

SVILUPPO SOFTWARE APPLICATIVO DI GESTIONE AZIENDALE NELL'ATTUALE AMBIENTE DI FORTI DINAMICHE CYBERSECURITY ED INTELLIGENZA ARTIFICIALE

- SICUREZZA INTEGRATA ALLO SVILUPPO
- COME UTILIZZARE L'INTELLIGENZA ARTIFICIALE

Italconsulta dal 1984 sviluppa software di gestione aziendale.

Lo sviluppo del software gestionale per noi è sempre stato una parte integrata all'esperienza vissuta in azienda.

Giornate, settimane, mesi, anni di lavoro con dirigenti, impiegati ed operai trascorsi nella loro azienda osservando e analizzando i processi per sviluppare procedure più efficienti per processi consolidati o a supporto di nuovi processi.

Sappiamo dialogare con le persone che lavorano in azienda con il loro stesso linguaggio di finanza, controllo di gestione, magazzino, produzione, commerciale ecc...

Questa esperienza e sensibilità si unisce alla continua ricerca tecnologica e metodologica per selezionare i migliori componenti di un sistema.

Sin dall'inizio, massima attenzione era dedicata alla sicurezza, con particolare riferimento agli accessi (anche quando internet non esisteva ancora), ai dati inseriti nel sistema, ai crash di sistema ed al disaster recovery.

I rischi erano più stabili e lenti nella loro evoluzione, oggi l'evoluzione della situazione di rischio è enormemente più rapida e diversificata.

Occorre, quindi, un continuo processo di analisi dei rischi e introduzione delle metodologie e misure di sicurezza più avanzate nel momento in cui divengono disponibili e affidabili.

Il rapido e intenso sviluppo dell'intelligenza artificiale, che è utilizzabile sia dalle aziende ma anche dai loro potenziali attaccanti, impone inderogabilmente la gestione più aggiornata ed opportuna di questa tecnologia.

È in questo contesto che si inserisce la nostra proposta: sviluppo software su misura con sicurezza integrata sin dalla progettazione ed utilizzo intelligente dell'AI.

I POSSIBILI PERCORSI PER SVILUPPARE APPLICAZIONI SOFTWARE GESTIONALI

Un'azienda che ha l'esigenza di dotarsi di una nuova applicazione informatica gestionale per gestire uno specifico processo particolare del proprio modello di business e, quindi, fuori da standard generalizzati; ha, teoricamente, la possibilità di scegliere tra almeno 3 percorsi principali.

a. Far sviluppare l'applicazione dall'intelligenza artificiale

Utilizzare generatori di applicazioni basate su IA.

Con tali strumenti sarebbe sufficiente descrivere l'applicazione desiderata e l'AI, in tempo rapidissimo, crea l'applicazione e permette di distribuirla.

In pratica, vi sono dei problemi che sconsigliano il suddetto approccio nel caso degli sviluppi software qui considerati.

Vi è una significativa probabilità che l'architettura prodotta sia incoerente con l'ambiente software.

Frequentemente, il software presenta dei bug critici che determinano problemi di funzionamento ma anche problemi di sicurezza, come ad esempio riferimenti a pacchetti software inesistenti che un'attaccante può sfruttare per inserire codice malevolo nell'applicazione.

Elevato è il rischio di vulnerabilità; in molti casi già catalogate tra le più pericolose al mondo secondo il MITRE CWE Top 25.

A differenza di uno sviluppatore esperto, l'IA non ragiona in termini di sicurezza: genera codice, non codice sicuro.

Questo significa che le vulnerabilità non sono eccezioni isolate, ma vengono replicate su scala industriale, incorporate silenziosamente in ogni funzionalità, ogni integrazione, ogni aggiornamento.

b. Utilizzare strumenti di Low-code e No-code

Questa soluzione potrebbe funzionare bene se limitata ad essere una semplice interfaccia di gestione dati (inserimento, visualizzazione ecc.) ma, se contiene delle logiche e degli algoritmi, vi sono molte limitazioni e potenziali problemi.

Lo strumento consente di passare da un'idea a un'applicazione funzionante senza scrivere codice, ma tutta la progettazione degli algoritmi e della sicurezza rimane a carico di chi sviluppa.

