					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P24					Titolo del documento: **Politica di sviluppo sicuro**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

1. Finalità

1.1 La presente politica definisce i requisiti di sicurezza obbligatori per le attività di sviluppo di software e sistemi all'interno dell'organizzazione, inclusi i progetti interni, lo sviluppo esternalizzato e l'integrazione di codice di terze parti.

1.2 L'obiettivo è garantire che la sicurezza sia integrata lungo l'intero ciclo di vita dello sviluppo del software (SDLC) e che le vulnerabilità siano individuate, mitigate e prevenute prima della messa in esercizio in produzione.

1.3 La presente politica supporta l'applicazione della Clausola 8.1 della ISO/IEC 27001:2022 e dei Controlli 8.25–8.28 dell'Allegato A, standardizzando la governance dello sviluppo sicuro, le pratiche di validazione del codice e la supervisione dello sviluppo affidato a terzi.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i seguenti elementi:

2.1.1 software, applicazioni, script, integrazioni e strumenti di automazione sviluppati internamente o esternamente

2.1.2 team di sviluppo, proprietari delle applicazioni, team DevOps, personale QA, architetti, project manager e collaboratori esterni

2.1.3 ambienti SDLC, inclusi sistemi di sviluppo, test, staging e preproduzione

2.1.4 componenti open source e di terze parti integrati nelle applicazioni interne

2.1.5 software distribuito on-premises, in cloud privato, in ambienti ibridi o in cloud pubblico

2.2 Tutti gli utenti e i soggetti che partecipano allo sviluppo, al test o al deployment dei sistemi nel contesto organizzativo sono soggetti alla presente politica, inclusi i fornitori di servizi gestiti e i fornitori di piattaforme.

3. Obiettivi

3.1 Integrare i controlli di sicurezza in tutte le fasi dello sviluppo software, dalla progettazione al deployment, assicurando una riduzione del rischio proattiva e continua.

3.2 Prevenire l'introduzione di vulnerabilità sfruttabili, quali difetti di injection, meccanismi di autenticazione non sicuri ed esposizione a debolezze note di terze parti.

3.3 Definire e applicare pratiche di programmazione sicura allineate a OWASP, SANS CWE e alle linee guida specifiche dei framework utilizzati.

3.4 Garantire che tutto il codice sia sottoposto a peer review, analisi automatizzata e validazione di sicurezza prima del deployment.

3.5 Gestire i rischi di sviluppo derivanti da attività esternalizzate, inclusione di codice di terze parti e riutilizzo di software open source.

3.6 Proteggere gli ambienti di sviluppo, test e staging dall'accesso non autorizzato e impedire l'uso di dati di produzione in assenza di approvato mascheramento dei dati o anonimizzazione.

3.7 Promuovere la consapevolezza in materia di sicurezza tra sviluppatori, product manager e professionisti della qualità (QA) attraverso percorsi formativi basati sui ruoli e aggiornamenti continui sui rischi emergenti.

4. Ruoli e responsabilità

4.1 Chief Information Security Officer (CISO)

4.1.1 È il titolare della politica e garantisce che i requisiti di sviluppo sicuro siano applicati a livello di tutta l'organizzazione.

4.1.2 Approva gli standard di programmazione sicura e gli accordi con terze parti per lo sviluppo.

4.1.3 Convalida le decisioni di trattamento del rischio relative a vulnerabilità irrisolte o differite.

4.2 Responsabile della sicurezza applicativa / DevSecOps Manager

4.2.1 Definisce, mantiene e promuove le linee guida di programmazione sicura.

4.2.2 Integra i test di sicurezza statici e dinamici nelle pipeline CI/CD.

4.2.3 Esegue riesami di sicurezza del codice e definisce le azioni correttive obbligatorie.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1 La presente politica deve essere riesaminata annualmente, o con maggiore frequenza in risposta a:

9.1.1 revisioni rilevanti delle metodologie di sviluppo o degli strumenti DevOps

9.1.2 incidenti di sicurezza significativi derivanti da vulnerabilità applicative

9.1.3 modifiche ai requisiti normativi relativi al software sicuro (ad es. GDPR, DORA)

9.1.4 nuovi standard di settore o informazioni sulle minacce (ad es. OWASP Top 10, SLSA, MITRE CWE)

9.2 Il riesame della politica deve essere guidato dal Responsabile della sicurezza applicativa in coordinamento con il CISO, gli architetti software, la direzione QA e il consulente legale, per gli impatti relativi al codice di terze parti.

