Procedura aperta,
(ai sensi del D.Lgs. 50/2016 e s.m.i.)

Per l'acquisizione del servizio
di manutenzione evolutiva, migliorativa, adeguativa e correttiva e
di supporto operativo del Sistema Informativo SIRFO
della Regione Basilicata

Numero gara SIMOG ……

MISURE PER GARANTIRE LA SICUREZZA DELLE APPLICAZIONI INFORMATICHE INSTALLATE NEL DATA CENTER REGIONALE

ALLEGATO

C/6

FSE 2014-2020 POR BasilicataEuropa

REGIONE BASILICATA

Unione Europea
Fondo Sociale Europeo

REGIONE BASILICATA

PRESIDENZA GIUNTA REGIONALE

UFFICIO SPECIALE
PER L'AMMINISTRAZIONE DIGITALE

Via Vincenzo Verrastro, 6 – 85100 Potenza
Tel. 0971.668335
ufficio.amministrazione.digitale@regione.basilicata.it
ufficio.amministrazione.digitale@cert.regione.basilicata.it

UFFICIO SPECIALE PER L'AMMINISTRAZIONE DIGITALE

MISURE PER GARANTIRE LA SICUREZZA DELLE APPLICAZIONI INFORMATICHE INSTALLATE NEL DATA CENTER REGIONALE

Versione 2.0

Via Vincenzo Verrastro, 6 – 85100 Potenza
Tel. 0971.668335
ufficio.amministrazione.digitale@regione.basilicata.it
ufficio.amministrazione.digitale@cert.regione.basilicata.it

INDICE

Via Vincenzo Verrastro, 6 – 85100 Potenza
Tel. 0971.668335
ufficio.amministrazione.digitale@regione.basilicata.it
ufficio.amministrazione.digitale@cert.regione.basilicata.it

1 INTRODUZIONE

L'Ufficio Speciale per l'Amministrazione Digitale della Regione Basilicata, cui compete la gestione del sistema informativo regionale e degli aspetti che afferiscono alla Digitalizzazione ed alla Sicurezza Informatica degli enti connessi alla rete pubblica regionale, ha inteso intraprendere un cammino di innovazione del governo dei processi di digitalizzazione e della gestione delle forniture di sviluppo e manutenzione applicativa con i seguenti obiettivi:

- Fornire un sistema unico di indirizzo, gestione e valutazione del patrimonio applicativo attuale e in divenire, a cui possano far riferimento i diversi uffici regionali, perseguendo una logica di *segregation-of-duty* quale prerequisito per il governo dei fornitori esterni
- Prevenire i rischi operativi cui si espone l'Ente in termini di Sicurezza, Affidabilità, Manutenibilità, Efficienza;
- Verificare la dimensione funzionale del patrimonio applicativo in essere e dei nuovi sviluppi per governare il processo di approvvigionamento relativo alle forniture di sviluppo e manutenzione software;
- Quantificare i rischi connessi all'utilizzo di componenti Open Source in termini di licensing e copyright, vulnerabilità di sicurezza note ed obsolescenza attraverso un processo di Software Composition Analysis;
- Abilitare e facilitare la migrazione al cloud degli applicativi costruendo una roadmap di migrazione e identificando le attività di re-factoring necessarie;
- Abbattere i costi di presa in carico degli applicativi da parte dei team di sviluppo e dei fornitori dotandosi di uno strumento per la ricostruzione automatica e la visualizzazione delle strutture interne degli applicativi software;
- Identificare misure e criteri in termini di KPI e SLA, utili ad abilitare un sistema di verifica strutturale e oggettiva verso i fornitori.

L'Ufficio Speciale per l'Amministrazione Digitale ha quindi avviato nel settembre del 2020 un primo progetto di implementazione di un centro di competenza sulla Software Intelligence ed ha scelto di utilizzare le piattaforme e le metodologie basate su standard internazionali riconosciuti e molto diffusi che utilizzano tecniche per l'analisi strutturale del codice, di tipo statico, applicativo e su una serie di algoritmi predittivi di analisi rapida dei sorgenti. Tali metodologie consentono di:

- Analizzare la qualità strutturale, delle performance e dei rischi degli applicativi e delle forniture software secondo lo standard ISO/IEC 5055:2021;
- Calcolare la dimensione della baseline applicativa effettiva, mediante la tecnica degli AFP-Automated Function Point (Standard ISO 19515:2019) e misurare le MEV sulle applicazioni;
- Effettuare Software Composition Analysis secondo lo standard ISO 5320;
- Ricostruire l'architettura delle applicazioni e le loro interazioni, preservando così la conoscenza strategica dell'amministrazione sui propri asset digitali;
- Verificare la Cloud Readiness degli applicativi ottenendo informazioni sulla difficoltà di portare in Cloud le applicazioni misurate.

