



**SGI – Sistema di Gestione Integrato**  
**ISO/IEC 27001:2013 - UNI EN ISO9001:2015**

**Politica per la Sicurezza delle**  
**Informazioni e la Protezione**  
**dei Dati Personali,**  
**e per la Qualità**

Curata da: Direzione Gerico Security Srl  
Direzione Gerico Lab Srl

Data: 08/07/2023

Ver. 4.0

Classificazione: Pubblico

| Versione | Data       | Note esplicative   |
|----------|------------|--|
| 1.0      | 27/09/2019 | Prima emissione per il SGSI                                    |
| 1.1      | 19/11/2021 | Correzioni editoriali  |
| 1.2      | 31/03/2022 | Revisione aspetti dati personali                               |
| 2.0      | 12/04/2022 | Integrazione quale SGI della Politica di Qualità e Politica SI |
| 3.0      | 07/06/2023 | Estensione SGI a Gerico Lab Srl                                |
| 4.0      | 08/07/2023 | Revisione politiche SGI  |

## Sommario

|  |          |
|--|----------|
| <b>1 SCOPO</b> .....   | <b>3</b> |
| <b>2 PRINCIPI DEL SISTEMA DI GESTIONE INTEGRATO</b> .....      | <b>3</b> |
| 2.1 OBIETTIVI DEL SISTEMA DI GESTIONE.....                     | 4        |
| <b>3 REALIZZAZIONE DEL SISTEMA DI GESTIONE INTEGRATO</b> ..... | <b>6</b> |
| <b>4 POLITICHE E PROTEZIONE DELLA DOCUMENTAZIONE</b> .....     | <b>6</b> |
| 4.1 REVISIONE .....  | 6        |

## 1 SCOPO

Gerico Security Srl e Gerico Lab Srl definiscono le proprie politiche per la sicurezza delle informazioni e per la qualità in conformità alle norme ISO/IEC 27001:2013 e UNI EN ISO9001:2015 nel rispetto del proprio Codice Etico. Gerico Security Srl e Gerico Lab Srl attuano tali politiche secondo principi di sviluppo sostenibile, efficacia, efficienza e qualità dei processi interni e delle attività erogate ai propri clienti.

## 2 PRINCIPI DEL SISTEMA DI GESTIONE INTEGRATO

Gerico Security ha stabilito un Sistema di Gestione Integrato (SGI) che ricomprende tutte le politiche applicate dall'azienda negli aspetti rilevanti di erogazione e gestione delle attività interne e verso i clienti. In particolare, si elencano e si integrano tra di loro le politiche relative a:

- Sicurezza delle Informazioni
- Qualità
- Salute e Sicurezza del Lavoro secondo quanto previsto sia dalla normativa cogente sia in termini di welfare aziendale,
- Parità di Genere,
- Sostenibilità Ambientale ed Efficienza Energetica.

Il Sistema di Gestione Integrato su tutte le sopracitate Politiche permette di garantire l'osservanza delle disposizioni del Codice Etico di Gruppo (disponibile alle parti interessate tramite il sito aziendale).

Il Sistema di Gestione Integrato è esteso e fatto proprio sia dalla capogruppo Gerico Security Srl sia dalle Società da essa controllate, con il fine di garantire l'osservanza delle disposizioni del Codice Etico di Gruppo, la qualità dei servizi erogati e la protezione da eventuali minacce il proprio patrimonio informativo, quello dei propri clienti e di tutti i soggetti interessati con i quali le Società interagiscono a vario titolo.

Date le attività svolte per i clienti, alcuni aspetti di queste politiche sono da questi ultimi ritenuti particolarmente rilevanti, e pertanto sono stati sottoposti a valutazione e monitoraggio terzo tramite apposita certificazione internazionale. In particolare, sono stati certificati i processi del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) secondo lo standard internazionale ISO/IEC27001 e di Qualità (SGQ) secondo quanto previsto dallo standard internazionale ISO 9001.

La presente Politica riguarda i due sopracitati Sistemi di Gestione per gli aspetti relativi alla Sicurezza delle Informazioni e Qualità.