9.3 Qualsiasi revisione deve essere registrata nel registro di controllo documentale del SGSI, sottoposta a controllo versione e comunicata ai team interessati tramite note di rilascio o formazione obbligatoria.

9.4 Le versioni legacy devono essere conservate nel repository di archiviazione per finalità di tracciabilità legale e di audit.

10. Politiche correlate e collegamenti

10.1 P1 – Politica per la sicurezza delle informazioni. Definisce il mandato strategico per integrare la sicurezza in tutti i sistemi informativi, di cui lo sviluppo sicuro costituisce un controllo operativo fondamentale.

10.2 P4 – Politica di controllo degli accessi. Definisce le misure di controllo per limitare l'accesso agli ambienti di sviluppo, ai repository, agli strumenti di build e alle pipeline CI/CD.

10.3 P5 – Politica di gestione delle modifiche. Garantisce che le modifiche al codice, i rilasci e i deployment siano soggetti ad adeguata approvazione, pianificazione del rollback e verifica successiva al deployment.

10.4 P12 – Politica di gestione degli asset. Supporta l'inventario degli ambienti di sviluppo, dei repository sorgente e dei sistemi di build quali asset gestiti soggetti a classificazione e protezione.

10.5 P22 – Politica di registrazione e monitoraggio. Si applica alle pipeline di sviluppo, garantendo che i processi di build, le promozioni del codice e gli eventi di deployment siano registrati, monitorati e analizzati per individuare anomalie di sicurezza.

10.6 P30 – Politica di risposta agli incidenti. Fornisce il quadro di riferimento per l'analisi e la risposta ai difetti di sicurezza individuati dopo il deployment o durante i test di sicurezza delle applicazioni.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Pianificazione e controllo operativi: richiede l'integrazione dei processi e dei controlli di sviluppo sicuro nelle operazioni.

11.2 ISO/IEC 27002:2022 – Controlli 8.25–8.28

11.2.1 Allegato A, Controllo 8.25 – Ciclo di vita dello sviluppo sicuro: richiede l'inclusione formale della sicurezza nella progettazione e nello sviluppo del software.

11.2.2 Allegato A, Controllo 8.26 – Requisiti di sicurezza delle applicazioni: richiede la definizione della programmazione sicura e dei criteri di accettazione della sicurezza.

11.2.3 Allegato A, Controllo 8.27 – Architettura di sistema sicura e principi di ingegneria: richiede l'applicazione dei principi di progettazione della sicurezza e la mitigazione delle debolezze note.

11.2.4 Allegato A, Controllo 8.28 – Programmazione sicura: richiede l'adozione di pratiche di codifica sicura e verifiche correlate.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 to SA-15: stabilisce pratiche strutturate di sviluppo della sicurezza applicativa, inclusi requisiti per progettazione, integrità del codice e test.

11.3.2 SI-10 – Validazione degli input informativi: riguarda le difese di programmazione sicura.

11.3.3 SR-3 – Protezione della supply chain: richiede la verifica di software, componenti e fornitori di sviluppo di terze parti.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita: richiede l'integrazione di sicurezza e privacy nello sviluppo dei sistemi.

11.4.2 Articolo 32 – Sicurezza del trattamento: supporta misure tecniche quali validazione degli input, controllo degli accessi e deployment sicuro.

11.5 Direttiva NIS2 UE (2022/2555)

11.5.1 Articolo 21(2)(e–f): richiede pratiche di sviluppo software che includano gestione delle vulnerabilità, sicurezza del codice e segnalazione degli incidenti.

11.6 DORA UE (2022/2554)

11.6.1 Articolo 9 – Gestione del rischio ICT: richiede pratiche di sviluppo sicuro per i soggetti finanziari, inclusi controlli sulla qualità del software e correzione dei difetti.

11.6.2 Articolo 10 – Continuità operativa e test: promuove test e validazione rigorosi dei sistemi ICT, incluse le applicazioni.

11.7 COBIT 2019

11.7.1 BAI03 – Gestione dell'identificazione e dello sviluppo delle soluzioni: disciplina la progettazione, lo sviluppo e l'integrazione della sicurezza nelle nuove soluzioni.

11.7.2 BAI07 – Gestione dell'accettazione del cambiamento e della transizione: garantisce deployment sicuro e valutazione successiva al deployment.

11.7.3 DSS05 – Gestire i servizi di sicurezza: applica la validazione della sicurezza al software e all'erogazione dei servizi.