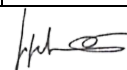


Politica Sistema di Gestione sulla Sicurezza delle Informazioni (SGSI)

Revisione	Data	Motivo della revisione	Elaborato	Verificato	Approvato
00	26/01/2026	Prima emissione	RSGSI 	RSGSI 	Direzione
					KOSTELIA srl P. Iva: 05461800483



INDICE

1.	POLITICA SGSI.....	2
----	--------------------	---

1. POLITICA SGSI

o Informativo Aziendale rappresenta la risorsa principale per gestire correttamente le relazioni con i Clienti, per pianificare l'innovazione continua dell'offerta e garantire la qualità del servizio erogato da KOSTELIA alla propria clientela nell'ambito delle attività oggetto della sua mission e del suo core business come tali, esse devono essere adeguatamente tutelati con un costante bilanciamento tra il livello di rischio accettato ed il corrispondente grado di protezione richiesto, coniugando correttamente l'esigenza di tutela del valore delle informazioni di compliance con la necessità di assicurare l'efficienza, l'efficacia e la continuità dei processi di business..

A tal proposito KOSTELIA ha quindi deciso l'implementazione del SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) modellato sulla base dello standard ISO/IEC 27001.

L'approccio metodologico adottato dall'Azienda, che si fonda sull'impianto normativo internazionale ISO/IEC 27000, comprende:

- ☐ La Norma ISO/IEC 27001 che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.
- ☐ Le Linee guida ISO/IEC 27002 che costituiscono una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO/IEC 27001 al fine di proteggere le risorse informative.

Col fine di governare la Sicurezza del Patrimonio Informativo aziendale nel rispetto e sulla base di standard riconosciuti, metodologie consolidate, obbligazioni contrattuali, Leggi e Regolamenti, richieste cogenti derivanti da audit di terze parti e operazioni di due diligence considerano i seguenti obiettivi di carattere generale:

- Coinvolgere tutto il personale interno nella realizzazione e nel mantenimento del Sistema di Gestione sulla Sicurezza delle Informazioni (SGSI), mediante continua e crescente sensibilizzazione sulle problematiche legate alla tutela dei dati, alla salvaguardia delle informazioni e alla soddisfazione dei Clienti/Committenti, agli impatti Ambientali delle operazioni e delle infrastrutture digitali, alla garanzia di un adeguato livello di Sicurezza delle Informazioni trattate sia di proprietà dell'Organizzazione stessa che di Clienti, Fornitori e Partner.
- Assicurare che le proprie attività siano svolte in conformità alla legislazione vigente, in tutti gli ambiti in cui deve operare, oltre che ai requisiti e alle procedure interne.

- Preservare al meglio l'immagine dell'Azienda, quale fornitore puntuale, affidabile, competente e sicuro quanto alla gestione dei dati e delle informazioni che le sono affidate.

Per raggiungere questi obiettivi, l'organizzazione di KOSTELIA ritiene indispensabile:

- L'applicazione di tecniche e metodologie proprie del Sistema di Gestione sulla Sicurezza delle Informazioni inteso come mezzo per gestire in forma controllata tutte le attività svolte nei processi coinvolti.
- L'organica e chiara definizione dei compiti e responsabilità di tutto il personale impiegato in tutti i processi operativi dell'Azienda ed il coinvolgimento attivo, proattivo e partecipativo degli stessi nelle procedure di monitoraggio e controllo.
- L'attiva sorveglianza e controllo operativo sul loro svolgimento e l'efficace comunicazione delle informazioni necessarie al loro coordinamento.
- La promozione della formazione tecnica e professionale dei dipendenti con il fine di rendere sempre maggiore l'Efficienza dei Servizi erogati nel rispetto della normativa vigente e delle prescrizioni della Norma ISO/IEC 27001.
- L'utilizzo di tecniche e criteri nello svolgimento di tutte delle attività affinché siano garantite la Segretezza/Riservatezza, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi; l'Integrità, ovvero la proprietà dell'informazione di essere modificata esclusivamente da chi ne possiede i privilegi; la Disponibilità, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.
- La completa e precisa identificazione dei pericoli nella valutazione dei rischi per la Sicurezza delle Informazioni di chiunque possa essere collegato direttamente o indirettamente con le realizzazioni dell'impresa.
- La continua formazione e informazione a tutti i dipendenti sensibilizzandoli e istruendoli relativamente ad un corretto approccio nello svolgimento delle proprie attività lavorative, con il fine di prevenire il possibile insorgere di rischi in merito alla gestione dei dati e delle informazioni proprie e di terzi.

Insieme agli obiettivi di carattere generale, precedentemente citati, il Management definisce anno per anno gli obiettivi specifici e misurabili che possono, riferirsi ad aspetti particolari.

L'Organizzazione con sistematicità ed imparzialità effettuerà degli Audit interni sul Sistema di Gestione della Sicurezza delle Informazioni (SGSI) al fine di verificarne l'efficacia nel raggiungere gli obiettivi, e pianificherà eventuali Azioni Correttive e/o di Miglioramento.



Il Management di KOSTELIA si impegna infine a riesaminare regolarmente la propria Politica, per accertarsi che permanga idonea all'attività e alla propria capacità di soddisfare i propri Clienti, Fornitori, Partner e tutte le altre parti interessate.

Nella consapevolezza che tali obiettivi siano raggiungibili solo con la piena partecipazione di tutti, il Management chiede la collaborazione attiva dei dipendenti, dei collaboratori e di tutte le parti interessate e si impegna a far sì che la presente politica sia diffusa, compresa e attuata non solo dal personale interno, ma anche da stagisti, collaboratori esterni, consulenti, fornitori sotto contratto, con particolare attenzione agli outsourcer che siano in qualsiasi modo coinvolti con le informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni.

La direzione di KOSTELIA si impegna infine a riesaminare regolarmente la politica ed eventuali modifiche che la influenzino, per accertarsi che permanga idonea all'attività e alla capacità aziendale di soddisfare i Clienti, i Fornitori e le altre parti interessate.