Gerico Security Srl e Gerico Lab Srl, sulla base dei propri obiettivi strategici e in coerenza con il Codice Etico, considerano la qualità e la sicurezza dei processi aziendali e dei servizi erogati ai clienti come elementi di primaria importanza e si impegnano per il loro

raggiungimento e miglioramento continuo anche attraverso il Sistema di Gestione Integrato per la Sicurezza delle Informazioni e per la Qualità.

Mediante un costante processo di analisi del rischio, Gerico Security Srl assicura la protezione delle risorse informative delle società del Gruppo, in base alla sensibilità delle informazioni, la loro disponibilità in caso di necessità, e la salvaguardia da accesso o modifica non autorizzate, nonché dei potenziali impatti agli interessati per quanto concerne i dati personali secondo il principio di Accountability ex art 5.2 GDPR.

Gerico Security Srl e Gerico lab Srl assicurano altresì che tutte le proprie risorse a livello di personale, le informazioni, i sistemi e le infrastrutture garantiscano la riservatezza, l'integrità e la disponibilità delle informazioni e la protezione dei dati personali nello svolgimento dei propri servizi, attraverso specifici controlli atti anche a soddisfare i requisiti normativi e cogenti attinenti alla sicurezza delle informazioni e alla tutela dei dati personali.

La Direzione aziendale delle singole Società del Gruppo assicura il proprio impegno per il miglioramento costante della Gestione della Sicurezza delle Informazioni e della Qualità, nonché il rispetto delle leggi vigenti e del Codice Etico.

## 2.1 Obiettivi del Sistema di Gestione

Gerico Security Srl e Gerico Lab Srl hanno stabilito e mantengono un SGI – Sistema di Gestione Integrato - in conformità alle norme ISO/IEC 27001:2013 e UNI EN ISO 9001:2015. Gli obiettivi del Sistema di Gestione sono:

### A. In merito alla sicurezza delle informazioni

- Proteggere le informazioni aziendali e dei clienti acquisite, trattate o generate nell'ambito dei servizi erogati, salvaguardando la loro riservatezza, l'integrità e la disponibilità.
- Garantire il corretto accesso alle giuste informazioni quando necessario e prevenire l'accesso non autorizzato, sia da parte di chi opera in Gerico Security Srl e/o in Gerico Lab Srl, sia di chi opera per proprio conto o in Partnership.
- Delineare e mettere in atto misure di sicurezza dell'ambito definito dell'SGI, per proteggere le informazioni da infrazioni, uso improprio e frodi.
- Definire ruoli e responsabilità interni ed esterni per la sicurezza delle informazioni.
- Supportare il personale e i collaboratori con un'adeguata istruzione e formazione per sensibilizzare in materia di sicurezza informatica al fine di minimizzare i rischi e diffondere la cultura della sicurezza e della protezione per i dati personali e per le informazioni
- Garantire la continuità della sicurezza delle informazioni in caso di scenario sfavorevole o qualora si concretizzi una minaccia.

- Garantire l’ottemperanza alla norma ISO/IEC 27001:2013.
- Mantenere l’osservanza delle disposizioni contrattuali, legislative e regolamentari, in particolare sulla protezione delle informazioni e dei dati personali trattati dall’organizzazione.

