POLITICA DELLA QUALITÀ E DELLA SICUREZZA DELLE INFORMAZIONI

MOD M05A - Rev. 0 | Anno 2025

---

0. Generalità

PA ABS fa parte del Gruppo ALVEO con un'esperienza più che ventennale nel mercato. La missione è supportare le aziende nel percorso di trasformazione digitale, offrendo consulenza e servizi avanzati di Business Integration e digitalizzazione.

Le competenze spaziano dalla progettazione e implementazione di architetture tecnologiche alla gestione di ecosistemi complessi, fino alla reingegnerizzazione dei processi aziendali. Ci occupiamo dell'implementazione di sistemi ERP e dello sviluppo di soluzioni specifiche per settori strategici come Industria, Finanza, Sanità e Pubblica Amministrazione, rivolgendoci sia alle grandi aziende che alle PMI.

---

1. Competenze e Specializzazioni

- **SAP & Business Technology**

Siamo **Gold Partner SAP** e aiutiamo le aziende a innovare con **S/4HANA® Cloud** (RISE with SAP e GROW with SAP). Con **SAP Business Technology Platform**, integriamo sistemi, applicazioni e processi e forniamo strumenti avanzati di analisi dati con **SAP Analytics Cloud e SAP Datasphere.**

- **Soluzioni per la Pubblica Amministrazione**

Progettiamo software e piattaforme conformi ai requisiti del **RIUSO**, che possono essere utilizzati in iniziative finanziate dal **PNRR**.

- **Finanza e IT**

Offriamo **consulenza tecnologica e funzionale**, progettazione software e gestione di applicazioni e sistemi per il settore finanziario.

- **Cybersecurity e Open Source**

Siamo **Advanced Partner RedHat** e collaboriamo con **Trellix e Skyhigh** per offrire soluzioni avanzate di cybersecurity.

---

2. Obiettivo della Politica

La presente **Politica della Qualità e della Sicurezza delle Informazioni** rappresenta il documento fondamentale di governance e impegno di PA ABS nei confronti della gestione integrata della qualità e della sicurezza delle informazioni.

Questo documento è il principale strumento di riferimento per tutti i temi correlati alla **Quality Assurance** e alla **Information Security**, ed è reso disponibile a tutto il personale, alle parti interessate, ai clienti e ai fornitori mediante pubblicazione nel sito web aziendale, nella intranet e nelle sedi fisiche.

La presente politica definisce e organizza l'approccio strategico di PA ABS verso la protezione della riservatezza, dell'integrità e della disponibilità delle informazioni, nonché gli aspetti organizzativi, tecnici e manageriali collegati.

---

3. Diffusione della Politica

Questa Politica è il documento di riferimento centrale per i temi di **Quality & Information Security** e deve essere condivisa con:

- Tutto il personale dipendente e contrattuale;
- Consulenti e collaboratori esterni;
- Terze parti rilevanti coinvolte in attività che impattano sulla sicurezza delle informazioni, sulla qualità e sui servizi IT;
- Partner commerciali e fornitori critici;
- Clienti, in particolare quelli che sottoscrivono servizi cloud e di gestione dati sensibili.

Il documento è sottoposto a **riesame almeno annuale** dalla Direzione e, in caso di modifiche significative, una nuova versione viene pubblicata nella intranet aziendale e comunicata a tutta la popolazione aziendale tramite comunicato ufficiale.

L'approvazione e l'emissione del documento sono di competenza del **Responsabile del Sistema di Gestione Integrato (RSGI)** in qualità di rappresentante della Direzione per la Qualità e la Sicurezza.

---

4. Politica per la Qualità

4.1 Mission - Vision - Valori

MISSION

Garantire ai clienti un'esperienza di digitalizzazione eccellente, sostenibile e innovativa, coprendo con competenza e attenzione ogni ambito IT e settore aziendale.

Uniamo alla ricerca dell’eccellenza e alla cultura del fare, una visione globale e un’esecuzione dettagliata, per fornire ai nostri clienti i migliori strumenti per raggiungere i loro obiettivi.

VISION

In un mondo in cui le persone e la tecnologia sono esponenzialmente interdipendenti, ci posizioniamo alla convergenza tra strategia di business e digitale.

Accompagniamo i clienti a costruire un futuro trasformativo basato su pragmatismo e innovazione, mirando a essere partner nella creazione di un futuro sostenibile per loro, i loro stakeholder, il loro ecosistema e la società.