Se chi usa lo strumento non sa come proteggere i dati degli utenti, come gestire i permessi di accesso o come difendersi dagli attacchi, lo strumento non segnala e non corregge: lascia semplicemente tutte le vulnerabilità aperte.

Un secondo limite riguarda la velocità e l'efficienza dell'applicazione in produzione.

Gli strumenti Low-code generano codice in modo automatico e generico, pensato per funzionare in molti contesti diversi.

Un'applicazione gestionale aziendale ha, invece, caratteristiche precise: certi processi vengono usati centinaia di volte al giorno, certi dati crescono nel tempo, certi report richiedono elaborazioni complesse.

Un codice scritto su misura da sviluppatori esperti può essere ottimizzato per queste esigenze reali.

Il codice generato automaticamente da uno strumento Low-code, invece, tende a essere ridondante e poco efficiente, con conseguenze dirette sulla lentezza dell'applicazione, sui costi di infrastruttura e sulla scalabilità nel tempo.

c. Sviluppare applicazioni predisponendo un progetto informatico e sviluppando il codice ad hoc

È la soluzione migliore quando vi è un processo aziendale particolare che deve essere supportato in modo fedele dal software gestionale per assicurare efficienza e vantaggio competitivo peculiare di una determinata attività.

Si tratta quindi di applicazioni software importanti per le quali si vuole avere: totale controllo del software, elevate prestazioni, scalabilità e integrazioni con l’ambiente gestionale generale aziendale.

Si otterrà quindi un’applicazione architetaturalmente ottimizzata, flessibile, scalabile, documentata, di elevate prestazioni e sulla quale si ha un completo controllo. Tutte le premesse utili e necessarie per la lunga vita del software a tutela dell’investimento.

In questo contesto, l'intelligenza artificiale non è esclusa ma, al contrario, è utilmente impiegata, con sicurezza ed efficienza, per l’identificazione di eventuali vulnerabilità ed ottenere un prodotto finale ai più elevati standard di sicurezza.

Strumenti di SAST (Static Application Security Testing) basati su intelligenza artificiale aiutano ad identificare eventuali vulnerabilità già durante la scrittura del codice.

Strumenti di DAST (Dynamic Application Security Testing) basati sull’intelligenza artificiale aiutano ad analizzare, in fase di test del prodotto finito, il comportamento dell’applicazione ed individuare le eventuali vulnerabilità che un attaccante potrebbe sfruttare.

MACROANALISI FUNZIONALE APPLICATIVA

Questa fase si svolge insieme al key user del cliente e degli utenti che lui vorrà eventualmente coinvolgere.

Si definiranno i risultati gestionali che dovrà produrre l'applicazione e le principali funzioni applicative.

Si procederà quindi ad identificare i principali elementi come, ad esempio, i processi aziendali coinvolti, classificare i dati trattati, definire ruoli ed autorizzazioni degli utenti con relativi criteri di sicurezza.

Nelle sessioni di analisi sarà prodotta la relativa documentazione.

MICROANALISI FUNZIONALE APPLICATIVA

Si definiscono, con il cliente, l'interfaccia utente e tutti i dettagli funzionali e di controllo come, ad esempio, input/output per ogni funzione ecc.

Particolare attenzione è dedicata alla sicurezza con definizione di autorizzazioni per ruolo, validazione input, gestione errori/eccezioni, organizzazione del logging ecc.

Nelle sessioni di analisi sarà prodotta la relativa documentazione comprendendo anche il layout dell’UI.

PROGETTAZIONE INFORMATICA APPLICATIVA

Progettazione applicazioni sicure fin dall’origine, riducendo il rischio operativo e proteggendo dati e processi aziendali.

Definizione delle funzionalità dell’applicazione e della loro interazione sia con l’utente che con le altre funzioni (casi d’uso).

Definizione autenticazione ed autorizzazioni utenti.

Threat modeling.

Applicare principi di secure design come zero-trust, minimo privilegio e configurazioni secure by default

Nelle fasi di progettazione sarà prodotta la relativa documentazione comprendendo i diagrammi architetaturali ed applicativi.