#### B. In merito alla Qualità

- Adottare ed implementare i principi e le buone pratiche riconosciute per garantire la Qualità dei processi aziendali, dei servizi erogati e promuovere l’acquisizione di certificazioni di conformità agli standard di riferimento.
- Stabilire un Sistema di Gestione Integrato garantendo la conformità ai requisiti UNI EN ISO 9001:2015, per garantire il diritto dei clienti al miglior servizio possibile basato su processi di qualità.
- Individuare ruoli e responsabilità, da assegnarsi al proprio organico, indipendentemente dal livello gerarchico occupato, coinvolgendo anche i soggetti terzi che svolgono incarichi chiave.
- Assegnare le risorse necessarie al fine di assicurare l’impiego di misure idonee per gli aspetti riguardanti la qualità dei processi interni e dei servizi alla clientela.
- Promuovere continuamente il Sistema di Gestione Integrato, anche mediante un impegno costante degli Organi e dei Soggetti apicali.
- Individuare, documentare ed applicare regole che disciplinano le modalità di erogazione dei servizi secondo principi etici e di costante miglioramento.
- Sviluppare un programma di consapevolezza per il personale, mediante sessioni informative e formative periodiche.
- Predisporre adeguate misure di reazione e gestione a fronte del verificarsi di eventi che possono compromettere la qualità dei processi aziendali e della qualità dei servizi offerti alla clientela.
- Mantenere l’osservanza delle disposizioni contrattuali, legislative e regolamentari sia nei processi interni che nelle attività per i clienti.
- Selezionare e promuovere lo sviluppo dei fornitori secondo i principi del Codice Etico e di questa politica impegnandoli a mantenere comportamenti coerenti con essi.
- Impegnarsi a svolgere un processo continuo di miglioramento ed evoluzione del Sistema di Gestione Integrato, pianificando, eseguendo, verificando e attuando con continuità misure ed accorgimenti atti al contrasto di potenziali eventi che possano compromettere la Qualità nei processi e servizi alla clientela.

### **3 REALIZZAZIONE DEL SISTEMA DI GESTIONE INTEGRATO**

Il SGI – Sistema di Gestione Integrato comprende tutte le politiche e le procedure messe in atto per il raggiungimento degli obiettivi della Sicurezza delle Informazioni, della Qualità e la Protezione dei Dati Personali.

L'ambito dell'SGI comprende tutte le attività e i processi riguardanti le attività operative erogate, quelle amministrative e di supporto.

L'osservanza della presente politica sulla sicurezza delle informazioni e della Qualità è obbligatoria per tutti i soci, dipendenti, collaboratori, fornitori, appaltatori, partner e parti esterne che gestiscono informazioni di Gerico Security Srl, Gerico Lab Srl o dei loro clienti. Il Consiglio di Amministrazione di Gerico Security Srl e di Gerico Lab Srl è direttamente responsabile dell'attuazione della politica e dell'osservanza della stessa da parte di tutte le parti interessate.

Il Consiglio di Amministrazione condivide i principi e gli obiettivi dell'SGI e ne sostiene pienamente la realizzazione e il mantenimento, fornendo le risorse necessarie a tale scopo. Il Consiglio di Amministrazione delle singole Società approva ed emette la presente Politica per la Sicurezza delle Informazioni, la Protezione dei Dati Personali e la Qualità, la quale costituisce il documento programmatico di riferimento per tutti gli altri documenti del SGI, la comunica e la rende disponibile a tutte le parti interessate per quanto ritenuto necessario.

### **4 POLITICHE E PROTEZIONE DELLA DOCUMENTAZIONE**

Gerico Security Srl e Gerico Lab Srl hanno definito, approvato, pubblicato e comunicato ai dipendenti e alle parti interessate la presente politica e la necessaria documentazione interna regolante la sicurezza delle informazioni, la protezione dei dati personali e la qualità. La presente politica viene resa disponibile alle parti interessate tramite la sua pubblicazione sul sito WEB istituzionale. La documentazione del sistema di gestione, per quanto condivisibile con terze parti, è a disposizione su richiesta.

Inoltre, Gerico Security Srl, congiuntamente con Gerico Lab Srl, produce periodicamente una documentazione volta a monitorare e tener traccia dello stato dell'SGI, della Qualità ed efficacia delle performance, del livello di conformità agli standard, alla legislazione, alla regolamentazione e alla normativa contrattuale e operativa.

#### **4.1 Revisione**

La presente politica è soggetta a revisioni su base periodica e/o in caso di cambiamenti significativi riguardanti la sicurezza delle informazioni e la protezione dei dati personali al fine di garantirne l'idoneità, l'adeguatezza e l'efficienza nonché il rispetto delle normative volontarie e cogenti di riferimento.

03-SGI

Politica per la Sicurezza delle Informazioni e per la Qualità



Monza, 08/07/2023

**GeRiCO Security Srl**

**Gerico Lab Srl**