VALORI

Affidabilità

Per i nostri clienti ci siamo sempre, garantendo un supporto continuo e affidabile. Crediamo in una cooperazione forte, nella trasparenza e nelle relazioni a lungo termine. **Si tratta di esserci, sempre.**

Innovazione

Crediamo che la natura pervasiva del digitale implichi la necessità di pensare ogni giorno in termini di Futuro e di Innovazione, sia nei progetti più trasformativi che in quelli tradizionali. **Guardiamo costantemente avanti.**

Pertinenza

Crediamo che l'unione di passione, competenza e esperienza sia ciò che rende il nostro approccio unico e ciò che aiuta noi e i nostri clienti a trovare ciò che meglio risponde alle loro necessità. **Aiutiamo a fare ciò che è giusto**.

Efficacia

Trasformiamo idee in soluzioni attraverso spirito imprenditoriale, creatività, iniziativa, proattività e il coraggio di osare, trovando soluzioni agili per scenari complessi. Aiutiamo a rendere le cose semplici.

Sostenibilità

Crediamo in una crescita sostenibile fondata sull'equilibrio di ambiente, economia ed equità, che supporti le generazioni attuali pur proteggendo quelle future. **Ci prendiamo cura di presente e futuro.**

4.2 Impegno per la Qualità

PA ABS ha scelto di sviluppare e mantenere un **Sistema di Gestione per la Qualità** conforme alla norma **UNI EN ISO 9001:2015** ("Sistema di Gestione per la qualità – Requisiti").

La qualità dei servizi erogati è una diretta conseguenza dell'approccio operativo della nostra organizzazione, che si impegna a:

- Allineare l'organizzazione, i processi interni e l'offerta ai clienti ai più riconosciuti standard internazionali;
- Considerare sistematicamente le esigenze di tutte le parti interessate (stakeholder interni ed esterni);
- Effettuare annualmente un'**analisi dei rischi aziendali** per definire obiettivi e azioni di mitigazione;
- Implementare e mantenere **controlli di qualità** su tutti i prodotti e servizi erogati;
- Misurare e monitorare la qualità tramite indicatori specifici (KPI) e riesame periodico della Direzione.

4.3 Obiettivi della Qualità

Gli obiettivi di qualità di PA ABS sono misurabili, quantificabili e allineati con la strategia aziendale. Essi vengono:

- Esplicitati a inizio anno in coerenza con la politica;
- Monitorati durante le fasi di riesame del sistema qualità;
- Revisionati periodicamente dalla Direzione sulla base dei risultati aziendali.

4.4 Responsabilità Organizzativa

Tutti i Responsabili aziendali sono tenuti a:

- Soddisfare tutti i requisiti del Sistema Qualità e diffonderne la conoscenza;
- Monitorare sistematicamente le attività operative di propria competenza;
- Assicurare che il personale operi con adeguata competenza, formazione e consapevolezza;
- Implementare le procedure stabilite e i criteri di controllo della qualità.

Tutto il personale è impegnato a perseguire il continuo miglioramento della qualità nello sviluppo delle proprie attività, nel quadro della politica e delle direttive aziendali.

---

5. Politica per la Sicurezza delle Informazioni

5.1 Dichiarazione di Principio

PA ABS ritiene che la **sicurezza delle informazioni** rappresenti un fattore critico di successo per la sostenibilità del business, la protezione del patrimonio aziendale, la tutela dei dati dei clienti e il rispetto dei diritti e delle libertà delle persone fisiche i cui dati sono trattati.

Per PA ABS, in particolare, la sicurezza delle informazioni è una responsabilità **strategica e prioritaria**, integrata in ogni aspetto della governance, della gestione operativa e dello sviluppo tecnologico.

5.2 Obiettivo Primario

La gestione della Sicurezza delle Informazioni ha come obiettivi primari:

1. **Protezione del patrimonio informativo** – Tutela delle conoscenze aziendali, della proprietà intellettuale e dei dati critici;
2. **Protezione dei dati dei clienti** – Garanzia della riservatezza, integrità e disponibilità dei dati affidati a PA ABS in qualità di Titolare o Responsabile del Trattamento;
3. **Protezione dei dati personali** – Tutela delle persone fisiche i cui dati personali sono trattati, in conformità al GDPR e alle leggi sulla privacy;
4. **Continuità operativa** – Assicurazione della disponibilità e della resilienza dei servizi erogati;
5. **Conformità normativa** – Adempimento degli obblighi derivanti da leggi, regolamenti, standard internazionali e contratti con clienti.

