POL Politica del sistema di gestione

Storia della versione

Versione	Data	Autore	Approvato da
1	13/07/2026	Manuele Pola	Gabriele Venier

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 esprime gli indirizzi strategici con cui il **Top Management** di Visup guida il Sistema di Gestione della Sicurezza delle Informazioni (SGSI). Visup progetta e sviluppa piattaforme SaaS cloud che raccolgono, gestiscono e valorizzano i dati generati da macchine industriali ed elettrodomestici professionali, arricchendoli con funzionalità di intelligenza artificiale, e-learning e troubleshooting. La sua missione è trasformare questi dati in valore per i clienti B2B, mentre la sua visione è essere un partner affidabile, anche sul piano della cybersicurezza, per i costruttori che operano in Europa e negli Stati Uniti.

Da questa missione discende la scelta di fare della sicurezza delle informazioni una leva di crescita. L'organizzazione riconosce che riservatezza, integrità e disponibilità dei dati affidati dai clienti sono condizioni essenziali per creare valore nel tempo, per rispondere alle richieste di assessment dei clienti e per migliorare la propria organizzazione interna. La politica fornisce quindi il quadro per fissare gli obiettivi dell'SGSI e per orientare tutte le politiche e le procedure che ne derivano.

Campo di applicazione

La politica si applica all'intero SGSI di Visup e, in particolare, alla progettazione, sviluppo, erogazione e gestione di soluzioni digitali, servizi cloud, applicazioni web e software per la visualizzazione e l'analisi di dati complessi, unitamente ai servizi di consulenza informatica e strategica. Comprende le piattaforme SaaS per il settore HoReCa e per il settore industriale, i servizi di assistenza e manutenzione e gli sviluppi personalizzati. Si applica alla sede operativa di Via Taboga 307, Gemona (UD), a tutto il personale, compreso il **Top Management** , e ai fornitori e partner che trattano informazioni dell'organizzazione o dei suoi clienti.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Regolamento (UE) 2016/679
- Regolamento (UE) 2023/2854
- Regolamento (UE) 2024/2847

Termini e definizioni

- **Politica** : intenzioni e indirizzi di un'organizzazione, espressi formalmente dalla sua alta direzione.

- **Alta direzione** : persona o gruppo di persone che dirige e controlla un'organizzazione al livello più elevato.
- **Sistema di gestione** : insieme di elementi correlati o interagenti di un'organizzazione, finalizzato a stabilire politiche, obiettivi e processi per conseguire tali obiettivi.
- **Obiettivo** : risultato da conseguire.
- **Miglioramento continuo** : attività ricorrente per accrescere le prestazioni.
- **Parte interessata** : persona o organizzazione che può influenzare, essere influenzata, o percepire sé stessa come influenzata da una decisione o attività.
- **Informazioni documentate** : informazioni che devono essere tenute sotto controllo e mantenute da parte di un'organizzazione e il mezzo che le contiene.
- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.

Ruoli e responsabilità

- **Top Management** : stabilisce, approva e tiene aggiornata la politica, ne assicura la coerenza con la strategia aziendale e garantisce le risorse necessarie per attuarla.
- **Amministratore Delegato / CEO** : integra gli obiettivi di sicurezza delle informazioni nella strategia di business e promuove una cultura aziendale orientata alla sicurezza.
- **Responsabile del Sistema di Gestione** : mantiene la politica come informazione documentata, ne cura la diffusione e la pubblicazione e la sottopone a riesame insieme agli obiettivi dell'SGSI.
- **CTO** : traduce gli impegni della politica nell'architettura di sicurezza delle piattaforme e dell'infrastruttura cloud.
- **DPO / RPD** : assicura che gli impegni della politica siano coerenti con gli obblighi in materia di protezione dei dati personali.
- **Project Manager** : incorpora i requisiti della politica nei progetti e nei rapporti con clienti e fornitori coinvolti.
- **Personale** : conosce la politica, la applica nelle proprie attività e segnala al **Responsabile del Sistema di Gestione** ogni situazione che possa comprometterla.

