Pubblico

POL Politica di sicurezza delle informazioni

Storia della versione

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

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Obiettivi di sicurezza delle informazioni
- Principi fondamentali di sicurezza delle informazioni
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente politica dichiara e formalizza l'impegno del Top Management di DG Impianti Industriali S.p.A. verso la protezione degli asset informativi dell'organizzazione. In qualità di documento quadro al vertice del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), essa stabilisce il riferimento strategico per istituire, attuare, mantenere e migliorare continuamente il sistema stesso, al fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni. Il documento enuncia i principi fondamentali che guidano tutte le politiche specifiche e le procedure operative di sicurezza, assicurando che la protezione delle informazioni sia allineata agli obiettivi strategici aziendali e alle esigenze dei clienti e dei partner operanti nei settori dell'energia, oil & gas, petrolchimico e farmaceutico. La presente politica costituisce altresì il quadro di riferimento per la definizione degli obiettivi di sicurezza delle informazioni e per l'adozione di un approccio sistematico basato sulla gestione del rischio.

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., compresa la sede legale di Via Napo Torriani n.22, Milano, e la sede operativa di Via Antonio Vivaldi n.4, Montesilvano (PE), nonché i siti temporanei di cantiere e le postazioni di lavoro da remoto. Essa coinvolge tutto il personale dell'organizzazione — dipendenti, collaboratori a contratto e dirigenti — nonché le terze parti, quali fornitori, appaltatori, consulenti e partner contrattuali, che accedono alle informazioni o ai sistemi aziendali, indipendentemente dalla loro ubicazione geografica. Ogni soggetto rientrante nel campo di applicazione deve conformarsi ai principi e alle disposizioni qui contenuti.

Riferimenti normativi

- **ISO 27001:2022:** Requisiti per i sistemi di gestione della sicurezza delle informazioni.
- **ISO 27002:2022:** Linee guida per i controlli di sicurezza delle informazioni.
- **Regolamento (UE) 2016/679 (GDPR):** Protezione delle persone fisiche con riguardo al trattamento dei dati personali.
- **D.Lgs. 196/2003:** Codice in materia di protezione dei dati personali e successive modifiche.

Termini e definizioni

- **Sicurezza delle Informazioni:** La tutela della riservatezza, integrità e disponibilità delle informazioni.
- **Riservatezza:** La proprietà per cui le informazioni non vengono 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 metodi di elaborazione.
- **Disponibilità:** La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.
- **SGSI (Sistema di Gestione della Sicurezza delle Informazioni):** L'approccio sistematico dell'organizzazione, basato sul rischio aziendale, per stabilire, implementare, operare, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni.
- **Asset informativo:** Qualsiasi informazione o risorsa ad essa associata che abbia valore per l'organizzazione, inclusi dati di progetto, proprietà intellettuale, sistemi informativi e infrastrutture tecnologiche.
- **Rischio per la sicurezza delle informazioni:** Potenziale che una data minaccia sfrutti le vulnerabilità di un asset o di un gruppo di asset, causando un danno all'organizzazione.
- **Top Management:** Persona o gruppo di persone che dirige e controlla l'organizzazione al livello più alto; in DG Impianti Industriali S.p.A. è costituito dal Chief Executive Officer e dal Managing Director.

Ruoli e responsabilità

- **Chief Executive Officer** : Approva la presente politica e le politiche specifiche per argomento, garantisce la disponibilità delle risorse umane, tecnologiche ed economiche necessarie per il SGSI e assicura l'integrazione dei requisiti di sicurezza delle informazioni negli indirizzi strategici dell'organizzazione.
- **Managing Director** : Supervisiona l'attuazione operativa delle misure di sicurezza delle informazioni, nomina formalmente il RSGSI e promuove una cultura della sicurezza a tutti i livelli aziendali.
- **ICT-RSGSI** : Assicura che il SGSI sia stabilito, attuato e mantenuto in conformità alla norma ISO 27001, coordina la valutazione del rischio informatico e la gestione degli incidenti, riferisce al Top Management sulle prestazioni del sistema e supervisiona i controlli tecnici sull'infrastruttura IT e di telecomunicazione.
- **HSEQ** : Supporta il mantenimento del Sistema di Gestione Integrato curando la documentazione e la gestione delle non conformità, collaborando con il RSGSI per gli aspetti di sovrapposizione tra sicurezza delle informazioni e sistemi qualità, salute, sicurezza e ambiente.
- **Tutto il personale, collaboratori e terze parti** : Comprendono e applicano la presente politica e i principi in essa contenuti, utilizzano gli asset informativi in modo responsabile e conforme alle regole stabilite, e segnalano tempestivamente qualsiasi incidente, anomalia o debolezza di sicurezza osservata attraverso i canali ufficiali definiti dal RSGSI.

