regionale;
- formazione tecnica rivolta al personale ICT regionale per l'uso avanzato delle dashboard, la configurazione dei Quality Gates e l'integrazione tramite API;
- formazione amministrativa destinata ai referenti gestionali per l'interpretazione dei report e delle metriche di conformità;
- porting delle analisi pregresse eseguite sulle precedenti versioni di CAST AIP e CAST Highlight.

Il Codice CPV dei servizi oggetto dell'appalto è **72200000-7 - Programmazione di Software e servizi di consulenza.**

L'operatore economico dovrà dimostrare, in sede di offerta, di essere in possesso dei titoli autorizzativi, accordi commerciali o certificazioni rilasciate dal produttore CAST, o da soggetti da questo autorizzati, che lo abilitino alla fornitura, manutenzione e supporto delle licenze oggetto del presente affidamento, nonché di essere un partner di tipo "System integrator" di CAST.



4. DESCRIZIONE DI DETTAGLIO DEI SERVIZI RICHIESTI

Attraverso la piattaforma di Software Intelligence CAST, già in uso dal 2021, la Regione vuole rafforzare il ruolo di erogatore di servizi cloud, garantendo la conformità normativa e la continuità operativa dei processi di analisi e controllo del software.

La soluzione individuata prevede l'integrazione di CAST Gatekeeper e CAST Highlight SCA nelle moderne pipeline DevSecOps per garantire qualità, sicurezza e sostenibilità del software.

Nello specifico:

1. **CAST Gatekeeper:** utilizza un motore di analisi strutturale che ricostruisce il metamodello architetturale delle applicazioni secondo lo standard ISO/IEC 19506. Questo strumento effettua misurazioni automatiche dei punti funzione (ISO 19515 - Automated Function Points), garantendo la conformità a standard internazionali come ISO/IEC 5055:2021, OMG ATDM (Automated Technical Debt Measure) e OWASP Top 10. Permette inoltre di configurare dei "Quality Gates" basati su metriche di qualità, sicurezza, sostenibilità e debito tecnico che permettono di bloccare automaticamente rilasci non conformi e fornisce metriche per la sostenibilità digitale, come il "Digital Energy Score", che si riferisce e si basa su standard riconosciuti come OMG ASCRSM / ISO 5055-3, GSF SCI e PdR UNI 147;
2. **CAST Highlight SCA:** analizza la composizione del software (Software Composition Analysis) e monitora l'utilizzo di componenti open source. Il software è in grado di rilevare vulnerabilità di sicurezza note (CVE), evidenziando in particolare quelle che sono già state attivamente sfruttate in attacchi reali (KEV), rischi legali legati alle licenze e obsolescenza dei componenti utilizzati. Genera inoltre in automatico le Software Bill of Materials (SBOM) in formati standard come CycloneDX e SPDX per garantire la conformità alle normative. È inoltre in grado di identificare le CWE di sicurezza presenti nei codici sorgente delle librerie e non ancora soggette a sfruttamento da parte di attaccanti potenziali. Infine, consente un alerting automatico ai responsabili applicativi qualora dovesse emergere una nuova CVE o KEV sulle librerie utilizzate.

L'integrazione con l'ecosistema VMware Tanzu è un elemento chiave della fornitura, in quanto consente di evolvere il tradizionale approccio alla qualità software basato su controlli manuali in un modello "intelligence-driven" automatizzato e basato su metriche oggettive. Le soluzioni CAST individuate possono essere integrate tramite un'architettura



API-first, supportando la containerizzazione e l'orchestrazione della catena di approvvigionamento tramite "Supply Chain Choreographer".

I benefici per la Regione Basilicata includono la possibilità di creare un Center of Excellence (CoE) autonomo per la software intelligence, standardizzare i processi di qualità e sicurezza e ottenere una visione unificata su tutte le applicazioni ospitate sul Data Center Unico Regionale. Il modello operativo si articola su tre livelli: Strategico (Governance), Tattico (Gestione delle Conoscenze) e Operativo (Supporto e Fornitura).

