Pubblico

POL Politica del sistema di gestione

Storia della versione

Versione	Data	Autore	Approvato da
1	28/04/2026	Glauco Timoteo	William Palozzo

Indice

Scopo

DG Impianti Industriali S.p.A., società di ingegneria multidisciplinare specializzata nella progettazione e costruzione di impianti industriali nei settori dell'energia, oil & gas, petrolchimico e farmaceutico, riconosce che la protezione del proprio patrimonio informativo e la gestione responsabile dei propri processi sono elementi imprescindibili per il raggiungimento degli obiettivi strategici e la creazione di valore sostenibile.

La presente politica esprime l'impegno formale dell'Alta Direzione a istituire, attuare, mantenere e migliorare continuamente un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO 27001, che sia appropriato al contesto organizzativo, al modello di business e agli indirizzi strategici dell'azienda. Essa integra le esigenze di sviluppo economico con la salvaguardia delle informazioni, il rispetto della normativa vigente e la diffusione di una cultura fondata sulla legalità, sulla responsabilità condivisa e sull'etica professionale.

Questo documento costituisce il riferimento primario per la definizione degli obiettivi di sicurezza delle informazioni e per l'orientamento di tutte le politiche operative, le procedure e le istruzioni del Sistema di Gestione.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi, i sistemi tecnologici e le sedi di DG Impianti Industriali S.p.A., con riferimento all'erogazione di servizi di ingegneria multidisciplinare per la progettazione (pre-FEED e FEED), costruzione, project management e manutenzione di impianti industriali. Essa coinvolge tutto il personale — dipendenti, collaboratori e terze parti — che accede alle informazioni o ai sistemi aziendali, indipendentemente dalla sede di lavoro o dalla modalità operativa, incluse le attività presso cantieri e in regime di lavoro remoto.

Le sedi interessate comprendono la sede legale di Milano (Via Napo Torriani n. 22) e la sede operativa di Montesilvano (Via Antonio Vivaldi n. 4), nonché ogni altro sito temporaneo in cui l'organizzazione opera.

Riferimenti normativi

- **ISO/IEC 27001:2022** — Sistemi di gestione della sicurezza delle informazioni — Requisiti
- **Regolamento (UE) 2016/679 (GDPR)** — Protezione delle persone fisiche con riguardo al trattamento dei dati personali
- **D.Lgs. 231/2001** — Disciplina della responsabilità amministrativa delle persone giuridiche

Termini e definizioni

- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI):** L'insieme di politiche, processi, procedure e controlli adottati dall'organizzazione per gestire in modo sistematico la sicurezza delle informazioni.
- **Riservatezza:** La proprietà per cui le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità:** La proprietà di salvaguardare l'accuratezza e la completezza delle informazioni e dei relativi metodi di elaborazione.
- **Disponibilità:** La proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.
- **Parte interessata (stakeholder):** Persona od organizzazione che può influenzare, essere influenzata da, o percepirsi come influenzata da una decisione o attività dell'organizzazione.
- **Rischio per la sicurezza delle informazioni:** Effetto dell'incertezza sugli obiettivi di sicurezza delle informazioni, espresso come combinazione della probabilità di un evento e delle sue conseguenze.
- **Miglioramento continuo:** Attività ricorrente finalizzata ad accrescere le prestazioni del Sistema di Gestione nel tempo.

Ruoli e responsabilità

- **Chief Executive Officer:** Approva la presente politica, garantisce la disponibilità delle risorse necessarie per il SGSI e promuove la cultura della sicurezza delle informazioni a tutti i livelli dell'organizzazione.
- **Managing Director:** Supervisiona l'attuazione degli indirizzi strategici definiti nella presente politica, assicurando che le operazioni quotidiane siano coerenti con gli impegni dichiarati.
- **ICT-RSGSI:** Gestisce l'infrastruttura ICT e sovrintende all'implementazione dei controlli tecnici di sicurezza delle informazioni, assicurando la disponibilità, l'integrità e la riservatezza dei dati e dei sistemi aziendali.
- **HSEQ:** Contribuisce all'integrazione dei requisiti di sicurezza delle informazioni con quelli di salute, sicurezza, ambiente e qualità, garantendo coerenza nei processi di audit e di gestione dei rischi trasversali.
- **Tutto il personale, collaboratori e terze parti:** Sono tenuti a comprendere e rispettare la presente politica, a partecipare attivamente alla protezione degli asset informativi e a segnalare tempestivamente qualsiasi evento o anomalia di sicurezza.

Impegno e obiettivi del sistema di gestione

Mission e Vision

DG Impianti Industriali S.p.A. ha come missione quella di fornire soluzioni ingegneristiche multidisciplinari ad alto valore aggiunto nei settori dell'energia, oil & gas, petrolchimico e

farmaceutico, operando con competenza, affidabilità e integrità al servizio di partner pubblici e privati, in Italia e all'estero. La visione dell'organizzazione è quella di affermarsi come punto di riferimento nel panorama dell'engineering e del contracting industriale, guidando l'innovazione nei settori della transizione energetica — biocarburanti, idrogeno, eolico, termovalorizzazione — e creando valore duraturo per tutte le parti interessate.

