REGESTA GROUP

1. Scopo

La presente Politica del Sistema di Gestione della Sicurezza delle Informazioni (di seguito "Politica") definisce i principi, gli obiettivi e gli indirizzi generali adottati dal Gruppo, composto da Regesta S.p.A., Regesta LAB, Regesta Group e Ultrafab, per garantire la protezione delle informazioni in conformità al requisito 5.2 della norma ISO/IEC 27001:2022.
La Politica è redatta per essere resa disponibile e comprensibile alle parti interessate interne ed esterne al Gruppo.

2. Ambito di applicazione

La Politica si applica a:

- tutte le società del Gruppo che aderiscono alla certificazione, ovvero Regesta SpA, Regesta Group, Regesta LAB e Ultrafab;
- tutti i dipendenti, collaboratori, consulenti, fornitori e altre parti terze che trattano informazioni per conto del Gruppo;
- tutte le informazioni, indipendentemente dalla forma (digitale, cartacea, verbale) e dal supporto;
- tutti i sistemi informativi, infrastrutture tecnologiche, applicazioni e processi aziendali.

3. Contesto organizzativo

Il Gruppo opera attraverso società con ruoli e responsabilità differenti ma fortemente interconnessi:

- **Regesta S.p.A.**: implementazione di sistemi gestionali, con particolare riferimento a soluzioni SAP;
- **Regesta LAB**: servizi di consulenza, sviluppo software, BI, CPM, AI, data analytics e data management;
- **Regesta Group**: gestione dei processi aziendali di amministrazione, back office commerciale, schedulazione funzionale, marketing e People;
- **Ultrafab**: progettazione, sviluppo e industrializzazione di prodotti software, inclusi sistemi che trattano e integrano dati dei clienti verso SAP e altre applicazioni dipartimentali.

Questa eterogeneità richiede un approccio coordinato e coerente alla sicurezza delle informazioni, basato su principi comuni e adattabile alle specificità operative di ciascuna società.

4. Obiettivi della sicurezza delle informazioni

Gli obiettivi principali della sicurezza delle informazioni del Gruppo sono:

- garantire **riservatezza**, **integrità** e **disponibilità** delle informazioni;
- proteggere i dati dei clienti, inclusi dati di produzione, amministrativi e di business;
- supportare la continuità operativa e l'affidabilità dei servizi e dei prodotti software;
- rispettare i requisiti contrattuali, normativi e regolamentari applicabili;
- ridurre i rischi di sicurezza delle informazioni a un livello accettabile.

5. Impegno della Direzione

La Direzione del Gruppo dimostra un impegno attivo e continuo nello sviluppo, nell'attuazione, nel mantenimento e nel miglioramento del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

In particolare, la Direzione si impegna a:

- garantire che il SGSI sia conforme a tutti i **requisiti applicabili**, inclusi quelli della norma ISO/IEC 27001:2022, i requisiti legali e regolamentari e gli obblighi contrattuali;
- definire e approvare obiettivi di sicurezza delle informazioni coerenti con gli indirizzi strategici del Gruppo;
- assicurare la disponibilità delle **risorse necessarie** (organizzative, tecnologiche ed economiche) per l'efficace funzionamento del SGSI;
- promuovere una cultura aziendale orientata alla sicurezza delle informazioni, supportando iniziative di formazione e sensibilizzazione;
- integrare i requisiti del SGSI nei processi aziendali e decisionali del Gruppo;
- sostenere il miglioramento continuo del SGSI attraverso il riesame periodico delle sue prestazioni.

6. Principi di riferimento

Il Gruppo adotta i seguenti principi fondamentali:

- **Approccio basato sul rischio**: le misure di sicurezza sono definite in funzione dei rischi identificati;
- **Responsabilità condivisa**: la sicurezza delle informazioni è responsabilità di tutte le persone che operano per il Gruppo;
- **Proporzionalità**: i controlli di sicurezza sono adeguati al valore delle informazioni e all'impatto potenziale;
- **Miglioramento continuo**: il sistema di gestione della sicurezza delle informazioni è soggetto a revisione e miglioramento costante.

7. Ruoli e responsabilità

- La **Direzione del Gruppo** approva la presente Politica e ne supporta l'attuazione.
- Le **Direzioni delle singole società** assicurano l'applicazione della Politica nei rispettivi ambiti.
- Il team **Responsabile del Sistema di Gestione** per la sicurezza delle informazioni definisce linee guida, controlli, strumenti comuni e ne verifica l'attuazione riportando direttamente alla Direzione del Gruppo
- Tutti i **dipendenti e collaboratori** sono tenuti a conoscere e rispettare la Politica e le procedure correlate.

8. Gestione delle informazioni e dei dati

Il Gruppo si impegna a:

- classificare le informazioni in base alla loro criticità e sensibilità;
- proteggere i dati dei clienti lungo l'intero ciclo di vita, inclusa la raccolta, l'elaborazione, l'integrazione, la conservazione e la dismissione;

- adottare misure tecniche e organizzative adeguate per i sistemi SAP, le piattaforme di data analytics, i prodotti software e le infrastrutture di supporto;
- garantire che l'accesso alle informazioni sia consentito solo a soggetti autorizzati.

9. Conformità e requisiti normativi

Il Gruppo si impegna a rispettare:

- la norma ISO/IEC 27001:2022;
- le leggi e i regolamenti applicabili in materia di protezione dei dati e sicurezza delle informazioni;
- gli obblighi contrattuali assunti con clienti e partner.

10. Comunicazione e consapevolezza

La Politica è comunicata a tutte le parti interessate rilevanti. Il Gruppo promuove attività di formazione e sensibilizzazione per garantire un adeguato livello di consapevolezza sulla sicurezza delle informazioni.

11. Riesame e aggiornamento

La presente Politica è riesaminata periodicamente e aggiornata in caso di cambiamenti organizzativi, tecnologici, normativi o a seguito di incidenti significativi di sicurezza delle informazioni.

12. Approvazione

La Politica di Sicurezza delle Informazioni è approvata dalla Direzione del Gruppo ed entra in vigore dalla data della sua pubblicazione.