Finanziato dall'Unione europea
NextGenerationEU

Avviso di indagine di mercato

Procedura negoziata ex art. 50, comma 1, lett. e) del Dlgs 36/2023

AVVSA_ 2025-005 - Accordo Quadro per l'affidamento di servizi di progettazione, manutenzione, sviluppo e rework sistema Virtual Desk HD e altre implementazioni per FSE 2.0 - CUP E47H22003310006 - PNRR Misura M6 C2 I1.3.1

1. Premessa

LepidaScpA, società in house della Regione Emilia-Romagna e dei suoi Enti Pubblici Soci, intende avviare un'indagine di mercato relativa all'affidamento delle attività specificate in oggetto, al fine di individuare nel rispetto dei principi di economicità, efficacia, tempestività, correttezza, libera concorrenza, non discriminazione, trasparenza e proporzionalità, i soggetti da invitare alla successiva procedura negoziata, ai sensi dell'art. 50 comma 1 lett.e) del D.Lgs. 36/2023, mediante Richiesta di Offerta sul mercato elettronico del portale Sistema Acquisti Telematici Emilia-Romagna (SATER) di Intercent-ER.

Il presente avviso, ai sensi del D.Lgs. 36/2023 e in particolare all'articolo 50 comma 2 e l'allegato II.1 al D.Lgs. 36/2023, non costituisce avvio di una procedura di gara pubblica né proposta contrattuale.

La manifestazione di interesse ha l'unico scopo di comunicare ai potenziali soggetti interessati la disponibilità ad essere invitati a successiva procedura.

LepidaScpA si riserva di interrompere, modificare o annullare, in qualsiasi momento, per ragioni di sua esclusiva competenza, il procedimento avviato, senza che i soggetti richiedenti possano vantare alcuna pretesa.

Il successivo invito, ai sensi dell'art. 50 comma 1 lett. e), verrà rivolto a tutti gli operatori economici tra coloro che presenteranno richiesta ed avranno dichiarato il possesso dei requisiti di seguito indicati.

Resta inteso che, qualora l'operatore economico proponente non risulti registrato sulla piattaforma SATER, non potrà essere destinatario della lettera di invito, senza che ciò possa comportare alcuna responsabilità in capo alla Stazione Appaltante, tenuta alla segretezza sull'elenco dei soggetti che sono stati invitati a presentare l'offerta, ai sensi dell'art. 35, comma 2, lett. b) del D.Lgs. 36/2023.

2. Responsabile unico di Progetto

Il **Responsabile Unico di Progetto** è Gianluca Mazzini.

3. Oggetto importo e durata dell'affidamento

Il presente avviso ha ad oggetto la sottoscrizione di un Accordo Quadro per l'affidamento di servizi di progettazione, manutenzione e sviluppo sistema HD per professionisti e cittadini banca dati strutture e percorsi sanitari e socio sanitari finalizzati a servizi aggiuntivi per FSE, servizi di sviluppo per interoperabilità e applicazioni per interconnessione, nell'ambito della Misura PNRR M6 C2 I1.3.1, per un importo massimo stimato dell'affidamento di euro 219.000,00 (duecentodiciannovemila/00), oltre IVA.
L'affidamento avrà durata di 36 mesi.

4. Requisiti di partecipazione

Possono presentare manifestazione di interesse gli operatori economici di cui all'art. 65 del D.Lgs. 36/2023, **iscritti al mercato elettronico di Intercent-ER alla categoria merceologica CPV 72232000-0** in possesso dei requisiti dei seguenti requisiti:

- Requisiti di carattere generale ai sensi degli artt. 94 e 95 del Dlgs 36/2023;
- Requisiti di idoneità professionale:

  a) i partecipanti devono essere iscritti alla C.C.I.A.A. o nel registro delle commissioni provinciali per l'artigianato, o presso i competenti ordini professionali. Al cittadino di altro Stato membro non residente in Italia, è richiesta la prova dell'iscrizione, secondo le modalità vigenti nello Stato di residenza, come indicato all'art. 100, c.3 del D.lgs.n. 36/2023;
- Requisiti di capacità economico-finanziaria. Il concorrente dovrà avere:

  a) Fatturato globale maturato nel triennio precedente almeno pari a 1.000.000,00 IVA esclusa;
- Requisiti di carattere tecnico-professionale. Il concorrente dovrà:
  A. **Esecuzione negli ultimi tre anni di almeno n. 1 servizi analoghi a quelli oggetto della presente procedura di importo minimo pari ad euro 150.000,00**

     La comprova del requisito, è fornita mediante:
     - certificati rilasciati dall'amministrazione/ente contraente, con l'indicazione dell'oggetto, dell'importo e del periodo di esecuzione;
     - contratti stipulati con le amministrazioni pubbliche, completi di copia delle fatture quietanzate ovvero dei documenti bancari attestanti il pagamento delle stesse; - attestazioni rilasciate dal committente privato, con l'indicazione dell'oggetto, dell'importo e del periodo di esecuzione;

- contratti stipulati con privati, completi di copia delle fatture quietanzate ovvero dei documenti bancari attestanti il pagamento delle stesse.

B. **Avere risorse umane, con competenze adeguate riferite per l'appalto da svolgere e risorse tecniche e l'esperienza necessarie per l'erogazione dei servizi richiesti;**

La comprova del possesso del requisito dovrà avvenire mediante la trasmissione dei *Curricula* in formato pseudo-anonimo delle risorse messe a disposizione che saranno impiegate nell'appalto. In particolare dai curricula vitae delle risorse umane dovranno emergere le seguenti competenze:

- esperienza pluriennale e comprovata capacità di analisi, progettazione e sviluppo di software nel linguaggio Java 11 e superiore, Angular 10 e superiore;
- esperienza pluriennale e comprovata conoscenza ed esperienza di applicativi sanitari e delle relative integrazioni con i sistemi nazionali e regionali;
- conoscenza approfondita di linguaggio SQL specifico di Oracle 19 e successive;
- conoscenza approfondita di JSON, XML, XSLT;
- conoscenza approfondita delle tecnologie di SOA; in particolare tecnologia Web Services REST e SOAP;
- conoscenza approfondita dell'ambiente di sviluppo Java Eclipse, di Apache Tomcat;
- conoscenza approfondita di Javascript, HTML5, CSS, Bootstrap, Hibernate, Spring,, MyBatis;
- ottima conoscenza del sistema operativo S.O. Linux;
- conoscenza approfondita di linguaggi di scripting, quali ad esempio "Bash".
- comprovata conoscenza ed approfondita esperienza di DocER in tutte le sue componenti, tra cui, a titolo esemplificativo e non esaustivo, Alfresco, SOLR e relative personalizzazioni (provider);
- ottima competenza sul prodotto Apache SOLR, tra cui la capacità di amministrazione, monitoraggio e di implementazione di personalizzazioni e ottimizzazioni del framework.

Trattandosi di procedura di affidamento esperita nell'ambito della misura del PNRR M6 C2 I1.3.1 gli operatori economici dovranno essere in possesso dei requisiti richiesti dalla normativa PNRR.

5. CCNL applicato e tutela dei lavoratori

Alla successiva procedura negoziata di affidamento si ritiene applicabile il Contratto collettivo nazionale di lavoro (CCNL) del Terziario, Distribuzione e Servizi. Gli operatori economici partecipanti alla procedura potranno indicare nella propria offerta un differente contratto collettivo da essi applicato, purché garantisca ai dipendenti le stesse tutele di quello indicato da Lepida.

6. Modalità di presentazione della manifestazione di interesse

Ciascun operatore, in possesso dei requisiti di partecipazione, potrà trasmettere la propria manifestazione di interesse predisposta secondo il modello allegato al presente avviso (**All. B**), **esclusivamente tramite la Piattaforma telematica Sater entro e non oltre le ore 12:00 del giorno 03.04.2025.**

Non saranno prese in considerazione le manifestazioni di interesse trasmesse oltre il termine sopra indicato.

