Di uso pubblico

Politica della Sicurezza delle Informazioni

Codice:	Politica della Sicurezza delle Informazioni
Edizione	0.6
Data di creazione	21/12/18
Data di aggiornamento:	25/02/26
Redatta da:	Team SGSI
Approvata da:	RSGSI
Livello di riservatezza:	PUBBLICO

Cronologia delle revisioni

Ed.	Rev.	Data	Oggetto	Autore	Approvatore	Distribuzione
00	01	21/12/18	Prima emissione	Team SGSI	RSGSI	e-mail
00	02	31/01/19	Revisione	Team SGSI	RSGSI	e-mail
00	03	15/05/19	Revisione	Team SGSI	RSGSI	e-mail
00	04	30/05/21	Verifica annuale	Team SGSI	RSGSI	e-mail
00	05	25/01/24	Verifica annuale	Team SGSI	RSGSI	e-mail
00	06	25/02/26	Verifica annuale	Team SGSI	RSGSI	e-mail

Sommario

* * *

1. Scopo e ambito

La presente Politica ("**Politica**") definisce i princìpi, gli obiettivi e l'impegno della Direzione di Axitea S.p.A. ("**Axitea**" o l'"**Azienda**") nella protezione delle informazioni, dei sistemi informativi e dei servizi digitali, in coerenza con il Sistema di Gestione della Sicurezza delle Informazioni ("**SGSI**").

Il SGSI di Axitea ha come obiettivo primario la protezione del patrimonio informativo di Axitea S.p.A. e il mantenimento dei requisiti di riservatezza, integrità e disponibilità delle informazioni proprie e dei clienti attraverso specifici controlli atti anche a soddisfare i requisiti normativi e cogenti attinenti alla sicurezza delle informazioni, con particolare riferimento alle norme applicabili alla vigilanza privata e alla tutela dei dati personali.

Il raggiungimento di adeguati ed efficaci livelli di sicurezza consente all'Azienda di mitigare e contrastare le perdite e i danneggiamenti che possano avere un impatto sulle persone, sull'immagine, sulla reputazione aziendale, sugli aspetti di natura economica e finanziaria. Parimenti, tali risultati garantiscono il rispetto del contesto contrattuale e legislativo vigente in materia di protezione delle informazioni.

La Politica è applicabile a:

- tutte le informazioni aziendali, indipendentemente dal formato;
- tutto il personale, collaboratori, fornitori e terze parti;
- tutti i sistemi IT, OT e cloud utilizzati per l'erogazione dei servizi.

2. Riferimenti normativi e framework

Axitea S.p.A. si impegna a mantenere la conformità e l'allineamento ai seguenti standard e normative di riferimento, considerando in modo integrato gli aspetti di sicurezza delle informazioni, sostenibilità, responsabilità sociale ed etica d'impresa:

- ISO/IEC 27001:2022 – Information Security Management Systems;
- Regolamento (UE) 2016/679 (GDPR);
- Direttiva (UE) 2022/2555 – NIS2 (ove applicabile);
- Linee guida ENISA e best practice di settore in ambito cybersicurezza e resilienza;
- Standard internazionali riconosciuti;
- Integrazione con le politiche aziendali in materia di Codice Etico, Whistleblowing, Sostenibilità, Responsabilità Sociale e Gestione dei Fornitori.

L'Azienda adotta un approccio coerente e trasversale, in cui la sicurezza delle informazioni contribuisce anche alla valutazione della maturità ESG, alla tutela degli stakeholder e alla creazione di valore sostenibile nel lungo periodo.

3. Princìpi di sicurezza delle informazioni

La sicurezza delle informazioni è garantita secondo i princìpi fondamentali di:

- **Riservatezza**: accesso alle informazioni consentito solo a soggetti autorizzati;
- **Integrità**: protezione da modifiche non autorizzate o accidentali;
- **Disponibilità**: accesso alle informazioni e ai servizi quando richiesto.

Tali princìpi sono declinati secondo un approccio di gestione del rischio continuo e documentato, in linea con ISO/IEC 27001:2022.

4. Obiettivi del Sistema di Gestione della Sicurezza delle Informazioni

In tale ambito, l'Azienda individua i seguenti obiettivi strategici e operativi del SGSI, coerenti con i requisiti ISO/IEC 27001:

i. Adozione e miglioramento continuo delle best practice di sicurezza delle informazioni e di cybersicurezza, nonché promozione e mantenimento delle certificazioni di conformità agli standard di riferimento;
ii. Definizione chiara di ruoli, responsabilità e accountability, assegnate a tutto il personale e, ove applicabile, ai soggetti terzi che svolgono incarichi rilevanti per la sicurezza delle informazioni;
iii. Allocazione di risorse adeguate (umane, tecnologiche ed economiche) per l'implementazione e il mantenimento di misure di sicurezza fisiche, logiche e organizzative proporzionate ai rischi;
iv. Promozione costante del SGSI e della cultura della sicurezza, con il coinvolgimento attivo della Direzione, degli Organi apicali e del management;
v. Definizione, documentazione e applicazione di regole e procedure per l'uso corretto delle informazioni, degli asset informativi e degli strumenti aziendali;
vi. Sviluppo e mantenimento di programmi di consapevolezza e formazione, volti a rafforzare il comportamento responsabile del personale e delle terze parti;
vii. Adozione di misure proattive e reattive per la prevenzione, la rilevazione e la gestione efficace degli incidenti di sicurezza delle informazioni e cyber;
viii. Miglioramento continuo del SGSI, attraverso attività pianificate di monitoraggio, audit, riesame e aggiornamento, in risposta all'evoluzione del contesto normativo, tecnologico e delle minacce.

