## 1. Premessa

La Direzione ha adottato un Sistema di Gestione Integrato che comprende:

- Qualità dei servizi
- Sicurezza delle informazioni
- Continuità operativa
- Gestione dei servizi IT
- Tutela ambientale

in conformità alle seguenti normative:
UNI EN ISO 9001
UNI EN ISO 14001
UNI EN ISO 22301
UNI CEI ISO/IEC 27001
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27035-1
ISO/IEC 20000-1

Genesys Informatica s.r.l. opera, inoltre, in conformità alla Regolamento Europeo 679/16 (GDPR) alla Direttiva NIS2 e al Regolamento UE 2024/2690, i cui requisiti sono trattati in modo specifico nei paragrafi successivi.

## 2. Linee strategiche

Genesys Informatica s.r.l. orienta le proprie attività ed i propri obiettivi secondo le seguenti linee strategiche:

- garantire continuità e affidabilità dei servizi, con elevati livelli di disponibilità;
- proteggere i dati e le informazioni, assicurandone riservatezza, integrità e disponibilità;
- mantenere l'infrastruttura tecnologica aggiornata, sicura e ad alte prestazioni;
- fornire un servizio di assistenza efficiente, rapido e orientato al cliente;
- assicurare la conformità alle normative applicabili, incluse quelle sulla protezione dei dati personali;
- ridurre l'impatto ambientale e promuovere soluzioni sostenibili;
- migliorare continuamente le performance aziendali e i sistemi di gestione.

## 3. Impegni della Direzione

La Direzione si impegna a:

- mantenere un Sistema di Gestione Integrato efficace e coerente con l'organizzazione;
- utilizzare in modo efficiente risorse umane e tecnologiche;
- sviluppare le competenze del personale attraverso formazione continua;
- monitorare costantemente processi, servizi e livelli di soddisfazione del cliente;
- gestire tempestivamente criticità, incidenti e reclami;
- proteggere i dati personali nel rispetto della normativa vigente (GDPR);
- promuovere comportamenti responsabili in ambito ambientale (riduzione consumi, riciclo, limitazione stampe);
- coinvolgere fornitori e partner nel rispetto di standard etici, di sicurezza e sostenibilità.

## 4. Gestione operativa del sistema

Il Sistema di Gestione Integrato si basa su:

- definizione e monitoraggio degli obiettivi;
- controllo dei processi e delle prestazioni;
- gestione delle non conformità e dei reclami;
- monitoraggio dell'affidabilità dei sistemi e delle infrastrutture;
- applicazione e verifica dei piani di continuità operativa;
- formazione e coinvolgimento del personale;
- utilizzo di sistemi informativi aggiornati ed efficienti.

## 5. Gestione dei Sistemi Informativi

In conformità alla ISO/IEC 20000-1, l'organizzazione:

- sviluppa e mantiene l'infrastruttura tecnologica adeguata al supporto di tutti i processi aziendali;
- garantisce i livelli di servizio concordati;
- garantisce la conformità dei Sistemi Informativi agli standard di sicurezza aziendali ed il monitoraggio continuo dei sistemi.

## 6. Gestione degli incidenti di sicurezza

In conformità alla ISO/IEC 27035-1, l'organizzazione:

- adotta procedure strutturate per la gestione degli incidenti;
- forma personale specializzato per rilevazione e gestione degli incidenti;
- forma personale specializzato per l'analisi degli incidenti al fine di prevenire il loro ripetersi;
- svolge attività di "lesson learned" a seguito della risoluzione di incidenti;

- collabora con soggetti esterni specializzati in cybersecurity;
- effettua regolarmente l'analisi del grado di rischio e dell'impatto sull'operatività derivante da incidenti e/o vulnerabilità rilevate.

## 7. Gestione del rischio

L'organizzazione adotta un processo strutturato di gestione del rischio, in conformità alle normative ISO/IEC 27001 e ISO 22301 integrato con i requisiti del Regolamento UE 2024/2690, per monitorare periodicamente, identificare, valutare e trattare i rischi relativi alla sicurezza delle informazioni, alla continuità operativa, alla disponibilità dei servizi essenziali e alle dipendenze critiche da terze parti.

## 8. Requisiti specifici NIS2

### 8.1 Ruoli e responsabilità

La Direzione assegna ruoli e responsabilità specifiche per la gestione della sicurezza dei sistemi di rete e informazione, tra cui:

• Responsabile del Sistema di Gestione Integrato (RGSI)
• Responsabile della Protezione dei Dati (DPO)
• Responsabile della Sicurezza delle Informazioni (CISO o equivalente)
• Responsabile della Gestione degli Incidenti
• Responsabile della Continuità Operativa
• Responsabile della Gestione della Supply Chain

Tali ruoli garantiscono l'attuazione delle misure previste dal Regolamento UE 2024/2690

### 8.2 Gestione del rischio

Genesys Informatica s.r.l. garantisce la gestione strutturata degli incidenti di sicurezza, assicurando la rilevazione tempestiva, la risposta coordinata e la comunicazione verso le autorità competenti secondo i tempi e le modalità previste dalla Direttiva NIS2 e dal Regolamento UE 2024/2690.

### 8.3 Continuità operativa e resilienza (rafforzamento)

Genesys Informatica s.r.l. assicura la resilienza dei servizi essenziali attraverso misure tecniche e organizzative adeguate, inclusa la ridondanza dei sistemi critici, la capacità di ripristino in tempi definiti e la verifica periodica dei piani di continuità operativa.

### 8.4 Sicurezza della supply chain

Genesys Informatica s.r.l. valuta e gestisce i rischi derivanti dalla supply chain, assicurando che fornitori e partner rispettino requisiti di sicurezza equivalenti ai

propri. Sono adottate procedure di qualifica, monitoraggio e revisione periodica dei fornitori critici.

### 8.5 Formazione e consapevolezza

Tutto il personale è formato e sensibilizzato sui requisiti della Direttiva NIS2, sulle procedure interne di sicurezza e sulla corretta gestione degli eventuali incidenti informatici

## 9. Obiettivi

Durante il “Riesame della Direzione” saranno definiti gli obiettivi per il miglioramento che l’organizzazione intende perseguire. Tali obiettivi saranno registrati nel “Piano di Miglioramento” o allegati al “Verbale di Riesame”, e dovranno concretizzare le indicazioni del presente documento.
La Direzione ha nominato il Responsabile Sistema di Gestione Integrato (RSGI) come suo rappresentante che ha l'autorità per:

a) assicurare che sia istituito, applicato e mantenuto attivo conforme alla norma UNI EN ISO 9001, UNI EN ISO 14001 UNI CEI ISO/IEC 27001 e UNI EN ISO 22301; ed in conformità alle ISO/IEC 27017; ISO/IEC 27018; ISO IEC 27035-1 ISO IEC 2000-1, ed a quanto indicato dal DLGS 138/24 (NIS2) e reg. eu 2690:24
b) riferire sull'andamento del SGI al fine di permetterne il riesame ed il miglioramento.

Data : 20/03/26 La Direzione