

POL Politica del sistema di gestione

Storia della versione

Versione	Data	Autore	Approvato da
1	27/05/2026	Daniele Collantoni	Andrea Biccocchi

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

Abstraqt S.r.l. riconosce la sicurezza delle informazioni come un pilastro strategico della propria attività di progettazione, sviluppo ed erogazione di servizi Cloud (SaaS), soluzioni digitali, applicazioni web e software proprietari per la gestione dei processi produttivi e aziendali, unitamente ai relativi servizi di assistenza tecnica e consulenza informatica. La presente politica traduce la visione dell' **Alta Direzione** in un quadro di impegni e obiettivi condivisi, dando forma al Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e garantendone la coerenza con il contesto organizzativo, gli indirizzi strategici e le aspettative legittime delle parti interessate.

Il documento costituisce il riferimento al vertice del SGSI: ogni politica operativa, procedura e istruzione di sicurezza si conforma ai principi qui enunciati, affinché la protezione del patrimonio informativo permei l'intera struttura organizzativa e accompagni tutte le fasi del ciclo di vita dei servizi e dei prodotti offerti dall'organizzazione.

Campo di applicazione

La presente politica si applica a tutte le funzioni organizzative, i processi e le attività di Abstraqt S.r.l. svolte presso la sede di Viale Giacomo Puccini 311/b, 55100 Lucca (LU). Il perimetro comprende la progettazione e lo sviluppo di software personalizzato per la pubblica amministrazione e per clienti privati, l'erogazione e la gestione di servizi Cloud (SaaS), le attività di assistenza tecnica e consulenza informatica, nonché ogni servizio di supporto correlato. La politica si rivolge a tutto il personale dipendente, ai collaboratori esterni e ai fornitori che operano per conto dell'organizzazione, indipendentemente dalla forma contrattuale.

Riferimenti normativi

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

Termini e definizioni

- **Sistema di gestione della sicurezza delle informazioni (SGSI)** : componente del sistema di gestione complessivo, basata su un approccio al rischio aziendale, finalizzata a stabilire, attuare, condurre, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni.
- **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 come combinazione delle conseguenze di un evento e della relativa probabilità di accadimento.
- **Valutazione del rischio** : processo complessivo di identificazione, analisi e ponderazione del rischio.
- **Trattamento del rischio** : processo volto a modificare il rischio mediante la selezione e l'attuazione di misure appropriate.
- **Parte interessata** : persona o organizzazione che può influenzare, essere influenzata o percepirsi influenzata da una decisione o da un'attività dell'organizzazione.
- **Politica** : intenzioni e orientamento di un'organizzazione, formalmente espressi dall'alta direzione.
- **Miglioramento continuo** : attività ricorrente svolta per accrescere le prestazioni del sistema di gestione.
- **Informazione documentata** : informazione che deve essere tenuta sotto controllo e mantenuta da un'organizzazione, unitamente al supporto che la contiene.

Ruoli e responsabilità

- **Alta Direzione** : stabilisce, approva e riesamina la politica del SGSI, assicurandone l'allineamento con il contesto operativo e gli indirizzi strategici dell'organizzazione.
- **Responsabile del sistema di gestione** : predispone la bozza della politica, ne cura la comunicazione al personale e alle parti interessate e ne supervisiona il riesame periodico.

Impegno e obiettivi del sistema di gestione

Impegno dell'Alta Direzione e principi fondamentali

L' **Alta Direzione** di Abstraqt S.r.l. promuove la sicurezza delle informazioni come valore fondante dell'organizzazione e si impegna a garantire che la presente politica resti appropriata allo scopo e al contesto in cui l'azienda opera, coerente con gli indirizzi strategici che ne orientano lo sviluppo. Tale impegno si concretizza nelle seguenti dichiarazioni:

- L'organizzazione adotta un approccio sistematico alla gestione del rischio: ogni decisione in materia di sicurezza delle informazioni si fonda sull'identificazione, sulla valutazione e sul trattamento dei rischi che insistono sugli asset informativi aziendali, secondo la metodologia definita nella *PRO Procedura di gestione dei rischi* . I risultati della valutazione determinano la selezione dei controlli e l'allocazione delle risorse, affinché le misure adottate risultino proporzionate alle minacce effettive.

- La protezione delle informazioni è proporzionata alla loro sensibilità: un sistema di classificazione consente di applicare controlli differenziati a ciascun livello, garantendo un trattamento, una trasmissione e una conservazione dei dati adeguati al grado di criticità.
- L'accesso alle informazioni e ai sistemi si fonda sui principi del minimo privilegio e della necessità operativa, cosicché ogni utente disponga esclusivamente delle autorizzazioni indispensabili allo svolgimento delle proprie mansioni.
- L'organizzazione si impegna a soddisfare i requisiti applicabili in materia di sicurezza delle informazioni, con particolare attenzione alla protezione dei dati personali e alle clausole di sicurezza previste nei rapporti con la pubblica amministrazione, conformemente al quadro normativo vigente.
- Il miglioramento continuo costituisce un valore fondante del SGSI: l' **Alta Direzione** promuove l'evoluzione costante delle pratiche di sicurezza, dei processi e delle competenze, verificandone periodicamente l'adeguatezza e l'efficacia attraverso il riesame della direzione.
- L' **Alta Direzione** assicura la disponibilità delle risorse finanziarie, umane e tecniche necessarie al funzionamento e al potenziamento del SGSI, integrando i requisiti di sicurezza in tutti i processi aziendali, dalla progettazione e dallo sviluppo del software fino all'erogazione dei servizi.