I soggetti interessati a presentare Manifestazione di interesse potranno inviare richiesta di chiarimenti, esclusivamente tramite piattaforma SATER entro il **26.03.2025 ore 12:00**

7. Ulteriori Informazioni

Il presente avviso è pubblicato anche sul sito istituzionale di LepidaScpA, all'indirizzo https://lepida.net/bandi-gara-contratti

Il Direttore generale
Responsabile Unico di Progetto
Prof. Ing. Gianluca Mazzini
(*f.to digitalmente*)

Allegato tecnico

Dettaglio dei servizi/prodotti richiesti

Oggetto della presente procedura sono i servizi di progettazione, manutenzione, sviluppo e rework sistema Virtual Desk HD e altre implementazioni per FSE 2.0.

Di seguito a titolo esemplificativo la descrizione del sistema attuale implementate attualmente in uso da Lepida S.c.p.A. ed oggetto della presente procedura e su cui potranno essere richiesti interventi evolutivi:

Il Virtual Desk (VD) o banca dati regionale è un sistema che consente la redazione e distribuzione di contenuti relativi alle prestazioni sanitarie erogate in Emilia-Romagna, con i luoghi e le modalità di erogazione. L'insieme delle schede relative alle prestazioni sanitarie sono importate da un altro sistema (il Catalogo SOLE) che, dialogando attraverso le API esposte dal VD, aggiorna i contenuti.
Il VD è la knowledge base su cui si appoggia un help desk interno per dare informazioni agli utenti nell'ambito di un numero verde regionale predisposto per tali scopi informativi; l'help desk dispone, sul VD, degli strumenti necessari per gestire e tracciare le chiamate degli utenti, a fini statistici.
Alcuni contenuti del VD vengono esposti, tramite API, al sito Guida ai servizi.

La piattaforma è composta da:

1. Repository Drupal: utilizzato per la memorizzazione delle schede informative e la gestione di autenticazione/autorizzazione.
2. API Rest: esposte da Drupal per l'integrazione con sistemi esterni come FSE, Cupweb, Pagonline e Guida ai Servizi.
3. Sito VD: applicativo PHP che consente la gestione delle schede informative e interagisce con Drupal tramite API.
4. Database Oracle: utilizzato per il ciclo di approvazione delle schede, gestione dei contenuti preferiti e tracciamento delle chiamate dell'help desk.
5. Integrazione con altri sistemi regionali: tramite API, vari sistemi accedono alle informazioni del VD (ad esempio alcuni sistemi dipartimentali delle AUSL/AOSP).

Obiettivi dell'Evoluzione

L'obiettivo principale è integrare il VD nel Fascicolo Sanitario Elettronico Regionale FSE 2.0, migliorandone funzionalità, efficienza e compatibilità con i sistemi esistenti. I principali obiettivi includono:

1. Migrazione dei Contenuti: Trasferire i dati su un RDBMS Oracle, adottando un modello ER che rappresenti entità chiave come Azienda, Distretto, FAQ, Persona, Gruppo di popolazione, Programma, Prestazione, Luogo, Modalità di erogazione, News, Comuni, Patologie, Nomenclatore e Contenuto generico.
2. Compatibilità con le API Attuali: Sviluppare nuove API conformi allo standard OpenAPI, garantendo retrocompatibilità con le API Rest esistenti per consentire ai sistemi già operativi di continuare a funzionare senza modifiche.
3. Interfaccia Utente Intuitiva: Migliorare l'attuale interfaccia utente, seguendo anche i criteri di accessibilità previsti, garantendo una semplice transizione per gli utenti
4. Integrazione con FSE: Facilitare l'esposizione dei contenuti del VD come parte integrante del FSE (attraverso una chatbot)
5. Revisione del Sistema di Autenticazione: Implementare un sistema di autenticazione moderno con supporto per username/password e migrazione dei dati di accesso esistenti.
6. Unit Test: il sistema nel suo complesso (front end e back end) deve poter essere sottoposto a strumenti di testing automatici
7. Nuove Funzionalità:
    - Introduzione di una chatbot alimentata da VD, Support FSE e il nuovo sistema di Help Desk.
    - Template HTML per rendere omogenea la creazione di contenuti.