Via Vincenzo Verrastro, 6 – 85100 Potenza
Tel. 0971.668335
ufficio.amministrazione.digitale@regione.basilicata.it
ufficio.amministrazione.digitale@cert.regione.basilicata.it

L'importanza di questo progetto non è solo relativa alla diffusione dell'utilizzo delle metriche efficaci per controllare i processi IT dell'amministrazione ma in sostanza aumenta significativamente la capacità dell'Ufficio Speciale per l'Amministrazione Digitale di agire nella direzione indicata dalle varie linee d'intervento indicate nel Piano Nazionale di Ripresa e Resilienza (PNRR) varato di recente. In particolare, il progetto di Software intelligence ha fornito gli strumenti per adempiere agli impegni a garantire la Cybersecurity dei servizi al cittadino, ad accelerare la migrazione al Cloud degli asset software all'interno del processo di Digitalizzazione della PA ed infine a costruire un processo efficace di controllo dei fornitori IT.

2 QUESTIONARIO

Laddove si prevede l'acquisizione, manutenzione sia correttiva che evolutiva mediante procedure negoziali di sistemi informativi da installare sull'architettura cloud del Data center regionale, viene richiesto all'operatore economico di compilare il seguente questionario per acquisire le prime informazioni dell'applicazione:

IDENTIFICARE LE PROPRIETÀ GENERALI DELL'APPLICAZIONE	
Qual è il nome del titolare dell'applicazione?	
In quale anno è stata messa in produzione per la prima volta l'applicazione?	
Si tratta di un'applicazione personalizzata o di un prodotto commerciale?	
Qual è il tipo di applicazione?	
VERIFICARE L'IMPATTO DELL'APPLICAZIONE	
Qual è il numero di versioni principali consegnate negli ultimi 12 mesi per l'applicazione?	
L'applicazione è in linea con la futura direzione tecnologica dell'ENTE?	
L'applicazione serve utenti interni o esterni?	
Qual è il numero medio di risorse FTE (Full Time Equivalent) che hanno lavorato sul codice sorgente per l'applicazione negli ultimi 12 mesi?	
Qual è il numero approssimativo di utenti finali per l'applicazione?	
Il fallimento dell'applicazione potrebbe causare interruzioni? Si prega di definire il livello di impatto.	

Via Vincenzo Verrastro, 6 – 85100 Potenza
Tel. 0971.668335
ufficio.amministrazione.digitale@regione.basilicata.it
ufficio.amministrazione.digitale@cert.regione.basilicata.it

Il fallimento dell'applicazione potrebbe comportare una perdita di entrate o opportunità di business? Si prega di definire il livello di impatto.	
Il fallimento dell'applicazione potrebbe danneggiare l'immagine pubblica dell'Ente? Si prega di definire il livello di impatto.	
Il fallimento dell'applicazione potrebbe portare alla perdita di fiducia degli utenti? Si prega di definire il livello di impatto.	
STIMARE LE RISORSE NECESSARIE PER GARANTIRE LA MANUTENZIONE DEL SOFTWARE	
Quale percentuale dello sforzo di sviluppo è stata spesa per la manutenzione dell'applicazione negli ultimi 12 mesi?	
Qual è il livello medio di competenza del team di sviluppo su questo tipo di applicazione?	
Qual è il turnover annuale del personale all'interno del team di sviluppo per l'applicazione?	
Qual è la percentuale di modifica del codice di base per l'applicazione negli ultimi 12 mesi?	
DETERMINARE LA CAPACITÀ DI EVOLVERE VERSO IL CLOUD (CLOUD ENABLING)	
Qual è il modello di evoluzione e l'approccio del ciclo di feedback per l'applicazione?	
Qual è l'attuale piattaforma di distribuzione per l'applicazione?	
Qual è il livello di automazione del processo di distribuzione per il provisioning e la configurazione per l'applicazione?	
L'applicazione è multi-tenant (istanze multiple dell'applicazione)?	
Quali sono le relazioni con altri componenti applicativi esterni all'applicazione?	
Qual è il fornitore del database dell'applicazione?	

