

POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	10/02/2026	Anna Miola	Anna Miola

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 costituisce il documento quadro del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di DOLOMITESWEB SRL. Con essa gli organi di amministrazione e direttivi dichiarano e comunicano il proprio impegno verso la protezione del patrimonio informativo aziendale, stabilendo il riferimento per istituire, attuare, mantenere e migliorare continuamente il SGSI.

DOLOMITESWEB SRL riconosce che la sicurezza delle informazioni è un fattore abilitante per la propria attività di agenzia di marketing digitale e comunicazione online, nonché una garanzia di fiducia nei confronti dei clienti — aziende e strutture ricettive del Trentino–Alto Adige e del Veneto — che affidano all'organizzazione dati, contenuti e piattaforme digitali. Attraverso questa politica, l'organizzazione persegue la tutela della riservatezza, dell'integrità e della disponibilità delle informazioni proprie e dei clienti, in coerenza con la propria strategia di crescita e con il contesto normativo in materia di cybersicurezza.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi e i sistemi tecnologici dell'organizzazione, inclusi quelli ospitati presso fornitori di servizi cloud esterni. Il campo di applicazione copre la sede operativa di Via San Francesco d'Assisi, n. 39 — Primiero San Martino di Castrozza (TN) — e qualsiasi ambiente di lavoro da remoto utilizzato dal personale.

La politica coinvolge tutto il personale di DOLOMITESWEB SRL, compresi collaboratori a contratto e terze parti che accedono alle informazioni o ai sistemi aziendali, indipendentemente dalla loro ubicazione geografica. Sono esclusi dal campo di applicazione i sistemi e le aree non pertinenti ai servizi erogati dall'organizzazione e alla relativa infrastruttura informativa.

Riferimenti normativi

- Direttiva (UE) 2022/2555
- D.Lgs. 138/2024
- Regolamento (UE) 2016/679

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **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 della probabilità di un evento e delle sue conseguenze.
- **Valutazione del rischio** : processo complessivo di identificazione, analisi e ponderazione del rischio.
- **Trattamento del rischio** : processo volto a modificare il rischio, che può includere mitigazione, accettazione, trasferimento o eliminazione.
- **Asset informativo** : qualsiasi bene, materiale o immateriale, che abbia valore per l'organizzazione in termini di informazione.
- **Incidente di sicurezza** : evento o serie di eventi che compromettono la riservatezza, l'integrità o la disponibilità dei sistemi informativi e di rete.
- **Misura di sicurezza** : controllo tecnico, organizzativo o procedurale attuato per ridurre il rischio a un livello accettabile.

Ruoli e responsabilità

- **Managing Partner** : approva la presente politica, accetta formalmente i rischi residui e garantisce la disponibilità delle risorse necessarie all'attuazione del SGSI.
- **Responsabile Sicurezza delle Informazioni** : definisce, implementa e mantiene il framework di sicurezza delle informazioni, conduce le valutazioni dei rischi e sviluppa i controlli allineati al quadro normativo di riferimento.
- **Responsabile del sistema di gestione** : cura la documentazione del SGSI, pianifica gli audit interni e monitora il programma di miglioramento continuo.
- **Responsabile Gestione Incidenti** : coordina la risposta agli incidenti di sicurezza informatica, gestisce le notifiche verso le autorità competenti e conduce le revisioni post-incidente.
- **Responsabile Rapporti con Fornitori IT** : verifica la conformità dei fornitori ai requisiti di sicurezza delle informazioni, monitora i livelli di servizio e gestisce le clausole contrattuali di cybersicurezza.
- **General Manager** : traduce gli indirizzi strategici della politica in piani operativi e assicura che le prestazioni dei team siano coerenti con gli obiettivi di sicurezza.
- **Tutto il personale** : osserva le disposizioni della presente politica, segnala tempestivamente eventi anomali o potenziali vulnerabilità e partecipa alle iniziative di formazione e consapevolezza in materia di sicurezza.

Obiettivi di sicurezza delle informazioni

DOLOMITESWEB SRL persegue obiettivi di sicurezza delle informazioni coerenti con la propria missione di agenzia digitale e con il contesto operativo in cui opera. Tali obiettivi

sono definiti tenendo conto della valutazione dei rischi, delle esigenze dei clienti e delle parti interessate, e vengono riesaminati periodicamente in sede di riesame della direzione.

L'organizzazione si impegna a:

- proteggere la riservatezza dei dati dei clienti — in particolare contenuti editoriali, credenziali di accesso alle piattaforme, campagne pubblicitarie e dati personali — lungo l'intero ciclo di vita del servizio;
- garantire l'integrità dei sistemi informativi e dei contenuti digitali gestiti per conto dei clienti, prevenendo alterazioni non autorizzate;
- assicurare la disponibilità delle piattaforme, degli strumenti di lavoro e dei servizi cloud da cui dipende l'erogazione dei servizi di marketing digitale, sviluppo web e comunicazione online;
- ridurre il livello di rischio di cybersicurezza entro soglie accettabili, adottando un approccio sistematico di identificazione, valutazione e trattamento dei rischi;
- soddisfare i requisiti normativi applicabili, con particolare riferimento alla disciplina sulla protezione dei dati personali e alla normativa in materia di sicurezza informatica;
- promuovere la consapevolezza di tutto il personale affinché ciascuno contribuisca attivamente alla protezione del patrimonio informativo aziendale;
- migliorare in modo continuo l'efficacia del SGSI, attraverso audit, riesami della direzione, monitoraggio degli indicatori e attuazione di piani di adeguamento approvati dagli organi di amministrazione e direttivi.

