

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

ESAMATIC S.R.L.

Documento S02 · Rev. 02 del 04/10/2026 · Sistema di Gestione per la Sicurezza delle Informazioni (ISMS) conforme a UNI CEI EN ISO/IEC 27001:2022, integrato con il Sistema Qualità ISO 9001:2015

ESAMATIC S.R.L., che opera nella **progettazione, sviluppo e manutenzione di software, nell'erogazione di formazione informatica e nella consulenza informatica**, riconosce che le informazioni proprie e quelle affidate dai clienti — codice sorgente, dati, credenziali, documentazione di progetto — sono un asset critico da proteggere, anche in ragione della partecipazione a **gare e forniture verso la Pubblica Amministrazione**.

La Direzione istituisce e mantiene un **Sistema di Gestione della Sicurezza delle Informazioni (ISMS)** conforme alla norma ISO/IEC 27001:2022, integrato con il Sistema di Gestione per la Qualità, impegnandosi a garantire i tre principi fondamentali della sicurezza delle informazioni:

- **Riservatezza (Confidentiality)** — le informazioni sono accessibili solo a chi è autorizzato;
- **Integrità (Integrity)** — le informazioni sono accurate, complete e protette da modifiche non autorizzate;
- **Disponibilità (Availability)** — le informazioni e i servizi sono disponibili quando servono.

Principi guida:

1. **Conformità** ai requisiti legali, contrattuali e regolamentari applicabili (GDPR/Reg. UE 2016/679, requisiti dei committenti pubblici e privati).
2. **Approccio basato sul rischio** — identificare, valutare e trattare i rischi per la sicurezza delle informazioni in modo sistematico e proporzionato (metodologia S04).
3. **Controllo degli accessi** — principio del privilegio minimo e del "need to know"; autenticazione forte (MFA) sui sistemi critici.
4. **Sviluppo sicuro** — integrare la sicurezza nell'intero ciclo di sviluppo software (secure SDLC), gestione sicura di segreti, ambienti separati, revisione del codice.
5. **Protezione dei dati dei clienti** — trattare dati, credenziali e codice dei clienti come asset ad alta criticità.
6. **Continuità** — backup, ripristino e continuità operativa per garantire la disponibilità dei servizi.
7. **Sicurezza dei fornitori** — presidiare la sicurezza dei servizi in cloud e delle terze parti (Microsoft, Cloudflare, eventuali collaboratori).
8. **Gestione degli incidenti** — rilevare, registrare, gestire e imparare dagli incidenti di sicurezza.
9. **Consapevolezza** — mantenere alta la competenza e la consapevolezza delle persone in materia di sicurezza.
10. **Miglioramento continuo** dell'ISMS mediante audit, riesami e trattamento delle non conformità.

Per attuare questa Politica, la Direzione definisce **obiettivi di sicurezza misurabili**, conduce la **valutazione del rischio** e la **Dichiarazione di Applicabilità (SoA)** dei controlli dell'Annex A, e assicura le risorse necessarie. La Politica è comunicata a tutte le persone che operano per l'organizzazione, resa disponibile alle parti interessate e riesaminata periodicamente.

Milano, 4 ottobre 2026

La Direzione ESAMATIC S.R.L. — Il Legale Rappresentante — Soldano Andrea Cesare

Documento sottoscritto con firma digitale (PAdES) dal Legale Rappresentante, ai sensi del D.Lgs. 82/2005 (CAD): data e ora di sottoscrizione sono attestate dal certificato di firma. Rev. 02 emessa il 04/10/2026; l'originale firmato è conservato tra le informazioni documentate controllate, le copie stampate non sono controllate.

Registro delle revisioni

Rev.	Data	Descrizione modifica	Redatto (RGQ)	Approvato (DIR)
00	—	Prima stesura (bozza di lavoro, non emessa)		
01	17/09/2026	Prima emissione controllata	Cesaretti Laura	Soldano Andrea Cesare
02	04/10/2026	Rilievo RGQ del 04/10 sulle intestazioni: codice S02 nell'intestazione, registro delle revisioni. Testo della politica invariato. Firmata in PAdES (la Rev. 01 era firmata in CAdES)	Cesaretti Laura	Soldano Andrea Cesare

S02 — Politica per la Sicurezza delle Informazioni — ESAMATIC S.R.L. — Rev. 02 del 04/10/2026