L'organizzazione riconosce che la sicurezza delle informazioni è una responsabilità condivisa: ogni persona che opera per conto di Abstraqt, indipendentemente dal ruolo e dalla forma contrattuale, contribuisce alla protezione del patrimonio informativo rispettando le politiche vigenti, partecipando ai programmi di formazione e sensibilizzazione e segnalando tempestivamente ogni potenziale minaccia.

Obiettivi strategici di sicurezza delle informazioni

La presente politica fornisce il quadro di riferimento per la definizione degli obiettivi di sicurezza delle informazioni. L' **Alta Direzione** persegue i seguenti obiettivi strategici, che trovano declinazione in traguardi misurabili nell'ambito del riesame della direzione:

- Tutelare la riservatezza, l'integrità e la disponibilità delle informazioni gestite nell'ambito dello sviluppo software, dell'erogazione di servizi SaaS e delle attività di consulenza informatica.
- Garantire la conformità ai requisiti normativi e contrattuali applicabili, con particolare attenzione alla protezione dei dati personali e alle clausole di sicurezza previste nei rapporti con la pubblica amministrazione.
- Contenere l'esposizione ai rischi per la sicurezza delle informazioni attraverso l'applicazione sistematica della metodologia di valutazione e trattamento dei rischi.
- Diffondere una cultura della sicurezza presso tutto il personale, promuovendo consapevolezza, competenza e responsabilità individuali.
- Assicurare la continuità dei servizi e la resilienza delle infrastrutture tecnologiche, minimizzando l'impatto di eventuali incidenti di sicurezza.

- Misurare le prestazioni del SGSI attraverso indicatori definiti e riesaminati periodicamente, in un'ottica di miglioramento continuo.

Il raggiungimento di tali obiettivi è monitorato attraverso gli indicatori registrati dal **Responsabile del sistema di gestione** e verificato in sede di riesame della direzione, secondo quanto stabilito nella *PRO Gestione riesame della direzione*.

Comunicazione e disponibilità della politica

L' **Alta Direzione** favorisce la piena diffusione della presente politica affinché sia compresa, applicata e costantemente aggiornata a ogni livello dell'organizzazione. A tal fine il **Responsabile del sistema di gestione** ne cura la comunicazione interna attraverso i canali aziendali approvati, conformemente alle modalità definite nella *PRO Procedura gestione comunicazione*, raccogliendo la conferma di ricezione da parte del personale.

La politica, classificata come pubblica, è resa disponibile alle parti interessate esterne attraverso la pubblicazione sul sito web istituzionale dell'organizzazione e, ove richiesto, mediante l'inclusione nella documentazione contrattuale. In tal modo clienti, fornitori e ogni altra parte interessata possono consultarla liberamente.

Il **Responsabile del sistema di gestione** supervisiona il riesame della politica con cadenza almeno annuale, verificando l'allineamento dei contenuti con l'evoluzione del contesto organizzativo, le risultanze della valutazione dei rischi e gli obiettivi del SGSI. L' **Alta Direzione** riesamina la politica in occasione di ogni riesame della direzione e ogniqualvolta si verifichino cambiamenti significativi nel contesto interno o esterno, disponendone l'aggiornamento secondo il medesimo ciclo di approvazione. Le modifiche approvate sono comunicate a tutto il personale e rese disponibili alle parti interessate.

Archiviazione e aggiornamento

La presente politica è conservata in formato digitale nei repository autorizzati dell'organizzazione e registrata nel registro centrale della documentazione del SGSI, che ne riporta la versione corrente, la data di ultima revisione e il livello di classificazione. Il **Responsabile del sistema di gestione** ne cura la revisione con cadenza almeno annuale, ovvero ogniqualvolta intervengano modifiche significative nel contesto organizzativo, nel quadro normativo applicabile o nella struttura del SGSI. Ogni aggiornamento segue il medesimo ciclo di approvazione da parte dell' **Alta Direzione** e viene successivamente comunicato a tutto il personale e reso disponibile alle parti interessate, secondo le modalità descritte nella *PRO Procedura di gestione delle informazioni documentate*.

Documenti di riferimento

- PRO Procedura di gestione dei rischi
- PRO Gestione riesame della direzione
- PRO Procedura gestione comunicazione
- PRO Procedura di gestione delle informazioni documentate