Sviluppi di Web Service

Interventi per lo sviluppo di Web Service che si concentrano sull'implementazione di funzionalità che consentano la comunicazione sicura e affidabile tra i diversi sistemi e piattaforme. Le attività richieste includono:

- Progettazione e sviluppo di Web Service basati su protocolli standard (es. SOAP e REST), garantendo interoperabilità tra i sistemi.
- Realizzazione di servizi per lo scambio dati.
- Gestione degli endpoint: Implementazione di endpoint specifici per integrazioni con

sistemi locali, regionali e nazionali.

- Sicurezza e conformità: Adozione di protocolli di sicurezza (es. autenticazione OAuth 2.0, crittografia TLS) per proteggere le comunicazioni.

Sviluppi di API

Gli interventi relativi alle API riguardano la progettazione e sviluppo di interfacce per consentire l'accesso standardizzato ai dati e alle funzionalità del sistema. Lo sviluppo di nuove API mediante lo standard OpenAPI 3.1.0.

Le componenti sono sviluppate utilizzando lo stack tecnologico adottato da Lepida ScpA, con versioni stabili delle seguenti librerie:

- Java con OpenJDK;
- Building tool con Gradle;
- Spring Framework e Spring Boot
- Web framework: Apache Wicket o Angular;
- Oracle;
- Apache Tomcat;
- MyBatis;
- Bootstrap o Bootstrap Italia;
- Sentry;
- OpenAPI.

L'utilizzo di librerie non incluse nell'elenco fornito dovrà essere valutato e approvato da Lepida ScpA; Lepida ScpA predilige l'utilizzo di librerie open-source (software libero), che siano correntemente manutenute e che siano ampiamente utilizzate dalla comunità. Gli sviluppi dovranno attenersi alla Politica per sviluppo sicuro del software di Lepida .

Gli sviluppi dovranno attenersi alla Politica per sviluppo sicuro del software di Lepida riportato nell' Allegato B - Politica per lo sviluppo sicuro del software.

Con la presente procedura LepidaScpA intende inoltre approvvigionarsi di servizi di supporto relativi alle attività di progettazione, sviluppo e alla manutenzione evolutiva delle piattaforme software sopra descritte e di altre applicazioni di Lepida.
Per queste piattaforme, la fornitura include le attività ed i servizi di seguito riportati, che dovranno essere pianificati nei dettagli da parte dell'Aggiudicatario in accordo con LepidaScpA nel rispetto

della tempistica prevista. Sono ricomprese nell'incarico le attività di knowledge transfer, attività che dovrà essere svolta immediatamente all'avvio del contratto e ricompresa nel periodo dei 24 mesi.
LepidaScpA fornirà la documentazione necessaria e la necessaria formazione ed affiancamento, per un massimo di 5 giorni a piattaforma, in funzione della complessità.

A titolo esemplificativo e non esaustivo, si fornisce nel seguito la descrizione di alcuni fabbisogni su applicativi e applicazioni software, attualmente in uso da LepidaScpA, su cui potrebbero essere richiesti servizi di supporto:

- Supporto alla progettazione e realizzazione delle modifiche evolutive da apportare al cd Virtual desk e la sua integrazione con i servizi di FSE 2.0 e Catalogo Sole, e altre piattaforme anche sanitarie;
- Supporto alla progettazione e realizzazione rinnovamento dei Front-end di applicativi in uso;
- Supporto all'aggiornamento e scrittura di back-end di applicativi in uso;
- Supporto alla progettazione e definizione di architettura software;
- Supporto alle integrazioni con le componenti di Lepida quali ad esempio: SOLE, FSE Anagrafi Regionali, Cartelle, Backbone Sanità On LinE, CUP; FedERa, PayER, Sistemi di firma, ADRIER, RecordER, GenIO;
- Supporto alla realizzazione di cruscotti per la business intelligence e reportistica evoluta;