Obiettivi di sicurezza delle informazioni

La dedizione di DG Impianti Industriali S.p.A. alla sicurezza delle informazioni è un pilastro strategico che si traduce in obiettivi chiari e misurabili, i quali guidano ogni decisione in materia.

- **Conformità normativa e contrattuale** — L'organizzazione deve garantire il pieno rispetto delle leggi, dei regolamenti e degli obblighi contrattuali applicabili, in particolare del GDPR e delle clausole di riservatezza sottoscritte con i clienti operanti nei settori dell'energia, oil & gas, petrolchimico e farmaceutico, assicurando che le pratiche di sicurezza siano costantemente allineate ai requisiti vigenti.
- **Protezione proattiva degli asset informativi** — L'organizzazione deve salvaguardare attivamente le informazioni affidate dai propri clienti, i dati di progetto e la proprietà intellettuale, proteggendoli da ogni minaccia interna o esterna. L'assegnazione formale degli asset, tracciata attraverso il *MOD Modulo di assegnazione dei beni* , e il censimento degli utenti autorizzati, documentato nel *Registro degli utenti autorizzati all'uso delle informazioni* , costituiscono strumenti essenziali a supporto di tale obiettivo.
- **Resilienza operativa** — L'organizzazione deve mantenere la continuità delle operazioni critiche e la capacità di ripristinare i servizi in modo rapido ed efficace in caso di incidente, minimizzando l'impatto sul business e sui clienti.
- **Cultura della sicurezza** — L'organizzazione deve promuovere una cultura pervasiva della sicurezza, in cui ogni membro del personale non solo conosca le politiche vigenti, ma comprenda il valore del proprio ruolo nella protezione delle informazioni e partecipi attivamente ai programmi di formazione e sensibilizzazione.
- **Gestione del rischio** — L'organizzazione deve adottare un approccio maturo e sistematico alla gestione del rischio, che consenta di identificare, valutare e trattare le minacce in modo prioritario e proporzionato, assicurando che le risorse siano investite dove possono generare il massimo valore per la sicurezza delle informazioni.

Principi fondamentali di sicurezza delle informazioni

La strategia di sicurezza delle informazioni di DG Impianti Industriali S.p.A. si fonda su un insieme di principi interconnessi che costituiscono le basi del SGSI e orientano tutte le politiche specifiche e le procedure operative dell'organizzazione.

Responsabilità condivisa

La sicurezza delle informazioni non è un compito relegato a un singolo reparto, ma un dovere che appartiene a ogni persona all'interno dell'organizzazione. Il Top Management deve promuovere una cultura in cui ogni dipendente, collaboratore e terza parte sia consapevole del proprio ruolo e si senta tenuto a segnalare tempestivamente qualsiasi incidente, debolezza o anomalia di sicurezza osservata o sospetta, attraverso i canali ufficiali definiti dal RSGSI. Gli eventi di sicurezza devono essere registrati nel *MOD Registro degli incidenti di sicurezza delle informazioni* per consentirne la ricostruzione e l'analisi. Le condotte attese e le relative conseguenze disciplinari sono dettagliate nel *Codice di condotta* .

Segnalazione eventi di sicurezza:

- Tutto il personale ha l'obbligo di segnalare tempestivamente qualsiasi evento di sicurezza delle informazioni osservato o sospetto, incluse anomalie di funzionamento dei sistemi, potenziali debolezze o violazioni delle policy.
- La segnalazione deve avvenire attraverso i canali ufficiali definiti dall'ICT-RSGSI
- In caso di smarrimento o furto di un asset aziendale, inclusi laptop, dispositivi mobili o badge di accesso, il dipendente deve notificarlo immediatamente al ICT-RSGSI
- Le modalità operative per la classificazione, la gestione e la risposta agli eventi sono dettagliate nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni".

Approccio basato sulla gestione del rischio

Le decisioni in materia di sicurezza delle informazioni devono derivare da un'analisi formale e documentata delle minacce e delle vulnerabilità, condotta secondo la metodologia definita nella *PRO Procedura di gestione dei rischi* . Tale approccio consente di implementare controlli proporzionati alla probabilità e all'impatto dei rischi identificati, assicurando un impiego efficiente delle risorse disponibili.