MACROANALISI INFORMATICA

In questa fase saranno scelti tutti gli elementi per realizzare efficientemente il progetto informatico definito.

Ad esempio: linguaggi e framework supportati, database, architettura a livelli (front-end / back-end / database).

Integriamo la sicurezza verificando eventuali vulnerabilità sull’architettura scelta (CVE) e definendo i dati da sottoporre a crittografia.

Nelle fasi di progettazione sarà prodotta la relativa documentazione.

MICROANALISI INFORMATICA

Definire le caratteristiche informatiche ogni particolare come, ad esempio controlli, gestione sessioni, policy password, logging e auditing.

Implementiamo la sicurezza definendo controlli contro le vulnerabilità come, ad esempio, SQL injection, XSS, CSRF ecc.

Nelle fasi di progettazione sarà prodotta la relativa documentazione.

SVILUPPO SOFTWARE SICURO

Sviluppo codice sicuro e verificabile individuando le vulnerabilità già in fase di scrittura del codice, riducendo drasticamente i rischi di attacchi futuri.

Saranno prese a riferimento le linee guida più riconosciute come, ad esempio, quelle di OWASP e NIST.

Le attività comprenderanno gestione delle chiavi/secret, code review ecc. Particolare attenzione sarà dedicata all’analisi delle vulnerabilità, incluse le eventuali dipendenze esterne, eseguita con strumenti SAST (static application security testing) basati su IA.

Saranno impiegati strumenti specializzati per le analisi svolte durante lo sviluppo e per l’analisi di vulnerabilità sulle eventuali dipendenze.

Nelle fasi di sviluppo sarà prodotta la relativa documentazione.

TEST APPLICAZIONE IN AMBIENTE DI SVILUPPO

Al termine dello sviluppo, il prodotto sarà testato per individuare errori e/o vulnerabilità prima di affidarlo al test cliente.

Saranno testati gli accessi e tutte le funzioni applicative con l’obiettivo di identificare eventuali errori.

Verifichiamo la sicurezza tramite analisi con strumenti DAST (dynamic application security testing) basati sull’AI, vulnerability scan e fuzz testing.

Al termine dell’attività il prodotto sarà consegnato in ambiente di test utente.

RILASCIO ALL’UTENTE IN AMBIENTE DI TEST

In questa fase il prodotto viene consegnato in ambiente di test all’utente affinché possa svolgere direttamente gli opportuni controlli in condizioni reali.

Sarà predisposto l’ambiente di test con implementazione di una configurazione sicura.

Sarà consegnato agli utente il manuale d’uso ed al referente tecnico del cliente la documentazione tecnica.

Vi saranno attività di formazione utenti e sarà concordato il programma di test che dovranno eseguire, inclusi scenari di sicurezza, ad esempio la prova di accedere a una funzione per cui non si è autorizzati.

La documentazione prodotta comprenderà i verbali di collaudo dove saranno descritti eventuali errori o richiesta di variazioni funzionali.

RILASCIO ALL’UTENTE IN AMBIENTE DI PRODUZIONE

La nuova applicazione software sarà integrata al sistema informatico aziendale e messa in produzione.

In questa fase potrebbe essere previsto un affiancamento all’utente per un tempo da stabilirsi per eventuali ulteriori attività di formazione o correzione.

Il supporto nel tempo è elemento che, in oltre 40 anni, Italconsulta ha sempre offerto.

IL VALORE CHE VORREMMO TRASFERIRE ALLE AZIENDE

Italconsulta nasce da una lunga storia industriale, ci è naturale quindi evidenziare che l’obiettivo non è semplicemente sviluppare software, ma costruire strumenti affidabili che supportino concretamente la crescita e l’organizzazione dell’azienda.

Con questa attitudine, dialogare con le aziende sulla digitalizzazione dei processi per aprire nuove aree di business o incrementare efficienza e competitività è attività a cui siamo sempre disponibili ed interessati.



www.italconsulta.it



Per approfondimenti:
Tel. 039 230 129 1
techline@italconsulta.it

Ed. 01 del 18/05/2026