



Politica di sicurezza delle informazioni

Questa politica si applica a tutte le informazioni gestite da Redion Italy Insurance S.p.A., Redion Italy Services S.p.A., Redion S.A., Sucursal en España, Redion Spain Integrated Services, S.A.U., Redion S.A., Sucursal em Portugal (di seguito Regione Mediterranea di Redion), ai relativi sistemi e servizi, nonché a dipendenti, collaboratori e terze parti che accedono a tali risorse.

Lo scopo di questa politica è proteggere gli asset informativi garantendone la riservatezza, l'integrità e la disponibilità, nonché la conformità ai requisiti legali, regolamentari e contrattuali applicabili.

Gli obiettivi sono definiti e aggiornati in funzione degli interessi di tutti gli stakeholder (quali il Gruppo Generali, i clienti, le parti terze e tutti i soggetti che hanno interesse nella gestione sicura dei dati di Redion) e in base alle priorità individuate mediante la gestione continua dei rischi di sicurezza.

Il framework ISO/IEC 27001 è utilizzato come riferimento per la definizione, il mantenimento e il riesame degli obiettivi di sicurezza delle informazioni.

Gli obiettivi di sicurezza delle informazioni sono monitorati e riesaminati periodicamente nell'ambito del riesame di direzione del Sistema di Gestione della Sicurezza delle Informazioni (ISMS).

I principali obiettivi di sicurezza delle informazioni sono:

- Proteggere le informazioni da accessi, utilizzi, divulgazioni, modifiche o distruzioni non autorizzate.
- Garantire la continuità dei servizi essenziali e minimizzare l'impatto degli incidenti di sicurezza.
- Gestire i rischi di sicurezza delle informazioni attraverso un approccio sistematico basato sulla ISO/IEC 27001.
- Promuovere la consapevolezza e la responsabilità in materia di sicurezza tra tutto il personale.

Impegno della Direzione e Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

Il Top Management delle società appartenenti alla Regione Mediterranea di Redion si impegna a mantenere e migliorare continuamente un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO/IEC 27001, fornendo le risorse necessarie e promuovendo una cultura della sicurezza all'interno dell'organizzazione.

Il Top Management si impegna inoltre a:

- Rispettare tutte le normative applicabili (ad esempio in materia di protezione dei dati, cybersecurity di settore e contratti con clienti e fornitori).
- Riesaminare periodicamente la presente policy, gli obiettivi di sicurezza e le prestazioni del SGSI.
- Integrare la gestione dei rischi di sicurezza delle informazioni nei principali processi aziendali.



Aree di interesse della Sicurezza delle Informazioni

Il SGSI di Redion copre un ampio insieme di ambiti necessari a garantire un adeguato livello di maturità della sicurezza all'interno dell'organizzazione. I processi relativi a tali ambiti sono definiti in specifiche policy e procedure. Le aree di sicurezza coperte dal SGSI includono:

- a) Sicurezza IT
- b) Cyber Security
- c) Sicurezza Fisica
- d) Sicurezza aziendale (Corporate)

Ruoli e responsabilità

La responsabilità ultima della sicurezza delle informazioni spetta al Top Management, che delega l'implementazione e il coordinamento del SGSI all'Information Security Manager (CISO/ISM o figura equivalente). Strutture dedicate sono incaricate di specifiche responsabilità, in conformità ai regolamenti interni definiti e approvati dalle società appartenenti alla Regione Mediterranea di Redion. In termini generali:

- L'organo di amministrazione, gestione o controllo (AMSB) locale è responsabile della gestione dei rischi di sicurezza a livello di organizzazione, garantendo l'implementazione degli obiettivi di Sicurezza del Gruppo.
- Il Security Officer è responsabile del monitoraggio dell'attuazione degli obiettivi di Sicurezza del Gruppo all'interno dei processi di sicurezza interni dell'organizzazione. Inoltre, la funzione Security è responsabile della reportistica verso il Top Management.
- Tutto il personale è responsabile del rispetto della presente policy e di tutte le normative interne definite sui temi della sicurezza, nonché della segnalazione di qualsiasi incidente o sospetta violazione della sicurezza secondo i canali definiti.
- Tutti i dipartimenti devono garantire che le procedure interne siano allineate alla presente policy, alle normative interne sui temi della sicurezza e al SGSI.
- Fornitori e terze parti che trattano informazioni appartenenti alle società della Regione Mediterranea di Redion devono rispettare requisiti contrattuali e di sicurezza equivalenti.

Gestione degli Incidenti e comunicazioni

Redion dispone di procedure per la gestione degli incidenti di sicurezza delle informazioni, che includono le attività di rilevazione, registrazione, analisi, risposta e notifica, ove prevista.

Ogni dipendente o collaboratore deve segnalare immediatamente qualsiasi incidente effettivo o sospetto attraverso i canali designati (ad esempio service desk o team di sicurezza), al fine di ridurre l'impatto e prevenirne il ripetersi.



Conformità e riesame

La mancata conformità alla presente policy può comportare l'adozione di misure disciplinari o contrattuali, in conformità ai regolamenti interni e alla normativa applicabile.

La presente Information Security Policy è comunicata a tutto il personale e resa disponibile alle parti interessate rilevanti attraverso adeguati canali di comunicazione interna.

La presente Information Security Policy è riesaminata almeno una volta all'anno o ogniqualvolta intervengano cambiamenti significativi nel contesto, nei rischi, nella normativa applicabile o nell'ambito di applicazione del SGSI.

Approvazione

La presente policy è stata approvata dal Top Management ed è efficace a partire dalla data sottoindicata.

25.09.2026

Approvata dal CEO