Controllo degli accessi e uso accettabile delle risorse

L'accesso alle informazioni e ai sistemi deve essere concesso secondo le logiche di "minimo privilegio" e "necessità di sapere" (need-to-know), assicurando che ogni utente disponga esclusivamente delle autorizzazioni indispensabili per svolgere le proprie mansioni. Le regole per l'uso accettabile delle informazioni e delle risorse associate — inclusi i dispositivi assegnati tramite il *MOD Modulo di assegnazione dei beni* — sono definite nella *POL Politica di sicurezza operativa* e disciplinate operativamente nella *PRO Procedura di gestione e controllo degli accessi logici* .

Protezione degli ambienti di lavoro fisici e remoti

Tutti gli spazi di lavoro, presso le sedi aziendali o in contesti esterni, devono essere gestiti in modo da prevenire l'accesso non autorizzato alle informazioni. Il personale deve adottare le regole di scrivania pulita e schermo pulito, configurando il blocco automatico dei dispositivi dopo un periodo di inattività e riponendo documenti e supporti di memorizzazione rimovibili in luoghi sicuri. I beni informativi utilizzati al di fuori delle sedi aziendali — durante trasferte, attività presso i siti dei clienti o in modalità di lavoro da remoto — devono essere protetti con le medesime garanzie di riservatezza, integrità e disponibilità previste per gli ambienti interni, in conformità alle disposizioni della *POL Politica di sicurezza operativa* e della *PRO Procedura di sicurezza fisica e ambientale* .

Sicurezza integrata e difesa in profondità

La sicurezza deve essere considerata una componente nativa fin dalla fase di progettazione di nuovi processi, sistemi o servizi, secondo il principio del security-by-design. L'organizzazione deve implementare più livelli di controlli — tecnologici, fisici e procedurali — in modo che, qualora una barriera dovesse risultare insufficiente, ulteriori

misure siano pronte a intervenire, garantendo una protezione stratificata e resiliente degli asset informativi.

Protezione degli asset aziendali:

- **Scrivania Pulita e Schermo Pulito** : Il personale deve assicurare che documenti e supporti contenenti informazioni sensibili non siano lasciati incustoditi sulle postazioni di lavoro. Tutte le postazioni informatiche devono essere bloccate (tramite blocco schermo protetto da password) quando lasciate incustodite. L'organizzazione impone un blocco automatico dello schermo dopo un periodo predefinito di inattività.
- **Asset Fuori Sede** : Gli asset aziendali utilizzati al di fuori delle sedi operative (ad esempio in modalità di lavoro remoto, presso clienti o in trasferta) devono essere protetti con la medesima diligenza applicata all'interno degli uffici. Il personale è responsabile della custodia fisica e della protezione logica degli asset assegnati, come da accettazione del "MOD Modulo di assegnazione dei beni".
- L'accesso remoto alle risorse aziendali è consentito esclusivamente tramite connessioni sicure (VPN) con autenticazione a più fattori (MFA). È vietato l'uso di reti pubbliche non protette senza l'attivazione dei controlli di sicurezza approvati.
- La gestione completa del ciclo di vita degli asset, dalla loro configurazione allo smaltimento, è disciplinata dalla "PRO Procedura di configurazione, gestione e smaltimento degli asset".

Comunicazione e diffusione delle politiche

La presente politica e le politiche specifiche per argomento devono essere comunicate a tutto il personale interessato e alle parti interessate rilevanti, sia interne sia esterne, e rese disponibili in formato aggiornato. L'organizzazione deve assicurare che ogni destinatario abbia preso visione e compreso i contenuti delle politiche del SGSI, promuovendo la consapevolezza attraverso programmi di formazione periodici.

Archiviazione e aggiornamento

La presente politica è un documento controllato, archiviato e gestito in formato digitale secondo le disposizioni della *PRO Procedura di gestione delle informazioni documentate* . Il ICT-RSGSI è responsabile della sua custodia, distribuzione e aggiornamento.

La politica deve essere riesaminata con cadenza almeno annuale, oppure a seguito di:

- Cambiamenti significativi nella struttura organizzativa, nei processi o nella tecnologia
- Evoluzione del contesto normativo o del panorama delle minacce
- Esiti di audit interni o esterni che evidenzino necessità di adeguamento
- Raccomandazioni emerse durante il riesame della direzione

Qualsiasi modifica deve essere approvata dal Top Management, documentata con indicazione della versione e della data di revisione e comunicata a tutto il personale e alle parti interessate rilevanti.

Documenti di riferimento

- *Codice di condotta*
- *POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni*
- *POL Politica del sistema di gestione*
- *POL Politica di classificazione ed etichettatura delle informazioni*
- *POL Politica di sicurezza operativa*
- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di sicurezza fisica e ambientale
- PRO Procedura di gestione delle informazioni documentate
- PRO Gestione riesame della direzione
- MOD Modulo di assegnazione dei beni
- MOD Registro degli incidenti di sicurezza delle informazioni