Impegno dell'Alta Direzione

L'Alta Direzione si impegna formalmente a:

- Garantire che la presente politica sia appropriata allo scopo e al contesto dell'organizzazione e ne supporti gli indirizzi strategici.
- Fornire le risorse umane, finanziarie e tecnologiche necessarie per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo del SGSI.
- Soddisfare i requisiti applicabili in materia di sicurezza delle informazioni, siano essi di natura legislativa, regolamentare, contrattuale o derivanti dalle aspettative delle parti interessate rilevanti.
- Promuovere il miglioramento continuo del Sistema di Gestione, attraverso la definizione di obiettivi misurabili, il riesame periodico delle prestazioni e l'attuazione tempestiva di azioni correttive.
- Diffondere a tutti i livelli aziendali la consapevolezza dell'importanza della sicurezza delle informazioni, sostenendo programmi di formazione e sensibilizzazione.
- Assicurare che la presente politica sia comunicata all'interno dell'organizzazione e resa disponibile alle parti interessate, ove opportuno.

Obiettivi del sistema di gestione

Gli obiettivi strategici del Sistema di Gestione sono articolati nelle seguenti aree:

- **Protezione degli asset informativi:** Salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni aziendali, dei dati di progetto e delle informazioni sensibili dei clienti e dei partner, applicando un approccio basato sul rischio e il principio di difesa in profondità.
- **Conformità normativa e contrattuale:** Garantire il pieno rispetto delle disposizioni legislative e regolamentari applicabili, degli obblighi contrattuali verso i clienti e dei requisiti della norma ISO 27001, mantenendo aggiornato il quadro delle prescrizioni cogenti.
- **Resilienza operativa e continuità del business:** Assicurare la capacità dell'organizzazione di prevenire, rispondere e ripristinare le proprie funzioni critiche a fronte di incidenti di sicurezza, eventi avversi o situazioni di emergenza, minimizzando l'impatto sulle operazioni e sui clienti.
- **Cultura della sicurezza e responsabilità condivisa:** Promuovere in ogni membro del personale la piena consapevolezza del proprio ruolo nella protezione delle informazioni, attraverso formazione continua, comunicazione efficace e l'adozione di comportamenti conformi alle policy aziendali.

- **Gestione proattiva del rischio:** Identificare, valutare e trattare sistematicamente i rischi e le opportunità per la sicurezza delle informazioni, assicurando che le risorse siano allocate in modo prioritario e proporzionato alla criticità delle minacce individuate.
- **Miglioramento continuo:** Perseguire l'incremento costante dell'efficacia del SGSI attraverso il monitoraggio degli indicatori di prestazione, l'analisi degli esiti degli audit interni, il riesame della direzione e l'attuazione delle lezioni apprese.

Gli obiettivi specifici e misurabili, con l'indicazione delle azioni, delle risorse, dei responsabili e delle tempistiche, sono formalizzati nel programma di miglioramento e riesaminati periodicamente dall'Alta Direzione in sede di riesame.

Principi fondamentali

La presente politica si fonda sui seguenti principi, che orientano ogni decisione e attività nell'ambito del Sistema di Gestione:

- **Approccio basato sul rischio:** Ogni decisione in materia di sicurezza delle informazioni deriva da un'analisi formale delle minacce e delle vulnerabilità, secondo la metodologia definita nella *PRO Procedura di gestione dei rischi* , al fine di implementare controlli proporzionati ed efficaci.
- **Minimo privilegio e necessità di sapere:** L'accesso alle informazioni e ai sistemi è concesso esclusivamente nella misura strettamente necessaria allo svolgimento delle mansioni assegnate, come disciplinato nella *PRO Procedura di gestione e controllo degli accessi logici* .
- **Sicurezza integrata (security-by-design):** La sicurezza delle informazioni è considerata fin dalla fase di progettazione di nuovi processi, sistemi e servizi, e non come un intervento a posteriori.
- **Difesa in profondità:** L'organizzazione implementa più livelli di controlli — tecnologici, fisici e procedurali — in modo che il cedimento di una singola misura non comprometta la protezione complessiva degli asset.
- **Responsabilità e trasparenza:** Ogni ruolo aziendale è associato a responsabilità chiare in materia di sicurezza delle informazioni, come definito nella *POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni* . L'organizzazione promuove la trasparenza nella comunicazione verso le parti interessate.
- **Legalità e conformità:** L'organizzazione si impegna al rispetto della normativa vigente e incoraggia una cultura dell'etica e della conformità, in coerenza con il *Codice di condotta* aziendale.

Archiviazione e aggiornamento

La presente politica è conservata in formato digitale controllato e resa accessibile a tutto il personale attraverso i canali di comunicazione interni dell'organizzazione. La versione vigente è quella approvata dall'Alta Direzione e pubblicata dal Responsabile del Sistema di Gestione, che ne cura la distribuzione e l'aggiornamento secondo le modalità stabilite nella *PRO Procedura di gestione delle informazioni documentate* .

Il riesame della politica è effettuato con cadenza almeno annuale in sede di riesame della direzione, e ogni qualvolta si verifichino cambiamenti significativi nel contesto organizzativo, tecnologico, normativo o nel panorama delle minacce. A seguito del riesame, il Responsabile del Sistema di Gestione sottopone le eventuali proposte di modifica all'approvazione del Chief Executive Officer e provvede alla comunicazione delle variazioni a tutto il personale e, ove opportuno, alle parti interessate esterne.

Documenti di riferimento

- Analisi del contesto
- Codice di condotta
- POL Politica di sicurezza delle informazioni
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di sicurezza operativa
- POL Politica di conservazione e cancellazione delle informazioni
- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Processi direzionali
- PRO Gestione riesame della direzione
- PRO Gestione audit interni
- PRO Procedura delle misurazioni e del monitoraggio