Il Direttore generale
Responsabile Unico di Progetto
Prof. Ing. Gianluca Mazzini
(*f.to digitalmente*)

Allegato A - INFORMATIVA per il trattamento dei dati personali ai sensi dell'art. 13 del Regolamento europeo n. 679/2016

1. **Premessa** Ai sensi dell'art. 13 del Regolamento europeo n. 679/2016, LepidaScpA, in qualità di "Titolare" del trattamento, è tenuta a fornirle informazioni in merito all'utilizzo dei suoi dati personali.
2. **Identità e dati di contatto del titolare del trattamento** Il Titolare del trattamento dei dati personali di cui alla presente Informativa è LepidaScpA, con sede in Via della Liberazione n. 15, in Bologna (40128). Al fine di semplificare le modalità di inoltro e ridurre i tempi per il riscontro si invita a presentare le richieste di cui al paragrafo n. 12, a LepidaScpA, Area Affari Legali, Societari e Privacy, via e-mail all'indirizzo verifichelegali@lepida.it
3. **Il Responsabile della protezione dei dati personali** Il Responsabile della protezione dei dati designato da LepidaScpA ai sensi dell'art. 37 del GDPR è contattabile all'indirizzo dpo@lepida.it.
4. **Responsabili del trattamento** LepidaScpA può avvalersi di soggetti terzi per l'espletamento di attività e relativi trattamenti di dati personali di cui LepidaScpA ha la titolarità. Conformemente a quanto stabilito dalla normativa, tali soggetti assicurano livelli di esperienza, capacità e affidabilità tali da garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati. Vengono formalizzate da parte di LepidaScpA istruzioni, compiti ed oneri in capo a tali soggetti terzi con la designazione degli stessi a "Responsabili del trattamento". Tali soggetti vengono sottoposti a verifiche periodiche al fine di constatare il mantenimento dei livelli di garanzia registrati in occasione dell'affidamento dell'incarico iniziale.
5. **Soggetti autorizzati al trattamento** I Suoi dati personali sono trattati da personale interno previamente autorizzato e designato quale "autorizzato" al trattamento ex artt. 29 e 4.10 del citato Regolamento europeo, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, modus operandi, tutti volti alla concreta tutela dei tuoi dati personali.
6. **Finalità e base giuridica del trattamento** Il trattamento dei suoi dati personali viene effettuato da LepidaScpA al fine di dare corso alla procedura di affidamento di beni, servizi o lavori. La base giuridica dei trattamenti è, quindi, costituita dall'art. 6 comma 1 lett. c) per i trattamenti relativi all'esecuzione degli obblighi disposti dalla normativa in materia di appalti e dall'art. 6 comma 1 lett. b) a seguito dell'eventuale aggiudicazione.

