



MANUALE DI GESTIONE INTEGRATO

**POLITICA SISTEMA GESTIONE
INTEGRATO**

Codice: MAGI_A 02

Redatto da: RGSi

Approvato da: DIR

Grado di riservatezza: Pubblico

Ver. 25.11.2024

Sommario

1. Mandato e impegno.....	2
2. Politica del sistema di gestione integrato	3
3. Politiche del SGI.....	4
Politica per la sicurezza delle informazioni	4
Obiettivi e misurazione	4
Requisiti di sicurezza delle informazioni	5
Controlli di sicurezza delle informazioni	5
Business continuity	5
4. Responsabilità	5
5. Comunicazione delle politiche del SGI	6
6. Supporto per l'attuazione del SGI.....	6

1. Mandato e impegno

L'adozione di un sistema di gestione integrato per la qualità, la sicurezza delle informazioni, la privacy e l'anticorruzione è una decisione del CDA, assunta in base alla visione delle strategie dell'organizzazione.

La scelta di adottare le Norme UNI EN ISO 9001, UNI CEI EN ISO/IEC 27001, UNI ISO 37001 è stata fatta per consentire a tutte le parti interessate di mantenere la fiducia nella struttura, garantendo il controllo del servizio, la corretta gestione delle attività, il miglioramento continuo e l'attenzione agli aspetti ambientali e ai cambiamenti climatici.

Attraverso la definizione della Politica del sistema di gestione integrato, il CDA esprime la volontà dei membri di informare e coinvolgere tutto il personale e, per quanto appropriato, le altre parti interessate, nell'attuazione del SGI adottato e nel raggiungimento degli obiettivi fissati.

Di seguito si riassumono gli impegni che il CDA si assume per dare concretezza al proprio mandato e gli strumenti e relative informazioni documentate di cui il CDA si avvarrà per realizzare ciascun impegno.

IMPEGNO	STRUMENTI A SUPPORTO
Assicurare che le Politiche e gli obiettivi del SGI siano stabiliti in modo adeguato.	<ul style="list-style-type: none"> • Politica del sistema di gestione integrato; • Riesame della Direzione; • Azioni di mitigazione dei rischi.
Assicurare un'adeguata integrazione dei processi del SGI nei processi di business dell'organizzazione.	<ul style="list-style-type: none"> • Attività di formazione e consapevolezza; • Attribuzione di adeguati ruoli, responsabilità e autorità.
Rendere disponibili adeguate risorse per il SGI.	<ul style="list-style-type: none"> • Azioni di mitigazione dei rischi; • Piani di miglioramento del SGI.
Comunicare l'importanza dell'efficacia del SGI e del conformarsi ai relativi requisiti	<ul style="list-style-type: none"> • Attività di formazione e consapevolezza.
Assicurare che il SGI raggiunga gli obiettivi stabiliti.	<ul style="list-style-type: none"> • Monitoraggio, misurazione e analisi delle azioni di mitigazione dei rischi.
Dirigere e supportare il personale nel contribuire all'efficacia del SGI.	<ul style="list-style-type: none"> • Attività di formazione e consapevolezza.
Promuovere il miglioramento continuo e la mitigazione degli impatti relativi ai cambiamenti climatici.	<ul style="list-style-type: none"> • Attività di formazione e consapevolezza • Piani di miglioramento del SGI.
Supportare i responsabili di processo nel consolidamento della leadership nelle attività di loro pertinenza.	<ul style="list-style-type: none"> • Convocazioni riunioni periodiche di pianificazione e comunicazione risultati.

2. Politica del sistema di gestione integrato

Il CDA consapevole dell'importanza dell'immagine dell'organizzazione nell'ambito dei clienti di riferimento e puntando al raggiungimento degli obiettivi qualitativi, di sicurezza delle informazioni, di tutela della privacy e di sostenibilità della governance ed ambientale nella gestione dei processi e nell'erogazione dei servizi, intende mantenere attivo e migliorare continuamente il proprio SGI in conformità alle norme UNI EN ISO 9001, UNI CEI EN ISO/IEC 27001, UNI ISO 37001 unitamente all'obiettivo di gestire con efficienza ed efficacia l'organizzazione e garantendone la continuità.

Evolve intende mantenere il controllo attraverso la verifica e il raggiungimento degli obiettivi fissati relativi a:

- Gestione delle risorse e della formazione;
- Gestione Clienti;
- Progettazione;
- Approvvigionamento e gestione fornitori;
- Analisi dei rischi;
- Realizzazione dei servizi;
- Controllo di gestione, qualità e sicurezza delle Informazioni.

Nel perseguire tali fini il CDA intende:

- Valorizzare le attitudini di ciascun componente dell'organizzazione e provvedere alla loro costante formazione e aggiornamento professionale;
- Garantire le risorse necessarie al funzionamento e al mantenimento del SGI;
- Favorire lo sviluppo tecnologico dell'intera organizzazione;
- Garantire ai propri clienti e alle parti interessate la riservatezza, l'integrità, la disponibilità delle informazioni, la tutela della privacy e la mitigazione degli impatti ambientali;
- Incrementare la cultura della qualità e della sicurezza delle Informazioni;
- Motivare e responsabilizzare il personale affinché contribuisca al raggiungimento degli obiettivi dell'organizzazione;
- Soddisfare il cliente individuandone le esigenze e fornendo adeguate risposte;
- Garantire il rispetto dei tempi programmati per la realizzazione dei progetti e dei servizi;
- Coinvolgere i fornitori strategici nell'erogazione di servizi di qualità, nel rispetto degli SLA e nella sensibilizzazione alla sostenibilità ambientale;
- Minimizzare i rischi strategici e operativi mediante l'implementazione di opportune azioni di mitigazione dei rischi;

- Informatizzare i processi e standardizzare le modalità operative al fine di ridurre gli errori degli operatori;
- Dare vita a un meccanismo di miglioramento continuo, il cui significato fondamentale sia di finalizzare l'attività di tutti gli addetti alla progressiva eliminazione degli errori, degli incidenti, delle imperfezioni e delle inefficienze;
- Migliorare i processi di realizzazione al fine di ridurre i tempi di evasione del servizio;
- Garantire il monitoraggio e l'aggiornamento tempestivo dei processi di erogazione a seguito di modifiche esterne e interne;
- Recepire, esaminare e valutare le esigenze e le aspettative di tutte le parti interessate (clienti, fornitori, personale, ecc.) in modo da garantirne sempre un'adeguata "risposta".