Inoltre, le soluzioni di Software Intelligence CAST supportano la certificazione della Sostenibilità Digitale, che garantisce la possibilità di implementare un processo di controllo degli aspetti di sostenibilità ambientale del software, inclusa la compliance agli standard di riferimento (es. OMG ASCRSM/ISO 5055-3, UNI PdR 147, GSF SCI/ISO 21031) o agli indici di settore (Digital Energy Score™), fino alla definizione di piani di miglioramento quantificabili e basati su obiettivi, con la conseguente ottimizzazione dei costi operativi connessi alla sostenibilità degli asset software (GreenOps, Energy saving, riduzione MAC etc.).

Le piattaforme sono predisposte per essere integrate con modelli LLM per la generazione del codice di remediation, al fine di ottimizzare le attività di risoluzione delle vulnerabilità individuate.

Più nel dettaglio, l'oggetto dell'appalto prevede una serie di attività finalizzate a rendere il personale della Regione Basilicata indipendente nella conduzione a regime dell'infrastruttura di misura. In particolare, le attività previste sono:

1) Realizzazione dell'infrastruttura di misura

L'infrastruttura di misura CAST dovrà essere configurata in modo da integrarsi con i sistemi Supply Chain Management (SCM) e DevSecOps basati su VMWare Tanzu della Regione Basilicata e da essere il più possibile flessibile, automatizzando il processo di produzione degli insight (valutazioni su sicurezza, qualità del codice, robustezza etc.) laddove lo si riterrà necessario in fase di analisi (esempi: innesco analisi, produzione di report, generazione automatica di piani di rimedio sulla base di set di regole o criteri di compliance). Questa attività include:

- installazione di CAST Gatekeeper sull'infrastruttura regionale (modalità on-premise) e integrazione di CAST Highlight SCA (modalità SaaS ibrido);
- porting delle analisi pregresse eseguite sulle precedenti versioni di CAST AIP e CAST Highlight;



- integrazione delle soluzioni nel processo DevSecOps Tanzu di VMware;
- test di roll-out della nuova piattaforma integrata;
- formazione specialistica rivolta al personale tecnico e amministrativo regionale;

Modello di integrazione nel processo DevSecOps

La soluzione dovrà integrarsi nei processi CI/CD (Continuous Integration/Continuous Delivery) e DevSecOps della Regione, garantendo l'automazione completa del ciclo di verifica, controllo e rilascio del software all'interno del Data Center Unico Regionale.

Le pipeline dovranno essere pienamente compatibili con gli ambienti GitLab, VMware Cloud Foundation e Tanzu Kubernetes Grid, e consentire una gestione centralizzata e configurabile dei processi di analisi, verifica e rilascio. Si descrive di seguito il modello di integrazione di CAST nei processi DevSecOps, che potrà essere ulteriormente affinato in fase di analisi dello scenario con l'aggiudicatario della gara. Tutte le fasi descritte dovranno essere tracciate ai fini di conformità normativa e controlli interni.

Pipeline per software di proprietà regionale:

1. Avvio deploy

Il fornitore dell'applicativo avvia il deploy dello stesso in ambiente di staging. Il sistema avvia automaticamente il processo di verifica;

2. Analisi statica (pre-deployment)

CAST Gatekeeper esegue l'analisi automatica dei sorgenti, verificando la conformità agli standard di qualità, sicurezza e architettura:

- a. se i risultati rispettano le soglie configurate (quality gates), il software viene rilasciato automaticamente in ambiente di staging attraverso pipeline CI/CD;
- b. in caso di non conformità, il sistema genera un report dettagliato (vulnerabilità, violazioni, debiti tecnici) e lo notifica automaticamente al fornitore e alle amministrazioni;

3. Analisi dinamica (post-deployment in ambiente di test)

CAST Highlight SCA esegue analisi continue in ambiente VMware Tanzu, identificando vulnerabilità runtime, librerie obsolete e componenti open source non conformi. Le analisi comprendono anche test funzionali e di regressione automatizzati, integrati nei quality gates.

