POL Politica di sicurezza delle informazioni

Storia della versione

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

Indice

Scopo

La presente politica dichiara e comunica l'impegno del Top Management di DATASKILLS S.r.l. verso la protezione degli asset informativi dell'organizzazione. Il documento definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), al fine di garantire la riservatezza, l'integrità e la disponibilità delle informazioni trattate nell'ambito dei servizi di consulenza, formazione e sviluppo di soluzioni in ambito data analytics, data science e gestione dei dati. La politica stabilisce i principi fondamentali e gli obiettivi strategici che guidano tutte le ulteriori politiche, procedure e controlli di sicurezza dell'organizzazione, assicurando che la protezione delle informazioni sia appropriata al contesto operativo aziendale e ne supporti gli indirizzi strategici.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi e gli asset informativi di DATASKILLS S.r.l. relativi alla progettazione ed erogazione di servizi di consulenza, formazione e sviluppo di soluzioni in ambito data analytics, data science e gestione dei dati. Coinvolge tutto il personale, inclusi dipendenti, collaboratori a contratto e terze parti che accedono alle informazioni o ai sistemi aziendali. Dato il modello operativo dell'organizzazione, basato interamente sul lavoro da remoto con utilizzo saltuario di spazi di coworking, la politica si estende a tutti gli ambienti di lavoro in cui il personale opera, indipendentemente dalla loro ubicazione geografica, nonché a tutti i dispositivi e le infrastrutture cloud utilizzate per l'erogazione dei servizi.

Riferimenti normativi

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

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Riservatezza** : proprietà per cui l'informazione non è resa disponibile o divulgata 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.

- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** : parte del sistema di gestione complessivo, basata su un approccio al rischio aziendale, volta a istituire, attuare, gestire, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni.
- **Rischio** : effetto dell'incertezza sugli obiettivi.
- **Valutazione del rischio** : processo complessivo di identificazione, analisi e ponderazione del rischio.
- **Trattamento del rischio** : processo per modificare il rischio.
- **Dichiarazione di applicabilità** : dichiarazione documentata che descrive gli obiettivi di controllo e i controlli pertinenti e applicabili al SGSI dell'organizzazione.
- **Asset informativo** : qualsiasi informazione o elemento di supporto alle informazioni che abbia valore per l'organizzazione.

Ruoli e responsabilità

- **Production Manager** : coordina l'attuazione operativa del SGSI, supervisiona l'assegnazione dei ruoli di sicurezza e verifica l'aderenza ai controlli durante l'erogazione dei servizi ai clienti.
- **Chief Data Engineer** : garantisce la sicurezza delle infrastrutture tecnologiche, delle pipeline dati e delle architetture cloud, e autorizza le configurazioni di sicurezza dei dispositivi.
- **Chief Data Scientist** : assicura che i progetti di data science e machine learning rispettino i requisiti di protezione dei dati e i livelli di classificazione stabiliti.
- **Chief BI Specialist** : verifica che le soluzioni di Business Intelligence e i relativi flussi informativi siano conformi alle politiche di sicurezza delle informazioni.
- **Resp. R&S** : integra i requisiti di sicurezza nelle attività di ricerca e sviluppo e nella valutazione di nuove tecnologie.
- **Data Engineer** : applica i controlli di sicurezza previsti durante lo sviluppo e la manutenzione delle pipeline dati.
- **Senior Data Engineer** : contribuisce alla definizione e al rispetto degli standard di sicurezza nell'ingegneria dei dati.
- **Data Scientist** : tratta i dati secondo le regole di classificazione ed etichettatura e segnala tempestivamente eventuali eventi di sicurezza osservati o sospetti.
- **Senior BI Specialist** : implementa le misure di protezione nelle soluzioni BI e garantisce la corretta gestione degli accessi ai report e alle dashboard.
- **Junior BI Specialist** : applica le politiche di sicurezza nello svolgimento delle proprie attività e segnala immediatamente qualsiasi anomalia o potenziale violazione.
- **Medico del Lavoro** : collabora con la direzione per gli aspetti di sicurezza correlati alla salute occupazionale e al benessere del personale in ambiente di lavoro remoto.

Obiettivi di sicurezza delle informazioni

L'organizzazione persegue obiettivi di sicurezza delle informazioni misurabili, coerenti con il proprio contesto operativo e con gli indirizzi strategici aziendali. Tali obiettivi devono essere comunicati a tutto il personale e riesaminati periodicamente per assicurarne la continua adeguatezza.

Gli obiettivi strategici che il SGSI deve garantire sono:

- Proteggere la riservatezza dei dati dei clienti e delle informazioni proprietarie trattate nell'ambito dei progetti di data analytics, data science e Business Intelligence, prevenendo accessi non autorizzati e divulgazioni indebite.
- Assicurare l'integrità dei dati e dei modelli analitici sviluppati, preservandone accuratezza e completezza lungo l'intero ciclo di vita del progetto.
- Garantire la disponibilità dei sistemi, delle infrastrutture cloud e dei servizi erogati, minimizzando i tempi di interruzione e sostenendo la continuità operativa.
- Mantenere la conformità ai requisiti normativi e contrattuali applicabili, con particolare riferimento alla protezione dei dati personali e agli obblighi verso i clienti dei settori bancario, assicurativo, farmaceutico e della grande distribuzione.
- Ridurre il livello di esposizione ai rischi di sicurezza delle informazioni attraverso l'applicazione sistematica di misure di trattamento proporzionate alla probabilità e all'impatto dei rischi identificati.
- Promuovere la consapevolezza e la competenza del personale in materia di sicurezza delle informazioni, attraverso programmi di formazione ricorrenti e personalizzati per ruolo.
- Migliorare continuamente l'efficacia del SGSI attraverso il monitoraggio degli indicatori di prestazione, l'analisi degli incidenti e l'attuazione di azioni correttive.