Impegno e obiettivi del sistema di gestione

Visup adotta questa politica come espressione della propria missione e la mantiene appropriata al contesto in cui opera: un'azienda di dimensioni contenute, con una sola sede, che eroga servizi cloud a costruttori B2B e si affida a fornitori critici per infrastruttura e intelligenza artificiale. L' *Analisi del contesto* e la valutazione dei rischi forniscono la base su cui il **Top Management** fonda e aggiorna questi indirizzi.

Impegni del Top Management

L'organizzazione si impegna a:

- proteggere riservatezza, integrità e disponibilità delle informazioni proprie e dei clienti trattate dalle piattaforme e dai servizi cloud;
- soddisfare i requisiti applicabili relativi alla sicurezza delle informazioni, siano essi legali, regolamentari, contrattuali o derivanti dalle parti interessate;
- applicare un approccio basato sul rischio, trattando i rischi in modo proporzionato al loro impatto sul business;
- integrare la sicurezza fin dalla progettazione nello sviluppo del software e nella gestione dell'infrastruttura;
- garantire le risorse, le competenze e la consapevolezza necessarie al funzionamento dell'SGSI;
- migliorare in modo continuo l'idoneità, l'adeguatezza e l'efficacia dell'SGSI.

Quadro per gli obiettivi

La politica fornisce il quadro entro cui l'organizzazione stabilisce gli obiettivi di sicurezza delle informazioni. Visup persegue obiettivi misurabili, coerenti con questi impegni e con l'esito della valutazione dei rischi, e li raccoglie nel *MOD Programma di miglioramento* , che per ciascun obiettivo indica l'azione prevista, il responsabile, le risorse dedicate, i tempi e l'indicatore di monitoraggio. Il **Top Management** riesamina gli obiettivi e il loro stato di avanzamento almeno una volta all'anno, nell'ambito del riesame della direzione descritto nella procedura *PRO Gestione riesame della direzione* . Gli indirizzi specifici per la protezione degli asset informativi sono sviluppati nella *POL Politica di sicurezza delle informazioni* , mentre le modalità di governo dell'SGSI sono descritte in *PRO Processi direzionali* .

Disponibilità e comunicazione della politica

Visup si impegna a rendere la politica conosciuta da chi deve applicarla e accessibile a chi ha interesse a conoscerla:

Ambito	Impegno
Informazione documentata	Il **Responsabile del Sistema di Gestione** mantiene la politica come informazione documentata e la tiene sotto controllo secondo la *PRO Procedura di gestione delle informazioni documentate* , dopo l'approvazione del **Top Management** .

Comunicazione interna	Il **Responsabile del Sistema di Gestione** comunica la politica a tutto il personale attraverso i canali di comunicazione interni definiti nella *PRO Procedura gestione comunicazione* .
Parti interessate	Visup pubblica la politica sul sito web aziendale, dove clienti, potenziali clienti e altre parti interessate possono consultarla liberamente.

Archiviazione e aggiornamento

Il **Responsabile del Sistema di Gestione** archivia la politica in formato elettronico nel sistema documentale dell'SGSI, conservandone le versioni superate secondo la *PRO Procedura di gestione delle informazioni documentate* . Il **Top Management** riesamina la politica almeno una volta all'anno in occasione del riesame della direzione, e comunque in presenza di cambiamenti significativi del contesto, dei requisiti applicabili o dei rischi; il **Responsabile del Sistema di Gestione** ne cura l'aggiornamento e il **Top Management** approva ogni nuova versione.

Documenti di riferimento

- Analisi del contesto
- MOD Programma di miglioramento
- PRO Gestione riesame della direzione
- POL Politica di sicurezza delle informazioni
- PRO Processi direzionali
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura gestione comunicazione