I risultati vengono correlati con la precedente analisi statica, consentendo una visione integrata del rischio applicativo, e notificati automaticamente al fornitore e alle amministrazioni;

4. Rilascio controllato in produzione



In caso di esito positivo di tutti i test, il fornitore può avviare il deploy in ambiente di produzione attraverso pipeline CI/CD, con metodologia blue/green deployment o equivalenti, per assicurare continuità operativa e rollback immediato in caso di anomalia;

5. Monitoraggio e analisi continua in produzione (non intrusiva)

In ambiente di produzione, la piattaforma effettua controlli programmati o passivi per intercettare vulnerabilità emergenti o comportamenti anomali a runtime, senza impatto sulle prestazioni.

Le evidenze vengono integrate nelle dashboard di sicurezza e correlate con le analisi statiche e dinamiche precedenti;

6. Feedback loop e reporting

La piattaforma monitora nel tempo la sicurezza applicativa, notificando automaticamente a fornitori e amministrazioni le vulnerabilità emergenti (CVE, componenti open source vulnerabili, librerie obsolete).

I report vengono archiviati e resi consultabili tramite dashboard centralizzata, con possibilità di esportazione automatica in formati standard.

Pipeline per software in licenza d'uso

Per gli applicativi in licenza d'uso, la pipeline dovrà garantire un controllo continuo di sicurezza e conformità, anche in assenza di accesso diretto al codice sorgente.

1. Ricezione e gestione SBOM

Il fornitore dell'applicativo dovrà fornire una Software Bill of Materials (SBOM) conforme agli standard CycloneDX o SPDX.

Il sistema dovrà consentire l'importazione automatica o semi-automatica di tali SBOM nel flusso di analisi, con validazione della loro coerenza e integrità;

2. Avvio deploy

Il fornitore avvia il deploy dell'applicativo in ambiente di staging;

3. Analisi dinamica e composizione software

CAST Highlight SCA effettua verifiche automatiche sulle componenti open source e sulle librerie dichiarate, segnalando eventuali vulnerabilità note, rischi di licenza o versioni non aggiornate.

Le informazioni provenienti dalle SBOM dovranno poter essere arricchite con le evidenze raccolte dalle analisi dinamiche reali eseguite in ambiente VMware Tanzu;

7. Rilascio controllato in produzione

In caso di esito positivo di tutti i test, il fornitore può avviare il deploy in ambiente di produzione attraverso pipeline CI/CD, con metodologia blue/green deployment o



equivalenti, per assicurare continuità operativa e rollback immediato in caso di anomalia;

4. Monitoraggio e notifiche

Il sistema dovrà monitorare nel tempo l'obsolescenza e l'emergere di nuove vulnerabilità relative ai componenti dichiarati, notificando automaticamente gli esiti al fornitore e alle amministrazioni;

Le pipeline dovranno essere completamente configurabili, automatizzate e documentabili, consentendo di:

- impostare soglie di qualità e rischio differenziate per tipologia di software o dominio applicativo;
- definire destinatari personalizzati per report e notifiche automatiche;
- configurare regole di blocco automatico per i rilasci non conformi;
- registrare e tracciare tutte le fasi del processo per finalità di audit e rendicontazione.

2) Formazione e training on the job

Le attività formative sono finalizzate a garantire la continuità operativa e il consolidamento delle competenze già acquisite dal personale regionale sulla piattaforma CAST. In particolare, dovrà essere prevista:

- a) **Formazione tecnica:** durante la fase di implementazione, il personale tecnico dovrà ricevere una formazione approfondita su come configurare e gestire la piattaforma CAST. La formazione dovrà coprire l'utilizzo avanzato delle dashboard, la creazione di report personalizzati, l'integrazione tramite API e la gestione delle policy dei "Quality Gates";
- b) **Formazione amministrativa:** dopo l'entrata in funzione ("go-live"), la formazione dovrà concentrarsi sul personale amministrativo per l'uso delle dashboard esecutive, la gestione dei report di conformità e la comprensione delle metriche di business e delle tendenze.

