					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P25					Titolo del documento: **Politica sui requisiti di sicurezza delle applicazioni**							
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**

Allineamento a standard e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	—
ISO/IEC 27002:2022	Controlli 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
Regolamento generale sulla protezione dei dati (GDPR) UE	Articoli 25, 32	—
Direttiva UE NIS2	Articoli 21(2)(f), 23	—
Regolamento UE DORA	Articoli 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Finalità

1.1 La presente politica definisce i requisiti di sicurezza applicativa obbligatori per il software sviluppato, acquisito, integrato o implementato dall'organizzazione. Essa assicura che tutte le applicazioni siano progettate, realizzate e mantenute in conformità ai principi di sviluppo sicuro, agli obblighi normativi e alla propensione al rischio dell'organizzazione.

1.2 La politica impone l'integrazione della sicurezza lungo l'intero ciclo di vita dell'applicazione, includendo l'autenticazione degli utenti, il trattamento dei dati, la protezione delle interfacce e l'interazione sicura con API o servizi.

1.3 Con l'adozione della presente politica, l'organizzazione intende prevenire l'introduzione di vulnerabilità software, proteggere i dati sensibili e garantire tracciabilità e resilienza rispetto a exploit e abusi.

2. Ambito di applicazione

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

2.1.1 applicazioni sviluppate internamente o acquisite da fonti esterne, incluse soluzioni SaaS e strumenti sviluppati su misura

2.1.2 applicazioni che supportano operazioni aziendali critiche, accesso dei clienti o trattamento di dati soggetti a regolamentazione

2.1.3 team di sviluppo, DevOps, QA, di prodotto e di sicurezza

2.1.4 sviluppatori terzi, fornitori di software e partner di integrazione con accesso alle applicazioni o alle API dell'organizzazione

2.2 Si applica in tutti gli ambienti: sviluppo, test, collaudo, produzione e ripristino di emergenza, indipendentemente dal fatto che siano ospitati on-premise, in data center privati o in ambienti cloud pubblici.

3. Obiettivi

3.1 Definire requisiti di sicurezza di base, funzionali e non funzionali, che devono essere soddisfatti da tutte le applicazioni, indipendentemente dal metodo di sviluppo o dallo stack tecnologico.

3.2 Assicurare l'integrazione di misure di protezione a livello applicativo, incluse la validazione degli input, la codifica degli output, la gestione degli errori e la sicurezza delle sessioni.

3.3 Richiedere l'implementazione sicura di meccanismi di autenticazione, autorizzazione e controllo degli accessi allineati alle politiche organizzative in materia di identità e accessi.

3.4 Imporre un'interazione sicura con API, interfacce web e componenti di terze parti tramite protocolli approvati e controlli di sicurezza.

3.5 Consentire il rilevamento tempestivo e la mitigazione delle vulnerabilità tramite analisi statica e dinamica, revisione del codice e modellazione delle minacce.

3.6 Proteggere i dati sensibili in conformità ai requisiti normativi mediante l'applicazione della cifratura, della classificazione e delle regole di conservazione.

3.7 Assicurare la validazione continua del livello di sicurezza delle applicazioni dopo il rilascio in esercizio tramite test, monitoraggio e capacità di dimostrare la conformità.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO)

4.1.1 È il titolare della politica e ne assicura l'allineamento con la strategia di sicurezza delle informazioni e la postura di rischio dell'organizzazione.

4.1.2 Approva i requisiti di sicurezza delle applicazioni e assicura l'applicazione dei controlli obbligatori nelle funzioni di sviluppo e approvvigionamento.

4.2 Responsabile della sicurezza applicativa / Responsabile DevSecOps

4.2.1 Definisce i controlli di sicurezza di base e le metodologie di test per i componenti applicativi.

4.2.2 Supervisiona l'integrazione sicura di strumenti quali SAST, DAST, IAST e SCA nella pipeline di rilascio del software.

4.2.3 Mantiene la checklist dei requisiti di sicurezza delle applicazioni e i criteri di validazione.

[... 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 divulgazioni di vulnerabilità critiche che interessano framework o dipendenze comuni

9.1.2 aggiornamenti agli obblighi normativi in materia di sicurezza applicativa, ad esempio NIS2 e DORA

9.1.3 modifiche rilevanti alle pratiche di sviluppo software, agli strumenti o all'architettura cloud dell'organizzazione

9.1.4 risultanze di audit interni o test di penetrazione esterni

9.2 Il riesame deve essere condotto dal Responsabile della sicurezza applicativa, in coordinamento con il Responsabile della sicurezza delle informazioni (CISO), l'ingegneria DevOps, la funzione legale, l'Approvvigionamento e i responsabili QA.

9.3 Tutte le revisioni devono essere sottoposte a controllo di versione nel Registro di controllo documentale del SGSI e distribuite a tutti i team di sviluppo e di prodotto interessati.