4.1. Obiettivi qualitativi

A supporto degli obiettivi sopra indicati, l'Azienda definisce e monitora indicatori e target, quali a titolo esemplificativo:

a) rafforzare la cultura della sicurezza delle informazioni a tutti i livelli aziendali;
b) migliorare il livello di consapevolezza sui rischi cyber e sulla protezione dei dati personali e delle informazioni riservate;
c) incrementare il livello di maturità del SGSI e l'integrazione con i processi ESG e di supply chain;
d) migliorare la capacità di risposta e coordinamento in caso di incidenti di sicurezza.

4.2. Obiettivi quantitativi

	Obiettivo quantitativo	Indicatore/Target	Scadenza
1.	Formazione del personale su sicurezza delle informazioni, privacy e cybersecurity Formazione del personale dotato di mail aziendale su tematiche di sicurezza delle informazioni, privacy e cybersecurity	Almeno il 50% del personale (riferito al totale in forza alla data del 31/10 di ogni anno) formato annualmente	2026 - 2030 (verifica annuale)
2.	Continuità operativa e risposta agli incidenti	Esecuzione di test di continuità operativa e incident response ≥ 1/anno	2026 - 2030 (verifica annuale)
3.	Riduzione degli incidenti di sicurezza presi in carico oltre 2 ore dalla segnalazione	≤ 5% degli incidenti di sicurezza presi in carico oltre 2 ore dalla segnalazione nell'ultimo semestre	2026 - 2030 (riesame annuale)

Gli obiettivi sono riesaminati periodicamente dalla Direzione e aggiornati in funzione dei risultati conseguiti e del contesto di riferimento.

5. Governance e responsabilità

La Direzione:

- definisce e approva la presente Politica;
- assegna ruoli, responsabilità e poteri in materia di sicurezza delle informazioni;
- garantisce risorse adeguate (organizzative, tecniche ed economiche);
- promuove una cultura della sicurezza a tutti i livelli aziendali.

Il SGSI è supervisionato dal Responsabile del Sistema di Gestione della Sicurezza delle Informazioni ("**RSGSI**"), con il supporto del Team SGSI.

6. Protezione delle informazioni e cybersicurezza

In coerenza con i requisiti ISO 27001, l'Azienda adotta misure di sicurezza:

6.1. Sicurezza logica e tecnica

- controllo degli accessi basato sul principio del least privilege;
- autenticazione forte e gestione delle identità;

- protezione delle reti e dei sistemi (firewall, monitoraggio, hardening);
- gestione delle vulnerabilità e aggiornamento continuo dei sistemi;
- protezione degli endpoint e dei dispositivi mobili.

6.2. Sicurezza dei dati e privacy

- classificazione e trattamento delle informazioni;
- adozione di misure di sicurezza (tecniche ed organizzative) volte a garantire che il trattamento dei dati personali sia conforme ai principi di "*accountability*" (tracciabilità delle decisioni, registrazione dei trattamenti e attività di audit), minimizzazione (trattamento limitato ai soli dati necessari al conseguimento delle finalità individuate), proporzionalità (valutazione dei rischi e adeguamento delle misure di sicurezza) nonché "*privacy by design*" e "*by default*" (integrazione della protezione dei dati fin dalla progettazione dei processi e dei servizi e, per impostazione predefinita, applicazione automatica delle misure idonee a garantire il trattamento dei soli dati personali strettamente necessari);
- gestione delle violazioni dei dati (data breach) secondo GDPR.

7. Gestione degli incidenti di sicurezza

Axitea S.p.A. ha definito processi strutturati per:

- rilevare, segnalare e gestire gli incidenti di sicurezza;
- mitigare l'impatto su servizi, clienti e parti interessate;
- garantire il miglioramento continuo attraverso l'analisi degli eventi.

La gestione degli incidenti è parte integrante del SGSI ed è verificata periodicamente.

8. Continuità operativa e resilienza

L'Azienda assicura la continuità dei servizi critici (c.d. *business continuity*) tramite:

- analisi dei rischi e degli impatti sul business;
- piani di continuità operativa e disaster recovery;
- test periodici e aggiornamento dei piani;
- integrazione della *cyber resilience* nei processi aziendali.

9. Sicurezza della catena di fornitura

Axitea S.p.A. riconosce l'importanza della sicurezza delle terze parti e della *Supply chain* in particolare e:

- valuta i rischi cyber associati a fornitori e partner;
- include requisiti di sicurezza nei contratti;
- promuove la conformità dei fornitori ai requisiti di sicurezza e protezione dei dati, assicurando che i relativi obblighi siano chiaramente definiti e formalizzati;
- monitora nel tempo il livello di rischio della supply chain.

10. Consapevolezza e formazione

L'Azienda promuove programmi strutturati di:

- formazione periodica sulla sicurezza delle informazioni e sulla protezione dei dati personali;

- sensibilizzazione sui rischi cyber e sulle minacce emergenti;
- responsabilizzazione del personale e delle terze parti.

11. Miglioramento continuo e riesame

Il SGSI è soggetto a un processo continuo di:

- pianificazione, attuazione, verifica e miglioramento;
- audit interni e riesami della Direzione;
- aggiornamento della presente Politica in funzione dell'evoluzione del contesto normativo, tecnologico e delle minacce cyber.

Milano, 25 febbraio 2026

LA DIREZIONE