7. **Destinatari dei dati personali** I suoi dati personali non sono oggetto di comunicazione o diffusione, fatta eccezione per la:
    a. comunicazione ai collaboratori di Lepida ScpA in qualità di persone autorizzate e/o Responsabili del trattamento e/o amministratori di sistema;
    b. comunicazione ai soggetti che effettuano istanza di accesso ai sensi della L. 241/1990;
    c. comunicazione ai soggetti che effettuano istanza di accesso civico, previa valutazione dei limiti cui è sottoposta tale comunicazione ai sensi dell'art. 5 bis del D.lgs. 33/2013;
    d. pubblicazione ai sensi della normativa in materia di trasparenza in caso di aggiudicazione.
8. **Categorie di dati personali trattati** Per il perseguimento delle finalità di cui al precedente punto 6, oggetto di trattamento potranno essere dati ordinari identificativi della persona, quali, a titolo esemplificativo, nome, cognome, data e luogo di nascita, codice fiscale, indirizzo e.mail. Al fine di ottemperare agli obblighi previsti dalla normativa in materia di appalti pubblici, potranno essere, altresì, oggetto di trattamento i dati personali rientranti nella categoria di cui all'art. 10 Reg. UE 2016/679 nella misura strettamente necessaria e pertinente rispetto alle finalità definite dalla legislazione vigente in materia.
9. **Modalità di trattamento** I Suoi dati personali sono trattati con modalità, strumenti e procedure informatiche e/o analogiche. Lepida S.c.p.A. osserva specifiche misure di sicurezza tecniche ed organizzative (ad es. crittografia del dato) per prevenire la perdita dei dati, gli usi illeciti o non corretti e gli accessi non autorizzati.
10. **Trasferimento dei dati personali a Paesi extra UE** I suoi dati personali non sono trasferiti al di fuori dell'Unione europea.
11. **Periodo di conservazione** I suoi dati sono conservati per un periodo non superiore a quello necessario per il perseguimento delle finalità sopra menzionate e comunque non oltre il termine ordinario decennale di prescrizione ai sensi dell'art. 2946 c.c. A tal fine, anche mediante controlli periodici, viene verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che Lei fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non sono utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.
12. **I suoi diritti** Nella sua qualità di interessato, Lei ha diritto, ai sensi degli artt. 15 e ss. del Regolamento europeo:

a. di accesso ai dati personali;
b. di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano;
c. di opporsi al trattamento;
d. di proporre reclamo al Garante per la protezione dei dati personali.

Per l'esercizio dei Suoi diritti può fare riferimento al "Disciplinare riguardante l'esercizio dei diritti dell'interessato" ed utilizzare il "Modulo per l'esercizio di diritti in materia di protezione dei dati personali", disponibili al link https://lepida.net/societa-trasparente/altri-contenuti/dati-ulteriori.

13. **Conferimento dei dati** Il conferimento dei Suoi dati è facoltativo, ma necessario per le finalità sopra indicate. Il mancato conferimento comporterà l'esclusione dalla procedura di affidamento di beni, servizi o lavori.

Politica per sviluppo sicuro del software

POL-SGSI-007 ver. 1.0

Sommario

Scopo e campo di applicazione

Il presente documento ha l'obiettivo di fornire indicazioni sullo stack tecnologico, sulla gestione del versioning, sulle linee guida per garantire la qualità e la sicurezza del software sviluppato e sulla gestione delle consegne sul repository.

1. Ruoli e Responsabilità

Tutte le attività oggetto del presente documento sono sotto la responsabilità dell'Area Realizzazione Software all'interno del Dipartimento Software & Piattaforme.

2. Definizione stack tecnologico

Le nuove componenti dovranno essere sviluppate utilizzando lo stack tecnologico adottato da Lepida ScpA, preferendo l'utilizzo delle ultime versioni stabili delle seguenti librerie e verificando che non siano state segnalate vulnerabilità nelle versioni utilizzate:

- Java con OpenJDK;
- Building tool con Gradle;
- Spring Framework e Spring Boot
- Web framework: Apache Wicket o Angular;
- Oracle;
- Apache Tomcat;
- MyBatis;
- Bootstrap o Bootstrap Italia;
- Sentry;
- OpenAPI.

L'utilizzo di librerie non incluse nell'elenco fornito dovrà essere valutato e approvato da Lepida ScpA; Lepida ScpA predilige l'utilizzo di librerie open-source (software libero), che siano correntemente manutenute e che siano ampiamente utilizzate dalla comunità.

3. Gestione del software (versionamento, regole, etc..)

Il codice deve aderire alle convenzioni di codifica specifiche del linguaggio utilizzato. L'architettura deve essere chiara e documentata. Ogni evoluzione del codice deve essere accompagnata da una documentazione aggiornata e migliorata.