Gli obiettivi vengono declinati in indicatori misurabili documentati nel programma di miglioramento, la cui attuazione e i cui esiti sono oggetto di relazioni periodiche agli organi di amministrazione e direttivi.

Principi fondamentali di sicurezza delle informazioni

Approccio basato sul rischio

DOLOMITESWEB SRL fonda ogni decisione di sicurezza sulla valutazione del rischio. L'organizzazione adotta una metodologia strutturata che combina probabilità e impatto per classificare i rischi e determinare le priorità di trattamento: i rischi che superano la soglia di accettabilità sono sottoposti a misure di mitigazione, trasferimento o eliminazione, mentre quelli al di sotto della soglia possono essere consapevolmente accettati con approvazione del **Managing Partner**. La valutazione è riesaminata almeno una volta l'anno e comunque in occasione di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce.

Responsabilità condivisa

La sicurezza delle informazioni è responsabilità di ogni persona che opera per conto dell'organizzazione. Gli organi di amministrazione e direttivi ne garantiscono la governance e le risorse; i ruoli specialistici — **Responsabile Sicurezza delle Informazioni**, **Responsabile Gestione Incidenti**, **Responsabile Rapporti con Fornitori IT** — ne

assicurano la supervisione operativa; tutto il personale concorre alla protezione degli asset informativi attraverso il rispetto delle politiche e delle procedure di sicurezza.

Necessità di conoscere e minimo privilegio

L'accesso alle informazioni e ai sistemi è concesso esclusivamente nella misura necessaria allo svolgimento delle attività assegnate. L'organizzazione adotta il principio del minimo privilegio per limitare l'esposizione degli asset informativi, controllando e riesaminando periodicamente i diritti di accesso assegnati al personale e agli amministratori di sistema.

Protezione proporzionata

Le misure di sicurezza sono proporzionate alla criticità degli asset e al livello di rischio associato. L'organizzazione classifica le proprie informazioni secondo livelli di riservatezza — pubblico, limitato, confidenziale — e applica controlli differenziati in relazione alla sensibilità dei dati trattati.

Sicurezza della catena di approvvigionamento

DOLOMITESWEB SRL estende le proprie esigenze di sicurezza ai fornitori e ai partner tecnologici che supportano l'infrastruttura digitale e i servizi erogati. La selezione, la qualificazione e il monitoraggio dei fornitori tengono conto dei rischi di cybersicurezza e delle garanzie offerte in termini di protezione dei dati e continuità del servizio.

Gestione degli incidenti e continuità operativa

L'organizzazione si impegna a prevenire gli incidenti di sicurezza e, qualora si verificano, a contenerli, eradicarli e ripristinare le normali condizioni operative nel più breve tempo possibile. Piani di continuità operativa e di ripristino in caso di disastro sono mantenuti per tutelare la disponibilità dei servizi critici.

Conformità normativa e miglioramento continuo

L'organizzazione opera in conformità alla normativa applicabile in materia di sicurezza informatica e protezione dei dati personali. Il SGSI è sottoposto a un ciclo continuo di verifica e miglioramento attraverso audit interni, riesami della direzione e piani di adeguamento; gli organi di amministrazione e direttivi sono periodicamente informati sullo stato di conformità e sull'efficacia delle misure adottate.

Copertura delle politiche di sicurezza

A supporto della presente politica quadro, l'organizzazione adotta e mantiene politiche e procedure operative che coprono almeno i seguenti ambiti:

- gestione del rischio

- ruoli e responsabilità
- affidabilità delle risorse umane
- conformità e audit di sicurezza
- gestione dei rischi della catena di approvvigionamento
- gestione degli asset
- gestione delle vulnerabilità
- continuità operativa, ripristino in caso di disastro e gestione delle crisi
- gestione dell'autenticazione, delle identità digitali e del controllo accessi
- sicurezza fisica
- formazione del personale e consapevolezza
- sicurezza dei dati
- sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete
- protezione delle reti e delle comunicazioni
- monitoraggio degli eventi di sicurezza
- risposta agli incidenti e ripristino

Tali politiche e procedure sono approvate dagli organi di amministrazione e direttivi e rese note alle articolazioni competenti dell'organizzazione, tenuto conto della necessità di conoscere.

Archiviazione e aggiornamento

La presente politica è un documento controllato, archiviato all'interno del sistema di gestione documentale dell'organizzazione e accessibile a tutto il personale autorizzato. Il **Responsabile del sistema di gestione** ne cura la distribuzione e la conservazione secondo le modalità definite nella *PRO Procedura di gestione delle informazioni documentate*.

La politica è riesaminata almeno con cadenza annuale e comunque in occasione di evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi. Il riesame verifica in particolare la conformità alla normativa vigente e l'adeguatezza degli obiettivi e dei principi dichiarati.

Ogni modifica è approvata dagli organi di amministrazione e direttivi e comunicata alle articolazioni competenti dell'organizzazione, tenuto conto della necessità di conoscere. Gli esiti del riesame e le relative decisioni sono registrati nel verbale di riesame della direzione.

Documenti di riferimento

- POL Politica di gestione del rischio
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- POL Politica di sicurezza operativa
- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di gestione dei rischi
- PRO Procedura dei ruoli e responsabilità
- PRO Procedura di gestione delle risorse umane
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di gestione della sicurezza della rete
- PRO Procedura di continuità operativa e di ripristino di emergenza
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Gestione audit interni
- PRO Gestione riesame della direzione
- PRO Procedura delle misurazioni e del monitoraggio