

POL Politica del sistema di gestione

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Alessandro Rezzani	Alessandro Rezzani

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Impegno e obiettivi del sistema di gestione
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente politica stabilisce gli indirizzi strategici e gli impegni del Top Management di DATASKILLS S.r.l. in materia di sicurezza delle informazioni, definendo il quadro di riferimento entro il quale l'organizzazione persegue la protezione dei propri asset informativi. Il documento formalizza i principi fondamentali, gli obiettivi e le responsabilità che governano il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), assicurando che esso sia appropriato al contesto di business — consulenza, formazione e sviluppo di soluzioni in ambito data analytics, data science e gestione dei dati — e coerente con la missione di generare valore dai dati dei clienti nel rispetto della riservatezza, dell'integrità e della disponibilità delle informazioni trattate.

Campo di applicazione

La presente politica si applica a tutte le attività di progettazione ed erogazione di servizi di consulenza, formazione e sviluppo di soluzioni di data analytics, data science, business intelligence e intelligenza artificiale svolte da DATASKILLS S.r.l. presso la sede legale di Via Vittor Pisani 7, Milano, nonché in regime di smart working e negli spazi di coworking utilizzati occasionalmente dal personale. Essa vincola tutto il personale dipendente, i collaboratori esterni, i consulenti e le terze parti che accedano alle informazioni o ai sistemi informativi aziendali, indipendentemente dalla modalità di lavoro adottata.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Regolamento (UE) 2016/679
- D.Lgs. 196/2003 e s.m.i.

Termini e definizioni

- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** : insieme di politiche, processi e controlli che un'organizzazione adotta per gestire in modo sistematico i rischi relativi alla sicurezza delle informazioni.
- **Politica** : dichiarazione di intenti e di indirizzo di un'organizzazione, espressa formalmente dal Top Management.
- **Riservatezza** : proprietà per cui le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità** : proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.

- **Rischio** : effetto dell'incertezza sugli obiettivi, espresso in termini di combinazione di probabilità di un evento e delle sue conseguenze.
- **Parte interessata** : persona o organizzazione che può influenzare, essere influenzata o percepirsi come influenzata da una decisione o un'attività.
- **Miglioramento continuo** : attività ricorrente finalizzata ad accrescere la capacità di soddisfare i requisiti.

Ruoli e responsabilità

- **Top Management** : approva e riesamina periodicamente la presente politica, garantendone l'allineamento agli indirizzi strategici e al contesto organizzativo, e assicura la disponibilità delle risorse necessarie al SGSI.
- **Responsabile del Sistema Integrato (RSI)** : coordina la diffusione della politica a tutto il personale e alle parti interessate esterne pertinenti, ne verifica la comprensione e raccoglie le dichiarazioni di presa visione.
- **Production Manager** : assicura che i requisiti di sicurezza derivanti dalla presente politica siano recepiti nella gestione operativa dei progetti e comunicati ai team di lavoro.
- **Chief Data Scientist** : garantisce che le attività di modellazione analitica e machine learning rispettino i principi di protezione delle informazioni stabiliti dalla presente politica.
- **Chief Data Engineer** : garantisce che la progettazione e la manutenzione delle architetture dati e delle pipeline siano condotte in conformità ai principi di sicurezza qui definiti.

Impegno e obiettivi del sistema di gestione

Il Top Management di DATASKILLS S.r.l. si impegna a istituire, attuare, mantenere e migliorare in modo continuo il Sistema di Gestione della Sicurezza delle Informazioni, in coerenza con il proprio ruolo di società di consulenza specializzata in data analytics, data science, business intelligence e intelligenza artificiale al servizio di imprese di medie e grandi dimensioni nei settori retail, FMCG, farmaceutico, bancario-assicurativo, logistico e Industry 4.0.

La politica del sistema di gestione si fonda sui seguenti impegni vincolanti:

- Proteggere la riservatezza dei dati dei clienti e delle informazioni proprietarie trattate nell'ambito dei progetti di analisi avanzata, garantendo che l'accesso sia limitato esclusivamente ai soggetti autorizzati.
- Preservare l'integrità dei dati e dei modelli analitici lungo l'intero ciclo di vita del progetto, prevenendo alterazioni non autorizzate e assicurando l'accuratezza dei risultati prodotti.
- Garantire la disponibilità dei sistemi, delle infrastrutture cloud e dei servizi erogati, minimizzando i tempi di indisponibilità anche in contesti di lavoro completamente da remoto.

- Soddisfare tutti i requisiti legali, regolamentari e contrattuali applicabili, con particolare riferimento alla protezione dei dati personali e agli obblighi verso i clienti dei settori regolamentati.
- Adottare un approccio basato sul rischio per l'identificazione, la valutazione e il trattamento delle minacce alla sicurezza delle informazioni, con revisione periodica del profilo di rischio e attuazione di misure proporzionate.
- Promuovere la consapevolezza e la competenza di tutto il personale mediante programmi di formazione ricorrenti e differenziati per ruolo, affinché ciascun collaboratore comprenda le proprie responsabilità in materia di sicurezza.
- Definire obiettivi misurabili di sicurezza delle informazioni, coerenti con gli indirizzi strategici dell'organizzazione, e monitorarne il raggiungimento attraverso indicatori di prestazione riesaminati in sede di riesame di direzione.
- Comunicare la presente politica a tutto il personale, ai collaboratori e alle parti interessate pertinenti, rendendola disponibile come informazione documentata e aggiornandola ogniqualvolta intervengano cambiamenti significativi nel contesto organizzativo, tecnologico o normativo.

Il Top Management si impegna inoltre a garantire che la direzione strategica dell'organizzazione e le esigenze di sviluppo economico siano sempre compatibili con il mantenimento di un livello adeguato di protezione delle informazioni, promuovendo una cultura della sicurezza condivisa a tutti i livelli e sostenendo l'efficacia del SGSI con risorse finanziarie, tecnologiche e umane proporzionate agli obiettivi dichiarati.

Archiviazione e aggiornamento

La presente politica è conservata nel sistema di gestione documentale dell'organizzazione come informazione documentata controllata, con classificazione pubblica. Il Top Management la riesamina almeno una volta l'anno, o in occasione di variazioni significative del contesto organizzativo, tecnologico, normativo o del panorama delle minacce, per verificarne la continua idoneità e approvare eventuali modifiche. Le versioni superate sono conservate per garantire la tracciabilità storica delle revisioni. Il Responsabile del Sistema Integrato (RSI) cura la distribuzione della versione aggiornata a tutto il personale e alle parti interessate esterne pertinenti, registrandone la presa visione.

Documenti di riferimento

- POL Politica di sicurezza delle informazioni
- PRO Processi direzionali
- PRO Gestione riesame della direzione
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura dei ruoli e responsabilità
- Codice di condotta
- Analisi del contesto