3. Politiche del SGI

Politica per la sicurezza delle informazioni

Obiettivi e misurazione

Gli obiettivi generali del SGI sono i seguenti:

- Rispettare i requisiti contrattuali, cogenti e normativi;
- Aumentare la consapevolezza dei collaboratori e delle parti sui rischi nella sicurezza delle informazioni;
- Aiutare la Direzione nella definizione delle strategie aziendali;
- Aumentare il valore aziendale e proteggere il patrimonio;
- Limitare o annullare i danni causati da incidenti;
- Attuare tutte le modalità operative a garanzia per il mantenimento a lungo termine dei documenti affidati dai clienti per la conservazione digitale.

DIR è responsabile della revisione degli obiettivi esistenti per la sicurezza delle informazioni e della definizione di nuovi obiettivi.

Gli obiettivi dei controlli o gruppi di controlli di sicurezza sono proposti da RSGI e approvati da DIR mediante lo strumento **SGSI**. Tali obiettivi sono riesaminati almeno una volta all'anno valutandone l'attuazione e il raggiungimento.

DIR, con la collaborazione di RSGI, è responsabile delle metodologie di valutazione degli obiettivi. Almeno una volta l'anno RSGI, rivaluta i risultati del funzionamento del SGI e li sottopone a DIR in occasione del Riesame della Direzione.

Requisiti di sicurezza delle informazioni

La politica e il SGSI sono conformi agli obblighi contrattuali e ai requisiti legali e normativi rilevanti per l'organizzazione per la sicurezza delle informazioni.

L'elenco dettagliato dei requisiti contrattuali e legali è definito nell'elenco **Documenti di origine esterna** riportato nella Wiki.

In qualsiasi caso i requisiti legali e normativi e gli obblighi contrattuali verso i clienti prevalgono sulle indicazioni riportate all'interno di questa documentazione e sulla gestione del SGSI.

Controlli di sicurezza delle informazioni

La selezione dei controlli di sicurezza è definita sulla base della valutazione dei rischi e della metodologia di trattamento. I controlli selezionati e il loro stato di attuazione sono elencati nella dichiarazione di applicabilità **SGSI**.

Business continuity

La gestione della continuità operativa è descritta in **PBC - Politica di Business continuity** e in **PCO – Piano di continuità operativa**.

4. Responsabilità

Le responsabilità sono le seguenti:

- Il CDA definisce le politiche per il SGI;
- DIR garantisce la disponibilità delle risorse necessarie per l'applicazione del SGI;
- RSGI è responsabile dell'applicazione e del mantenimento del SGI;
- RSGI con il supporto di DIR, è responsabile del coordinamento operativo del SGI, nonché della valutazione delle prestazioni del SGI;
- DIR deve rivalutare il SGI almeno una volta l'anno o ogni volta che si verifichi un cambiamento significativo nella struttura organizzativa, nei processi o nella tecnologia;
- Il Riesame della Direzione stabilisce l'idoneità, l'adeguatezza e l'efficacia del SGI;
- I possessori degli asset hanno la responsabilità di proteggere l'integrità, la disponibilità e la riservatezza delle informazioni e degli asset;
- Gli incidenti relativi alla sicurezza o i punti deboli del sistema devono essere sempre comunicati ai responsabili tramite Easy Redmine;
- DIR con la collaborazione di RIU pianifica e attua programmi di formazione sulla sicurezza delle informazioni e di sensibilizzazione dei collaboratori;
- I responsabili dei servizi devono garantire il corretto funzionamento del sistema e il rispetto degli standard stabiliti.

5. Comunicazione delle politiche del SGI

Il CDA garantisce che i collaboratori e le parti interessate siano consapevoli delle politiche specificate in questo documento, della Mission pubblicata nel sito web aziendale e delle pratiche per il SGI.

La presente politica del SGI è pubblicata sul sito web aziendale, al fine di renderla disponibile alle parti interessate.

6. Supporto per l'attuazione del SGI

Con la presente il CDA dichiara che l'attuazione del SGI e il miglioramento continuo saranno sostenuti con risorse adeguate al fine di raggiungere gli obiettivi fissati nella presente politica.

Al fine di perseguire gli obiettivi prefissati il CDA si impegna a:

- Sostenere, diffondere e rendere comprensibile la Politica per la qualità e la sicurezza delle informazioni mettendo a disposizione del personale la documentazione informativa e promuovendo azioni mirate di formazione e di coinvolgimento.
- Comunicare, per quanto appropriato, tale politica alle parti interessate;
- Definire gli obiettivi per ciascun processo mettendo a disposizione le competenze e le risorse per il loro raggiungimento;
- Riesaminare sistematicamente la politica e gli obiettivi del SGI e i rischi connessi al loro raggiungimento e qualora necessario definire nuovi obiettivi e modificare le azioni intraprese per la riduzione del rischio di insuccesso.