9.4 Le versioni sostituite devono essere archiviate per non meno di tre anni al fine di garantire tracciabilità, verificabilità e supporto alle indagini sulle violazioni.

10. Politiche correlate e collegamenti

10.1 P1 – Politica per la sicurezza delle informazioni. Definisce il quadro di riferimento per la protezione di sistemi e dati, nell'ambito del quale sono richiesti controlli a livello applicativo per prevenire accessi non autorizzati, perdite di dati e sfruttamento illecito.

10.2 P4 – Politica di controllo degli accessi. Definisce gli standard di gestione dell'identità e delle sessioni che devono essere applicati da tutte le applicazioni, inclusi autenticazione forte, principio del privilegio minimo e requisiti di riesame degli accessi.

10.3 P5 – Politica di gestione delle modifiche. Disciplina la promozione del codice applicativo e delle configurazioni negli ambienti di produzione, assicurando il blocco delle modifiche non autorizzate o non testate.

10.4 P17 – Politica di protezione dei dati e privacy. Richiede alle applicazioni di implementare la privacy by design e assicurare il trattamento lecito, la cifratura e la conservazione dei dati personali e sensibili in tutti gli ambienti.

10.5 P24 – Politica di sviluppo sicuro. Fornisce il quadro di riferimento più ampio per integrare la sicurezza nello SDLC, di cui la presente politica definisce i requisiti concreti e i controlli tecnici da implementare a livello applicativo.

10.6 P30 – Politica di risposta agli incidenti (P30). Impone una gestione strutturata degli incidenti di sicurezza applicativa, incluse vulnerabilità identificate dopo il rilascio o durante i test di penetrazione, e definisce procedure di escalation, contenimento e ripristino.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001:2022

11.1.1 Clausola 8.1 – Pianificazione e controllo operativi: richiede che la sicurezza applicativa sia integrata nei processi e nei sistemi per assicurare riservatezza, integrità e disponibilità (CIA).

11.2 ISO/IEC 27002:2022

11.2.1 Controlli 8.25–8.26: dettagliano le aspettative in materia di sicurezza a livello applicativo, incluse pratiche di programmazione sicura, modellazione delle minacce, controlli architetturali e validazione del software di terze parti.

11.2.2 Allegato A, Controllo 8.25 – Cicli di vita di sviluppo sicuro dei sistemi: impone l'integrazione della sicurezza lungo il ciclo di vita dell'applicazione.

11.2.3 Allegato A, Controllo 8.26 – Requisiti di sicurezza delle applicazioni: richiede la definizione e l'applicazione di controlli tecnici per proteggere le applicazioni da uso improprio e compromissione dei sistemi.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Test e valutazione della sicurezza da parte degli sviluppatori: richiede test statici, dinamici e di penetrazione durante lo sviluppo.

11.3.2 SA-15 – Processo di sviluppo, standard e strumenti: stabilisce standard formali per lo sviluppo sicuro delle applicazioni.

11.3.3 SI-10 – Validazione degli input informativi: richiede meccanismi di controllo per prevenire attacchi di injection e di parsing.

11.4 Regolamento generale sulla protezione dei dati (GDPR) UE (2016/679)

11.4.1 Articolo 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita: richiede l'integrazione della protezione dei dati e della tutela della privacy nella logica applicativa e nei flussi di lavoro.

11.4.2 Articolo 32 – Sicurezza del trattamento: richiede misure tecniche appropriate, quali validazione degli input, cifratura e controlli di accesso sicuri.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articolo 21(2)(f): richiede il trattamento delle vulnerabilità e pratiche sicure lungo il ciclo di vita delle applicazioni per i soggetti essenziali e importanti.

11.5.2 Articolo 23 – Segnalazione degli incidenti di sicurezza: richiede capacità di logging di audit e monitoraggio a livello applicativo per rilevare e segnalare incidenti significativi.

11.6 Regolamento UE DORA (2022/2554)

11.6.1 Articolo 9 – Gestione del rischio ICT: obbliga i soggetti finanziari ad assicurare che le applicazioni siano sicure, testate e resilienti rispetto alle minacce informatiche.

11.6.2 Articolo 11 – Test degli strumenti ICT: promuove test di penetrazione periodici ed esercitazioni di red teaming su applicazioni e servizi critici.

11.7 COBIT 2019

11.7.1 BAI03 – Gestione dell'identificazione e dello sviluppo delle soluzioni: stabilisce requisiti di progettazione e controllo durante lo sviluppo delle applicazioni.

11.7.2 BAI09 – Gestire le applicazioni: pone l'accento sulla manutenzione sicura, sul monitoraggio e sul miglioramento delle applicazioni in esercizio.

11.7.3 DSS05 – Gestire i servizi di sicurezza: collega la protezione delle applicazioni a operazioni e controlli di sicurezza più ampi dell'organizzazione.