Il codice deve essere sottoposto a un sistema di controllo delle versioni (Version Control System - VCS), con commit settimanali obbligatori e una gestione precisa delle patch. Ogni bug fix deve includere i test necessari a verificare la risoluzione del problema.

4. Building, Release-notes e Tagging

Le build devono essere automatizzate e compatibili con l'infrastruttura di Lepida ScpA. Il processo di build deve includere test unitari e generare artefatti versionati (es. jar, war).

Ogni rilascio deve includere una chiara descrizione delle modifiche apportate, bug fix, e note di aggiornamento.

Ogni versione significativa del software deve essere taggata nel sistema VCS, seguita da un processo di verifica e convalida.

5. Uso di GitLab

Accesso e Permessi

- L'accesso al GitLab di Lepida avviene solo mediante VPN con credenziali LDAP
- Fornire ai fornitori esterni solo l'accesso necessario ai repository pertinenti, limitando i permessi in base al principio del privilegio minimo.
- Utilizzare gruppi e ruoli in GitLab per controllare l'accesso ai progetti e alle risorse condivise.

Branching e Workflow di Sviluppo

- Adottare una strategia di branching chiara, come *GitFlow*, per organizzare lo sviluppo. Ogni fornitore deve lavorare su branch separati e nominati in modo coerente (es. feature/nome-funzionalita).
- Utilizzare le *merge request*, verificando il codice prima dell'integrazione del codice nei branch principali.

Commit e Best Practice

- I messaggi di commit devono essere chiari e seguire uno standard predefinito (es. type: descrizione, dove type può essere fix, feat, docs, ecc.).
- I commit devono essere frequenti e rappresentare piccoli cambiamenti incrementali, per facilitare il processo di revisione e il tracciamento delle modifiche.

6. Aspetti di sicurezza

Validazione degli input

- Sanitizzazione dei dati: Tutti gli input devono essere validati e sanitizzati per evitare attacchi di tipo SQL Injection, XSS, o altre forme di injection.
- Validazione lato client e lato server: Verifica che gli input vengano validati sia lato client che lato server.
- Length validation: Limitare la lunghezza massima degli input per prevenire buffer overflow o altre vulnerabilità basate sulla lunghezza degli input.
- Gestione dei caratteri speciali: Gli input devono essere trattati correttamente in presenza di caratteri speciali come <>, ', ", ecc.
- Non esposizione dei dati sensibili in URL: Evitare di inserire informazioni sensibili o sessioni nei parametri URL, come la trasmissione di ID utente o token queste informazioni devono essere trasmesse in modo sicuro tramite POST o nell'intestazione, poiché questi possono essere salvati nei log dei server o nei browser.

- File Upload Security: Se l'applicazione prevede l'upload di file, assicurarsi che i file vengano validati (tipo MIME), limitati nella dimensione e salvati in percorsi sicuri. Implementare controlli per evitare esecuzioni di file pericolosi (es. script).

Autenticazione e Autorizzazione

- Autenticazione robusta: Utilizzare meccanismi di autenticazione sicuri come OAuth, OpenID Connect o SAML.
- Lato applicativi web dove possibile utilizzare l'autenticazione tramite FedERa.
- Autorizzazione dei ruoli: Verificare che gli utenti abbiano accesso solo alle risorse per cui sono autorizzati in base al loro ruolo.
- Scadenza delle sessioni: Implementare una scadenza di sessione per prevenire sessioni persistenti non sicure.
- Utilizzo di token sicuri: Se vengono utilizzati token per l'autenticazione o l'autorizzazione, assicurarsi che siano sufficientemente lunghi e generati in modo sicuro (es. JWT con chiave sicura).
- Token CSRF: Implementare token anti-CSRF per proteggere le sessioni degli utenti da attacchi di tipo Cross-Site Request Forgery. I token anti-CSRF devono essere unici per ogni sessione e dovrebbero essere validati sia lato client che lato server.