Principi fondamentali di sicurezza delle informazioni

La presente politica si fonda su principi cardine che devono orientare tutte le decisioni, i comportamenti e i controlli in materia di sicurezza delle informazioni all'interno di DATASKILLS S.r.l.

Approccio basato sul rischio. Ogni decisione relativa alla protezione degli asset informativi deve basarsi su una valutazione sistematica dei rischi, condotta secondo criteri definiti di probabilità e impatto. L'organizzazione deve identificare, analizzare, ponderare e trattare i rischi per la sicurezza delle informazioni con cadenza periodica e ogniqualvolta si verifichino cambiamenti significativi nel contesto interno o esterno. I rischi con livello superiore alla soglia di accettabilità devono essere oggetto di specifiche misure di mitigazione documentate e monitorate.

Responsabilità condivisa. La sicurezza delle informazioni è responsabilità di tutto il personale, indipendentemente dal ruolo ricoperto. Ogni collaboratore deve contribuire attivamente alla protezione degli asset informativi applicando le politiche e le procedure stabilite e segnalando tempestivamente, attraverso i canali designati, qualsiasi evento di

sicurezza osservato o sospetto. Il personale che opera in smart working o in spazi di coworking deve adottare le medesime cautele previste per qualsiasi ambiente lavorativo aziendale.

Classificazione e protezione delle informazioni. Tutte le informazioni trattate dall'organizzazione devono essere classificate in base alla propria sensibilità secondo i livelli stabiliti — Riservato, Limitato, Pubblico — ed etichettate di conseguenza. Ad ogni livello di classificazione devono corrispondere misure di protezione proporzionate per il trattamento, la trasmissione, la conservazione e la distruzione delle informazioni.

Uso accettabile delle risorse. Le informazioni e le risorse informatiche aziendali devono essere utilizzate esclusivamente per finalità lavorative legittime, nel rispetto dei livelli di classificazione assegnati. L'installazione di software non autorizzato, la condivisione delle credenziali di accesso, la disabilitazione dei controlli di sicurezza e il trasferimento di informazioni classificate su canali o dispositivi non approvati sono espressamente vietati.

Protezione dell'ambiente di lavoro remoto. L'organizzazione opera prevalentemente in modalità di lavoro da remoto; pertanto ogni postazione deve garantire un livello di protezione adeguato. Il personale deve applicare le regole di schermo protetto e scrivania pulita in qualsiasi ambiente in cui opera, impedendo a terzi non autorizzati — inclusi familiari e persone presenti negli spazi di coworking — di accedere a informazioni classificate. I dispositivi devono essere configurati con blocco automatico dello schermo e il personale deve attivarli manualmente in caso di allontanamento, anche temporaneo.

Sicurezza dei beni fuori sede. Tutti i dispositivi e i supporti aziendali utilizzati al di fuori delle sedi dell'organizzazione devono essere protetti da furto, smarrimento e accesso non autorizzato mediante crittografia del disco, autenticazione forte e custodia diligente durante il trasporto e l'utilizzo.

Segnalazione degli eventi di sicurezza. L'organizzazione deve mettere a disposizione del personale un meccanismo chiaro e accessibile per la segnalazione tempestiva di eventi di sicurezza osservati o sospetti. Ogni collaboratore ha l'obbligo di segnalare senza ritardo qualsiasi anomalia, tentativo di phishing, vulnerabilità o potenziale violazione, fornendo il maggior numero possibile di dettagli utili alla valutazione dell'evento.

Miglioramento continuo. L'organizzazione si impegna a migliorare costantemente l'efficacia del SGSI attraverso il riesame periodico della politica e degli obiettivi, l'analisi dei risultati degli audit interni ed esterni, il monitoraggio degli indicatori di prestazione e l'applicazione tempestiva delle azioni correttive necessarie.

Conformità normativa e contrattuale. L'organizzazione deve soddisfare tutti i requisiti legali, regolamentari e contrattuali applicabili in materia di sicurezza delle informazioni e protezione dei dati personali, verificando periodicamente la propria conformità e adeguando i propri controlli alle evoluzioni del quadro normativo.

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGSI, archiviato nel sistema documentale dell'organizzazione secondo le modalità definite nella procedura di gestione delle informazioni documentate. Il Production Manager ne cura la revisione con cadenza almeno annuale, oppure a seguito di cambiamenti significativi nel contesto organizzativo, nell'infrastruttura tecnologica, nel panorama delle minacce o nel quadro normativo

applicabile. Ogni revisione deve essere approvata dal Top Management e comunicata a tutto il personale e alle parti interessate rilevanti. Le versioni superate devono essere conservate a fini di tracciabilità per il periodo definito nelle politiche di conservazione dell'organizzazione.

Documenti di riferimento

- POL Politica di sicurezza operativa
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- POL Politica del sistema di gestione
- POL Politica di conservazione e cancellazione delle informazioni
- 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 configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di sicurezza fisica e ambientale
- PRO Procedura di sviluppo sicuro
- PRO Procedura di crittografia e gestione delle chiavi crittografiche
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di gestione delle risorse umane
- Codice di condotta
- MOD Modulo di assegnazione dei beni