POL Politica del sistema di gestione

Storia della versione

Versione	Data	Autore	Approvato da
1	01/05/2026	Marco Capanna	Marco Capanna

Indice

Scopo

Rimini Informatica S.r.l. promuove, attraverso la presente politica, un modello di gestione che coniuga le esigenze di sviluppo economico e di creazione di valore, proprie della propria attività di impresa, con la tutela della sicurezza delle informazioni e dei dati, il rispetto della normativa vigente e la responsabilità sociale. Questo documento rappresenta l'espressione formale dell'impegno del vertice aziendale a favore del Sistema di Gestione Integrato (SGI) e ne costituisce il pilastro strategico: definisce i principi, gli orientamenti e gli obiettivi che guidano l'intera organizzazione nel perseguimento della qualità dei servizi erogati e nella protezione degli asset informativi.

La politica è concepita per essere appropriata al contesto in cui opera l'organizzazione e al suo modello di business, supportandone gli indirizzi strategici. In quanto espressione della missione e della visione aziendale, essa orienta le decisioni operative e gestionali verso un miglioramento continuo delle prestazioni, la soddisfazione delle esigenze dei clienti e delle altre parti interessate, nonché il pieno rispetto dei requisiti applicabili in materia di qualità e sicurezza delle informazioni. Il governo complessivo del SGI è assicurato attraverso i *PRO Processi direzionali* , che disciplinano le attività di leadership e governance del vertice aziendale. La presente politica costituisce, insieme alla *POL Politica di sicurezza delle informazioni* , il riferimento di alto livello cui si conformano tutte le procedure e i controlli del SGI. Essa incoraggia, altresì, la diffusione di una cultura del rispetto dei principi legali e delle buone prassi a tutti i livelli dell'organizzazione.

Campo di applicazione

La presente politica si applica a tutti i processi, le attività e gli asset informativi di Rimini Informatica S.r.l. presso la sede operativa di Via Pomposa 43/A, 47924 Rimini. Essa coinvolge tutto il personale, compresi dipendenti, collaboratori e terze parti che accedono alle informazioni o ai sistemi aziendali, indipendentemente dalla modalità di lavoro adottata (in sede, da remoto o presso clienti). I principi e gli impegni qui espressi si estendono all'intera gamma dei servizi offerti:

- assistenza IT
- infrastrutture di rete e connettività
- cybersecurity
- sistemi telefonici avanzati
- soluzioni di smart working
- videosorveglianza

Riferimenti normativi

- ISO 9001:2015
- ISO/IEC 27001:2022

- Regolamento (UE) 2016/679
- D.Lgs. 196/2003

Termini e definizioni

- **Alta direzione** : persona o gruppo di persone che dirigono e controllano un'organizzazione al livello più elevato.
- **Sistema di gestione** : insieme di elementi correlati o interagenti di un'organizzazione finalizzato a stabilire politiche, obiettivi e processi per conseguire tali obiettivi.
- **Politica** : intenzioni e orientamento di un'organizzazione espressi formalmente dalla sua alta direzione.
- **Obiettivo** : risultato da conseguire, che può essere strategico, tattico od operativo, riferito a diverse discipline e applicabile a differenti livelli dell'organizzazione.
- **Miglioramento continuo** : attività ricorrente finalizzata ad accrescere le prestazioni.
- **Parte interessata** : persona o organizzazione che può influenzare, essere influenzata da, o percepire di essere influenzata da una decisione o attività.
- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Rischio** : effetto dell'incertezza sugli obiettivi.
- **Informazione documentata** : informazione che deve essere tenuta sotto controllo e mantenuta da un'organizzazione, unitamente al supporto che la contiene.
- **Requisito** : esigenza o aspettativa che può essere espressa, generalmente implicita o cogente.