Via Vincenzo Verrastro, 6 – 85100 Potenza
Tel. 0971.668335
ufficio.amministrazione.digitale@regione.basilicata.it
ufficio.amministrazione.digitale@cert.regione.basilicata.it

Qual è la competenza media sulle tecnologie e le pratiche cloud all'interno del team di sviluppo per l'applicazione?	
Qual è l'attuale (o previsto) Service Level Agreement per questa applicazione?	
Qual è l'attuale meccanismo di autenticazione dell'utente utilizzato dall'applicazione?	
In che modo l'applicazione viene esposta a servizi/applicazioni esterne?	
Come vengono consumati i dati dell'applicazione?	
L'applicazione corrisponde a un carico di lavoro specifico?	

3 SPECIFICHE TECNICHE DI SISTEMA

Di seguito si forniscono le specifiche di sistema per la predisposizione di uno spazio hosting.

SISTEMA OPERATIVO	☐ CentOS 7.9 (supportata fino al 30 GIU 2022) ☐ AlmaLinux 8.5 (supportata fino al 01 Maggio 2024) ☐ AlmaLinux 8.6 (supportata fino al 01 Marzo 2029) ☐ Windows 2016 (supportata fino al 11 Gennaio 2027) ☐ Windows 2019 (supportata fino al 09 Gennaio 2029) ☐ Windows 2022 (supportata fino al 14 ottobre 2031) ☐ Windows 2012 (supportata fino al 10 ottobre 2023)
LINGUAGGIO	☐ PHP 7.4 (*supportata fino al 28 Novembre 2022*) ☐ PHP 8.0 (*supportata fino al 26 Novembre 2023*) ☐ PHP 8.1 (*supportata fino al 25 Novembre 2024*) ☐ ASP.NET (specificare versione ……) ☐ JSP & Servlet (specificare versione ……)
DATABASE	☐ MySQL 5.7 (*supportata fino a Ottobre 2023*) ☐ MySQL 8.0 (*supportata fino a Aprile 2026*) ☐ Oracle 19.g ☐ Postgresql (specificare versione ……)
WEB SERVER	☐ Tomcat 9.0 (*supportata fino al 26 Novembre 2022*) ☐ Tomcat 10.0 (*supportata fino al 02 Marzo 2024*) ☐ Apache 2.4 ☐ IIS 10 (*supportata fino al 09 Gennaio 2029*) ☐ IIS 8.5 (*supportata fino al 10 Ottobre 2023*)

Via Vincenzo Verrastro, 6 – 85100 Potenza
Tel. 0971.668335
ufficio.amministrazione.digitale@regione.basilicata.it
ufficio.amministrazione.digitale@cert.regione.basilicata.it

4 ANALISI RAPIDA SULLO STATO DI SALUTE DEL SOFTWARE, SULLA COMPOSIZIONE E SUL GRADO DI PORTABILITÀ IN CLOUD

L'obiettivo che l'ufficio si prefigge di raggiungere con la compilazione del questionario è quello di effettuare un'analisi generale dell'applicazione volta a:

- Identificare lo stato di portabilità al cloud, identificare le modifiche necessarie e stimarne l'effort;
- Identificare la composizione del software in termini di software custom e software open source e tecnologie;
- Identificare i rischi indotti dalla presenza di software open source identificandone le vulnerabilità di sicurezza note o latenti e l'esposizione a rischi legali relativi al licensing di questi componenti e produzione dell'inventario dei componenti Open Source utilizzati secondo lo standard ISO/IEC 5230:2020;
- Identificare lo stato di resilienza, manutenibilità e complessità;

L'ufficio produce una prima classificazione d'analisi basata sull'indicatore RRA (rango del rischio applicativo), che è rappresentato dalla media pesata degli indici di rischio operativo, di complessità e di rischio di carenza di agilità, filtrato dall'indicatore di impatto di business dedotto dalle interviste.