Il personale della Regione Basilicata coinvolto nella conduzione del sistema CAST dovrà inoltre avere accesso ai corsi della CAST University, in autogestione, per acquisire le conoscenze necessarie alle attività di misurazione e gestione della piattaforma.

A completamento della formazione di CAST University, è richiesta l'organizzazione di workshop durante i quali il personale della Regione Basilicata dovrà essere affiancato per l'esecuzione di operazioni di analisi e pubblicazione delle misure, al fine di



consolidare la formazione con attività operative ed esempi su applicazioni reali del portfolio da analizzare.

3) Manutenzione e supporto tecnico specializzato

Il modello di manutenzione e supporto tecnico dovrà essere continuo e assicurare che la piattaforma rimanga efficiente e aggiornata:

- a) **Manutenzione:** dovrà includere assistenza prioritaria e rilascio di tutti gli aggiornamenti e le patch delle due piattaforme, assicurando altresì che l'infrastruttura di misura si evolva di pari passo con le nuove tecnologie e le esigenze del Data center regionale. Questo approccio garantisce che la soluzione non diventi obsoleta, bensì sia costantemente allineata agli standard di sicurezza e alle best practices più recenti. Il servizio di manutenzione dovrà prevedere livelli di servizio (SLA) definiti, con tempi di presa in carico e risoluzione differenziati per criticità;
- b) **Supporto tecnico specializzato:** oltre all'accesso al servizio di supporto CAST per l'apertura di ticket di servizio, la Regione Basilicata dovrà poter contare su personale specializzato per attività volte a mantenere il servizio in piena efficienza, quali:
 - ottimizzazioni delle configurazioni;
 - risoluzione di problemi complessi;
 - applicazione di patch e nuove release;
 - controlli regolari ("health checks") sul funzionamento e sul livello di prestazione del sistema CAST;
 - capacity planning e verifica del consumo reale di risorse;
 - adeguamento delle soluzioni per garantire la compatibilità con gli aggiornamenti dell'infrastruttura VMware e degli strumenti DevSecOps adottati dalla Regione.

5. DURATA

La durata dell'appalto è stabilita in 36 mesi decorrenti dalla data di sottoscrizione del contratto.

La Regione si riserva la facoltà di prorogare la durata del contratto per un massimo di 36 mesi ai sensi dell'art. 120 comma 10 del D.lgs. n. 36/2023 e di applicare quanto disposto dall'art. 120, comma 9, dello stesso decreto (quinto d'obbligo).

6. TEMPI E MODALITÀ DI ESECUZIONE

L'Aggiudicatario si impegna a mettere in esercizio le piattaforme CAST Gatekeeper e CAST Highlight SCA entro 30 giorni dalla sottoscrizione del contratto.



La piattaforma CAST Gatekeeper dovrà essere installata sul Data Center Unico Regionale, adottando un'architettura che garantisca livelli elevati di sicurezza, continuità operativa e compliance normative, mentre la piattaforma CAST Highlight SCA dovrà essere resa disponibile in modalità SaaS ibrido.

I servizi di integrazione delle piattaforme nell'infrastruttura cloud regionale, formazione specialistica e porting delle analisi effettuate con le precedenti versioni della piattaforma CAST saranno erogati secondo un piano di attività condiviso con la Regione successivamente all'aggiudicazione della gara.

Nel corso dell'affidamento, l'Aggiudicatario dovrà assicurare il continuo trasferimento al personale dell'Amministrazione e del Cloud Operations Center (COC) del know-how sulle attività condotte nell'appalto, al fine di rendere l'eventuale prosecuzione delle attività più efficace possibile. Le attività si svolgeranno da remoto, la presenza del personale dell'operatore economico presso la stazione appaltante potrà essere saltuaria e limitata a riunioni in ambiente di ufficio, non si ravvisano rischi interferenti ai sensi dell'art. 26 del D. Lgs. 81/2008. Pertanto, non è previsto il DUVRI.