Ruoli e responsabilità

- **CEO** : stabilisce, approva e mantiene aggiornata la politica del SGI, assicurando la disponibilità delle risorse necessarie e promuovendo la cultura della qualità e della sicurezza delle informazioni a livello strategico.
- **Responsabile del Sistema Integrato (RSI)** : coordina le attività di governance del SGI trasversali alle norme di riferimento, verifica la coerenza complessiva tra politiche, obiettivi e processi aziendali e propone al **CEO** gli aggiornamenti della politica.
- **Responsabile del sistema di gestione** : supporta il **CEO** nella redazione e nella revisione della politica, verificandone la coerenza con gli esiti del riesame della Direzione e con le risultanze dell'analisi del contesto.
- **Tecnico sistemista** : contribuisce alla protezione degli asset informativi aziendali e alla continuità operativa dell'infrastruttura IT, in coerenza con i principi stabiliti dalla presente politica.
- **Commerciale** : raccoglie e formalizza i requisiti e le aspettative dei clienti, contribuendo ad alimentare il processo di miglioramento della qualità dei servizi.

- **Amministrativo** : cura la documentazione amministrativa e contabile nel rispetto delle procedure del SGI e segnala eventuali anomalie o non conformità riscontrate.

Impegno e obiettivi del sistema di gestione

Impegno della direzione

Rimini Informatica S.r.l. riconosce nel proprio SGI lo strumento fondamentale per garantire la qualità dei servizi IT erogati ai clienti e per proteggere il patrimonio informativo aziendale. Il **CEO** assume in prima persona la responsabilità di promuovere e sostenere il SGI, assicurando che esso resti costantemente appropriato al contesto organizzativo e allineato agli indirizzi strategici dell'azienda.

L'organizzazione si posiziona come partner tecnologico per le PMI del territorio, offrendo soluzioni integrate di infrastruttura IT, cybersecurity e telecomunicazioni. In tale contesto, la direzione si impegna a:

- perseguire la soddisfazione dei clienti attraverso servizi puntuali, affidabili e rispondenti alle esigenze concordate, con particolare attenzione alla capacità di risoluzione, alla competenza tecnica e alla qualità dell'assistenza;
- garantire la riservatezza, l'integrità e la disponibilità delle informazioni gestite, adottando un approccio sistematico basato sulla valutazione e sul trattamento dei rischi;
- soddisfare i requisiti applicabili, siano essi cogenti, normativi o contrattuali, monitorando l'evoluzione del quadro legislativo e regolamentare;
- promuovere la responsabilità condivisa in materia di sicurezza delle informazioni, coinvolgendo tutto il personale, i collaboratori e le terze parti che operano per conto dell'organizzazione;
- rendere disponibili le risorse umane, tecnologiche e finanziarie necessarie al funzionamento efficace del SGI e al raggiungimento degli obiettivi prefissati;
- favorire il miglioramento continuo del SGI, misurando l'efficacia dei controlli attraverso indicatori definiti e sottoposti a riesame periodico.

Principi fondamentali

La presente politica è ispirata a principi che guidano l'operato quotidiano di ogni persona all'interno dell'organizzazione. L'approccio basato sul rischio costituisce la lente attraverso cui vengono valutate le decisioni, in modo che probabilità e impatto dei possibili scenari orientino le scelte operative e strategiche. La protezione delle informazioni non ricade su una singola funzione, bensì è una responsabilità diffusa che coinvolge ciascun membro dell'organizzazione. Le risorse e le informazioni aziendali vengono utilizzate esclusivamente per finalità coerenti con il ruolo assegnato, nel rispetto dei livelli di classificazione stabiliti. Ogni evento o sospetto di violazione della sicurezza viene segnalato tempestivamente attraverso i canali dedicati, a tutela dell'integrità complessiva del SGI.