Gli estremi dell'indice RRA sono i valori 1 e 100 e rappresentano, su scala crescente, quanto urgentemente il rischio richieda mitigazione. Gli indicatori sottostanti possono essere ulteriormente così dettagliati:

- Il rischio operativo si riferisce a possibili difetti relativi al dominio della sicurezza, efficienza e robustezza.
- Il rischio di complessità è il puro rischio di difficoltà crescente della modifica di software stratificati e modificati a più riprese.

Il rischio da carenza di agilità è relativo a possibili difetti di regressioni e difficoltà non previste nella modifica evolutiva del software.

5 ANALISI PROFONDA DELLA QUALITÀ STRUTTURALE DEL SOFTWARE

Prendendo le mosse dall'analisi di primo livello, vengono analizzati in profondità tutti gli aspetti relativi alla sicurezza intrinseca degli applicativi in ambito, alla qualità strutturale e alla dimensione funzionale. Vengono rilevate le debolezze strutturali di sicurezza contenute negli applicativi, con un'analisi di tipo SAST (Static Application Security Testing), nonché le vulnerabilità, note o latenti, contenute nelle librerie Open Source utilizzate all'interno delle applicazioni. Per tale finalità è richiesto il rispetto dei seguenti requisiti:

- Indicatori della qualità del software secondo lo standard **ISO/IEC 5055:2021** "Misurazione automatizzata della qualità del codice sorgente";
- Vulnerabilità e fattori critici di sicurezza secondo gli standard **OWASP** e **MITRE;**
- Dimensione funzionale degli asset e delle MEV attraverso lo standard **ISO/IEC 19515:2019** degli Automated Function Point (Punti funzione automatizzati);
- Architettura software degli applicativi ed auto-documentazione tecnica secondo lo standard **ISO/IEC 19506:2012.**

Via Vincenzo Verrastro, 6 – 85100 Potenza
Tel. 0971.668335
ufficio.amministrazione.digitale@regione.basilicata.it
ufficio.amministrazione.digitale@cert.regione.basilicata.it

Tali misurazioni sono effettuate automaticamente su tutti i rilasci del software dei fornitori prima della messa in produzione in modo da poter minimizzare i rischi operativi (resilienza, efficienza, sicurezza e manutenibilità) e quantificare l'effettivo volume delle forniture stesse.

Mediante l'uso di una serie di strumenti integrati utilizzati dal Centro di Competenza di Software Engineering della Regione Basilicata, sono realizzano i quattro pilastri di base della disciplina di misurazione:

- Misurazione del rischi software;
- Misurazione della dimensione funzionale;
- Mitigazione dei rischi e remediation plan;
- Modernizzazione del software.

I valori dell'indicatore di sicurezza riscontrati in fase di analisi sono dettagliatamente documentati sulla piattaforma in fase di post analisi attraverso la puntuale indicazione delle problematiche riscontrate, secondo lo standard OWASP, la numerosità delle vulnerabilità relative, la loro collocazione nel codice sorgente e la priorità di fix di sicurezza.

In tal modo possono essere costruiti piani di fix puntuali per portare il rischio di sicurezza più vicino al valore target. Attraverso questa attività vengono riscontrate le vulnerabilità, catalogate come CWE dall'OWASP, che possono essere inserite in un piano di fix prioritario laddove risultino esporre le applicazioni ad intrusioni da parte di hacker. Casi tipici possono essere i seguenti:

- "*Avoid SQL injection in dynamic SQL for Oracle (CWE-89)*": espone un'applicazione ad accessi non autorizzati direttamente sui dati, fino alla loro cancellazione totale;
- "*Avoid using unsecured cookie (Javascript) (CWE-614)*": permette agli hacker di intercettare le informazioni private inserite dagli utenti su un'applicazione;
- "*Avoid uncontrolled format string (CWE-134)*" consente ad un hacker di effettuare attività di Denial of Service (DoS) bloccando un'applicazione attraverso l'inserimento di istruzioni malevoli;
- "*Avoid missing release of stream connection after an effective lifetime (ASCRM-CWE-772)*" permette di effettuare azioni DoS.