5.3 Ambito di Applicazione

La Politica della Sicurezza delle Informazioni si applica a:

- **Tutto il personale interno** di PA ABS (dipendenti, consulenti, tirocinanti);
- **Terze parti e partner** che collaborano con PA ABS o accedono alle informazioni gestite;
- **Tutti i processi, servizi e risorse** coinvolti nella progettazione, realizzazione, avviamento ed erogazione continuativa dei servizi di PA ABS;
- **Tutte le forme di informazione** (digitali, cartacee, vocali, visive) trattate nell'ambito del sistema informativo aziendale.

5.4 Pilastri della Sicurezza: I Principi Fondamentali

Tutte le persone che lavorano e collaborano con PA ABS sono impegnate a rispettare i seguenti **principi fondamentali della sicurezza delle informazioni**:

5.4.1 Riservatezza

Assicurare che l'informazione sia accessibile esclusivamente ai soggetti e/o ai processi debitamente autorizzati, prevenendo che informazioni sensibili siano rese disponibili o divulgate a persone o entità non autorizzate.

5.4.2 Integrità

Salvaguardare la consistenza, l'accuratezza e la completezza dell'informazione, prevenendo modifiche non autorizzate e garantendo che l'informazione non subisca alterazioni dovute a errori, azioni volontarie, malfunzionamenti dei sistemi o danni accidentali.

5.4.3 Disponibilità

Assicurare che gli utenti autorizzati abbiano accesso alle informazioni e alle risorse critiche quando necessario, garantendo operatività continua dei servizi, prevenendo interruzioni e riducendo i rischi legati a indisponibilità (accessi non autorizzati, furto di dati, denial of service).

5.4.4 Controllo

Assicurare che la gestione dei dati, dei sistemi e dei processi avvenga sempre attraverso meccanismi sicuri, testati, documentati e sottoposti a monitoraggio continuo.

5.4.5 Privacy

Garantire la protezione e il controllo dei dati personali, il rispetto dei diritti degli interessati e l'adempimento degli obblighi derivanti dal GDPR e dalle leggi sulla privacy applicabili.

5.5 Aree Critiche della Gestione della Sicurezza

La Politica della Sicurezza delle Informazioni di PA ABS comprende e organizza le seguenti aree critiche:

- **Identificazione delle aree critiche e classificazione dei dati** – Mappatura e categorizzazione del patrimonio informativo in base al valore e alla sensibilità;
- **Gestione dei rischi** – Valutazione sistematica dei rischi, definizione delle misure di mitigazione e controllo continuo;

- **Gestione della rete e dei sistemi** – Progettazione, manutenzione, monitoraggio e aggiornamento dell'infrastruttura tecnologica;
- **Gestione delle vulnerabilità e delle patch** – Identificazione, tracciamento e rimedio delle lacune di sicurezza;
- **Gestione degli incidenti e delle anomalie** – Riconoscimento, risposta, documentazione e apprendimento dagli incidenti di sicurezza;
- **Controllo degli accessi (logici e fisici)** – Autorizzazione, autenticazione, tracciamento e revoca dei diritti di accesso;
- **Gestione della privacy e della compliance** – Implementazione delle misure tecniche e organizzative per il rispetto della normativa sulla protezione dei dati;
- **Business Continuity e Disaster Recovery** – Piani e procedure per assicurare la continuità operativa in caso di disastri o anomalie critiche;
- **Aspetti tecnici, manageriali e di business** – Integrazione della sicurezza in tutti gli ambiti organizzativi.

5.6 Approccio Organizzativo alla Sicurezza

Per perseguire gli obiettivi di sicurezza, PA ABS pone grande attenzione a:

- **Progettazione della struttura tecnologica** – Infrastrutture cloud sicure, sistemi di rete robusti, architetture resilienti;
- **Gestione della struttura fisica** – Controllo degli accessi ai locali;
- **Gestione della struttura logica** – Sistemi di backup, disaster recovery, segmentazione di rete, crittografia;
- **Gestione della struttura organizzativa** – Chiari ruoli e responsabilità, procedure documentate, competenze specializzate, cultura della sicurezza.

PA ABS si impegna quindi a sviluppare e mantenere un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** che garantisca in modo continuativo la **disponibilità, l'integrità e la riservatezza** dei dati, delle informazioni, degli accessi e dei servizi gestiti.

---

6. Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

6.1 Fondamenti

Per dare attuazione concreta alla propria politica della sicurezza delle informazioni, PA ABS ha sviluppato e si impegna a mantenere un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** conforme ai requisiti delle seguenti norme:

- **ISO/IEC 27001:2022** – "Information security, cybersecurity and privacy protection – Information security management systems – Requirements" (data pubblicazione: 25 ottobre 2022);
- **ISO/IEC 27017:2021** – "Code of practice for information security controls based on ISO/IEC 27002 for cloud services" (2021);

- **ISO/IEC 27018:2019/2020** – "Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors" (2019/2020).