Obiettivi strategici

Coerentemente con l'analisi del contesto interno ed esterno, con la valutazione dei rischi e delle opportunità e con le esigenze delle parti interessate, l'organizzazione persegue i seguenti obiettivi:

- ridurre l'esposizione ai rischi che possono compromettere riservatezza, integrità e disponibilità delle informazioni, mediante un processo sistematico di valutazione e trattamento;
- rafforzare la consapevolezza e le competenze del personale attraverso attività periodiche di formazione e sensibilizzazione in materia di qualità e sicurezza;
- assicurare la conformità ai requisiti normativi, contrattuali e degli standard di riferimento, monitorando gli sviluppi legislativi e adeguando prontamente i processi aziendali;
- garantire la continuità dei servizi ai clienti, proteggendo l'infrastruttura IT e i dati da interruzioni, perdite e accessi non autorizzati;
- promuovere il miglioramento continuo del SGI, raccogliendo e analizzando dati di prestazione, esiti degli audit, risultati della soddisfazione dei clienti e indicazioni emerse dal riesame della direzione.

Ogni obiettivo trova declinazione in un programma operativo che specifica tempi, risorse, indicatori di monitoraggio e responsabilità, secondo le modalità definite nella *PRO Obiettivi e pianificazione per il loro raggiungimento* . Gli esiti della valutazione dei rischi, condotta in conformità alla *PRO Procedura di gestione dei rischi* , e le risultanze dell' *Analisi del contesto* alimentano periodicamente l'aggiornamento degli obiettivi stessi.

Comunicazione della politica

La presente politica è mantenuta come informazione documentata ed è comunicata, compresa e applicata all'interno dell'organizzazione, secondo le modalità stabilite nella *PRO Procedura gestione comunicazione* . I canali approvati per la diffusione interna sono:

- posta elettronica aziendale e PEC
- intranet e SharePoint
- piattaforme di messaggistica aziendale (Microsoft Teams o equivalenti)
- riunioni di team e sessioni formative

L'utilizzo di canali personali e non aziendali per la diffusione della politica è espressamente vietato.

La politica è altresì resa disponibile alle parti interessate esterne, ove appropriato, attraverso:

- le pagine pubbliche del sito web aziendale
- le specifiche contrattuali con i fornitori
- la sezione trasparenza dei contratti con i clienti

Il **Responsabile del Sistema Integrato (RSI)** autorizza le comunicazioni esterne che presentano impatto sulla sicurezza delle informazioni.

Archiviazione e aggiornamento

La presente politica è conservata in formato digitale sulla piattaforma documentale aziendale, protetta dalle misure di sicurezza IT gestite dal **Tecnico sistemista** , con copie di backup cifrate in almeno due sedi separate. L'eventuale copia cartacea è custodita in armadio chiuso nell'area amministrativa, accessibile al solo personale autorizzato. Le modalità di gestione delle informazioni documentate seguono quanto stabilito nella *PRO Procedura di gestione delle informazioni documentate* .

Il **Responsabile del Sistema Integrato (RSI)** verifica il documento con cadenza almeno annuale, in occasione del *PRO Gestione riesame della direzione* , oppure quando intervengono cambiamenti significativi nel contesto organizzativo, tecnologico, nel panorama delle minacce o nel quadro normativo di riferimento. Il **Responsabile del sistema di gestione** supporta la revisione e ne cura la coerenza con gli esiti del riesame e dell'analisi del contesto. Ogni aggiornamento è sottoposto all'approvazione del **CEO** prima della pubblicazione, registrato con numero di revisione progressivo, data e sintesi delle modifiche apportate. Le versioni superate sono contrassegnate come sostituite e rese non accessibili come riferimento operativo corrente, ma conservate a fini di consultazione storica.

Documenti di riferimento

- PRO Processi direzionali
- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Procedura di gestione dei rischi
- POL Politica di sicurezza delle informazioni
- PRO Procedura gestione comunicazione
- PRO Gestione riesame della direzione
- Analisi del contesto
- PRO Procedura di gestione delle informazioni documentate