RINA GROUP
POLITICA

POLITICA DI SECURITY

Revisione	Data	Redazione	Controllo		Approvazione
0	26/07/2022	PSL	PSL	FSU	USN
1	21/11/2022	PSL	PSL		USN

La “Politica di Security” ha lo scopo di:

1. stabilire i principi generali di azione per assicurare un adeguato livello di sicurezza e protezione di persone e asset (“security fisica”), dati e informazioni (“information security”) da minacce derivanti da situazioni e comportamenti avversi endogeni ed esogeni;
2. confermare il proprio impegno nel proteggere costantemente le persone e i beni aziendali (asset, dati e informazioni) nel rispetto della normativa vigente;
3. delineare un modello di security omogeneo e integrato – che tutte le società del Gruppo RINA sono chiamate a implementare - atto a garantire la riduzione del rischio che si verifichino eventi negativi, minimizzando probabilità e impatto, e un’efficiente gestione e un adeguato coordinamento delle crisi, nel caso si verifichino.

A tal fine, RINA svolge le seguenti attività di security:

a) la valutazione preventiva dei rischi di security per le persone e i beni aziendali, sulla base di metodologie di valutazione del rischio riconosciute, predefinite e non soggette alla discrezionalità dei singoli, al fine di individuare e attuare idonee misure di mitigazione;

b) la gestione della security nel rispetto delle norme internazionali e nazionali applicabili e dei più alti standard di riferimento, tra cui la Dichiarazione sui Diritti Umani e i Principi Volontari sulla Sicurezza e i Diritti Umani; a dimostrazione di ciò, RINA ha adottato il Modello di Organizzazione e Gestione ed il contestuale Codice Etico;

c) l’adozione di un programma di gestione del rischio di viaggio, che includa la valutazione dei rischi di security dei viaggiatori anche in aree a rischio e i criteri per l’adozione di protocolli di security atti a minimizzarli;

d) la gestione della information security, per minimizzare le violazioni della riservatezza, dell’integrità e della disponibilità dei dati, dovuti ad azioni avverse endogene ed esogene;

e) business intelligence e third party due diligence per effettuare, in ottemperanza al Codice Etico, e nei soli casi previsti dalle procedure interne di RINA, verifiche informative su persone fisiche e giuridiche al fine di valutarne l’affidabilità;

f) un programma di protezione del CEO e dei vertici aziendali di RINA per garantire continuità nella gestione e nell’indirizzo strategico dell’azienda;

g) la promozione di una cultura della security attraverso i mezzi di comunicazione interni e attività formative dedicate;

h) la promozione a tutti i livelli del monitoraggio e della gestione dei rischi di security.

Relativamente alla information security, RINA adotta un sistema di gestione certificato secondo lo standard ISO 27001, con i seguenti obiettivi specifici:

i. proteggere i beni aziendali garantendo la riservatezza, l’integrità e la disponibilità delle informazioni e dei sistemi attraverso cui esse sono gestite;

ii. garantire il rispetto delle norme nazionali e internazionali applicabili e dei più alti standard di riferimento;

iii. valutare i rischi inerenti relativi alla information security e gestire i rischi residui a seguito delle misure di mitigazione e controllo adottate per ridurre i rischi ad un livello “As Low As Reasonably Practicable” (ALARP);

iv. garantire la continuità operativa aziendale attraverso iniziative volte al miglioramento della resilienza e un’efficace gestione degli incidenti;

v. perseguire il miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni riesaminandone periodicamente l’adeguatezza e l’efficacia mediante attività interne di controllo e verifiche condotte da enti esterni accreditati.

Il presente documento si applica a tutte le controllate di RINA S.p.A., nei limiti stabiliti dalla legge.

La presente Politica è sottoposta a revisione almeno triennale e ogniqualvolta ritenuto necessario, al fine di assicurare che la gestione dei rischi di security sia efficacemente applicata all’interno dell’organizzazione.

Ugo Salerno

Presidente e Amministratore Delegato