7. DOCUMENTAZIONE TECNICA RICHIESTA

L'Aggiudicatario dovrà consegnare:

- Manualistica completa in lingua italiana e inglese;
- Documentazione di installazione e configurazione;
- Piano di integrazione con l'ambiente GitLab e VMware;
- Documentazione tecnica relativa alle configurazioni implementate e alle integrazioni realizzate.

8. PASSAGGIO DI CONSEGNA

Negli ultimi due mesi, la Regione si riserva di chiedere all'Aggiudicatario di trasferire a personale dalla stessa individuato le conoscenze necessarie a gestire i servizi oggetto di questo Capitolato e della Relazione tecnica, nonché la documentazione aggiornata necessaria alla gestione dei servizi. Il Piano delle attività per il passaggio di consegne dovrà essere concordato tra le parti. Nel periodo dell'eventuale passaggio di consegne l'Aggiudicatario uscente dovrà continuare ad assicurare i livelli di servizio previsti dal contratto. In ogni caso, l'Aggiudicatario dovrà garantire per tutto il periodo di validità del contratto un costante trasferimento di know-how al personale individuato dalla Regione riguardo i servizi oggetto dell'appalto, al fine di favorire per quanto più possibile l'autonoma gestione in prospettiva di tali servizi.



9. REVISIONE DEI PREZZI

Ai sensi dell'articolo 60 del D.Lgs. 36/2023, è prevista la revisione dei prezzi al verificarsi di particolari condizioni di natura oggettiva che determinino una variazione, in aumento o in diminuzione, dei costi di esecuzione delle prestazioni contrattuali.

La revisione è riconosciuta qualora la variazione dell'indice di riferimento, rispetto al valore base individuato alla data di aggiudicazione del contratto, sia superiore al 5 per cento. In tal caso, la revisione opera nella misura dell'80 per cento della variazione eccedente la suddetta soglia del 5 per cento.

La data di riferimento per il calcolo della variazione è quella dell'aggiudicazione del contratto; gli indici ISTAT relativi a tale data costituiscono il valore base di confronto.

La variazione dei costi è determinata mediante l'Indice dei Prezzi alla Produzione dei Servizi (PPI - Servizi), settore ATECO 62 "Produzione di software, consulenza informatica e attività connesse", pubblicato dall'ISTAT sul proprio portale istituzionale.

Il monitoraggio dell'andamento dell'indice è effettuato con cadenza trimestrale. Il superamento della soglia del 5 per cento comporta l'attivazione automatica del meccanismo di revisione, senza necessità di apposita istanza da parte dell'appaltatore.

Il RUP provvede alla rilevazione degli indici, alla verifica del superamento della soglia, all'applicazione della percentuale dell'80 per cento sulla quota eccedente il 5 per cento e alla formalizzazione dell'adeguamento del corrispettivo.

Qualora l'applicazione dell'articolo 60 del Codice non consenta di garantire il principio di conservazione dell'equilibrio contrattuale e tale equilibrio non possa essere ristabilito mediante rinegoziazione secondo buona fede, resta salva, ai sensi dell'articolo 12, comma 1, lettera b), dell'Allegato II.2-bis al Codice, la possibilità per la stazione appaltante o per l'appaltatore di invocare la risoluzione del contratto per eccessiva onerosità sopravvenuta. In tutti i casi di risoluzione ai sensi del presente articolo, si applica l'articolo 122, comma 5, del Codice.

10. VERIFICA, COLLAUDO E PENALI

Il servizio sarà soggetto a verifica di conformità da parte dell'Amministrazione. In caso di ritardi o inadempienze saranno applicate penali secondo le norme previste nel contratto.

11. NORME FINALI

Per quanto non espressamente previsto si fa riferimento al D.lgs. n. 36/2023 ed alla normativa vigente in materia.