Crittografia

- Crittografia dei dati sensibili: I dati sensibili (come password, numeri di carte di credito) devono essere crittografati sia in transito che a riposo.
- TLS: Verificare che tutte le comunicazioni utilizzino il protocollo TLS (Transport Layer Security).
- Hash sicuro delle password: Le password devono essere memorizzate usando algoritmi di hashing sicuri come bcrypt, scrypt o Argon2.
- Non utilizzare algoritmi di crittografia deboli: Evitare l'uso di algoritmi di crittografia obsoleti o deboli come MD5 o SHA-1.
- Cookie con flag Secure: Assicurarsi che tutti i cookie contenenti informazioni sensibili o di sessione abbiano il flag Secure impostato per garantire che vengano trasmessi solo tramite connessioni HTTPS.

Gestione delle Vulnerabilità

- Aggiornamento delle dipendenze: Assicurarsi che tutte le librerie e i framework utilizzati siano aggiornati alle ultime versioni stabili.
- Scansione delle vulnerabilità: Effettuare una scansione del codice con strumenti di sicurezza per rilevare eventuali vulnerabilità conosciute.
- Rimozione di componenti non utilizzati: Rimuovere tutti i moduli, le librerie o i servizi non necessari che potrebbero rappresentare una potenziale vulnerabilità.

Logging e Monitoraggio

- Registrazione degli eventi: implementare/prevedere un sistema di logging per gli eventi significativi, come i tentativi di accesso falliti o le modifiche ai dati sensibili.
- Protezione dei log: Assicurarsi che i file di log non contengano informazioni sensibili come password.
- Monitoraggio attivo: Implementare/prevedere un sistema di monitoraggio per rilevare attività sospette in tempo reale.

Sicurezza delle API

- Autenticazione API: Utilizzare API key o meccanismi di autenticazione sicuri per proteggere l'accesso alle API.
- Rate limiting: Implementare meccanismi di rate limiting per prevenire attacchi di tipo denial-of-service (DoS).
- Accesso basato su ruoli (RBAC): Assicurarsi che le API implementino una gestione dell'accesso basata sui ruoli (Role-Based Access Control).
- Prevenzione del caching delle pagine sensibili: Impostare header HTTP adeguati per evitare che le pagine contenenti dati sensibili vengano memorizzate nella cache del browser.

Gestione degli Errori

- Messaggi di errore generici: Evitare di mostrare messaggi di errore dettagliati agli utenti finali, per non rivelare informazioni sensibili sull'infrastruttura o sull'applicazione.
- Gestione sicura delle eccezioni: Implementare una gestione sicura delle eccezioni per evitare crash o divulgazione di informazioni sensibili.

Hardening del Componente

- Disabilitazione delle funzionalità non necessarie: Disabilitare funzioni o servizi non utilizzati che potrebbero essere sfruttati per attacchi.
- Configurazioni sicure: Verificare che le configurazioni del componente siano impostate secondo le linee guida di sicurezza (ad esempio, limitare i permessi delle directory e dei file).
- Principio del privilegio minimo: Garantire che il componente operi con il minor numero di privilegi possibile.
- Secure headers: Implementare intestazioni HTTP sicure come **Content Security Policy (CSP)**, **X-Content-Type-Options**, **X-Frame-Options**, e **X-XSS-Protection** per migliorare la protezione dell'applicazione.

Sicurezza del Deployment

- Ambienti di produzione separati: Garantire che l'ambiente di produzione sia separato da quello di sviluppo e test, per evitare contaminazioni di dati o accessi indesiderati.
- Restrizioni sugli ambienti di sviluppo: Assicurarsi che gli ambienti di sviluppo e test non utilizzino dati reali o, se necessario, che questi dati siano anonimi e crittografati.

Storia del documento				
Ver.	**Autore**	**Verifica**	**Approvazione**	**Commenti**
1.0	Area Realizzazione Software	Direttore Sicurezza, Ambiente & Emergenza (31/10/2024)	Direttore Software & Piattaforme (31/10/2024)	Emissione