Inoltre, PA ABS assicura il pieno rispetto delle leggi e dei regolamenti cogenti, contrattualmente vincolanti e volontariamente adottati nel territorio e nei settori in cui opera.

6.2 Impegno Operativo

Nell'ambito della gestione dei servizi offerti, PA ABS assicura:

- **Osservanza dei livelli di sicurezza stabiliti** attraverso l'implementazione e il mantenimento del SGSI conforme agli standard ISO e alla legislazione applicabile;
- **Rispetto della normativa vigente e degli standard internazionali** per l'infrastruttura tecnologica, organizzativa e per i servizi erogati;
- **Selezione rigorosa di fornitori e partner affidabili** dal punto di vista della gestione sicura delle informazioni e della protezione dei dati personali, mediante clausole contrattuali specifiche;
- **Continuità del miglioramento** del SGSI attraverso riesame periodico, valutazione dei rischi aggiornati, adeguamento alle normative emergenti e implementazione di best practice.

6.3 Campo di Applicazione del SGSI

Il SGSI di PA ABS si applica a:

- **Tutto il personale interno** e quello delle terze parti che collaborano alla gestione delle informazioni;
- **Tutti i processi, le risorse e i sistemi** coinvolti nella progettazione, realizzazione, avviamento ed erogazione continuativa dei servizi;
- **Tutte le attività** che impattano sulla sicurezza delle informazioni, sulla qualità e sulla conformità normativa.

6.4 Garanzie fornite dal SGSI

La Politica della Sicurezza delle Informazioni di PA ABS, concretizzata nel SGSI, garantisce che:

1. **L'organizzazione abbia piena conoscenza** delle informazioni gestite e valuti di volta in volta la loro criticità, per implementare adeguati livelli di protezione;
2. **L'accesso alle informazioni avvenga in modo sicuro** e idoneo a prevenire i trattamenti non autorizzati o realizzati senza diritti necessari;
3. **L'organizzazione e le terze parti collaborino** al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
4. **L'organizzazione e le terze parti siano adeguatamente formate** e abbiano piena consapevolezza delle problematiche di sicurezza e privacy;
5. **Le anomalie e gli incidenti** aventi ripercussioni sul sistema informativo, sui servizi e sulla sicurezza aziendale siano tempestivamente riconosciuti, gestiti e documentati, minimizzando l'impatto sul business;
6. **L'accesso ai locali e alle aree fisiche** di PA ABS avvenga esclusivamente da personale autorizzato, garantendo la sicurezza dei locali e dei beni presenti;

7. **La conformità con i requisiti di legge** e il rispetto degli impegni di sicurezza stabiliti nei contratti con clienti e partner;
8. **La rilevazione tempestiva** di eventi anomali, incidenti, vulnerabilità e minacce dei sistemi informativi, per mantenere i livelli di sicurezza e disponibilità dei servizi;
9. **La business continuity aziendale** e il disaster recovery, attraverso l'applicazione di procedure e piani di sicurezza stabiliti;
10. **I trattamenti dei dati personali** (sia nei casi in cui PA ABS operi in qualità di Titolare che di Responsabile del Trattamento) avvengano nel pieno rispetto del **Regolamento (UE) 2016/679 (GDPR)**, della normativa nazionale sulla privacy e di ogni obbligo derivante da contratti e standard applicabili.

---

7. Dichiarazione di Impegno della Direzione

La Direzione di PA ABS si impegna formalmente e pubblicamente a garantire e implementare i seguenti principi e azioni nel contesto della gestione della sicurezza delle informazioni:

7.1 Protezione della Riservatezza

PA ABS si impegna a garantire la riservatezza delle informazioni attraverso:

- **Definizione puntuale delle responsabilità interne** per la gestione dei servizi e delle informazioni ad essi connesse;
- **Controllo degli accessi fisici** ai locali, agli archivi cartacei e alle aree critiche esclusivamente da parte di personale autorizzato e competente;
- **Controllo degli accessi logici** ai sistemi informativi, alle banche dati e agli archivi elettronici mediante autenticazione robusta e autorizzazione basata su ruoli;
- **Implementazione di misure di crittografia** per i dati in transito e a riposo, proporzionate al livello di sensibilità;
- **Gestione della documentazione riservata** secondo procedure definite, con tracciamento dell'accesso e della distribuzione.

7.2 Protezione dell'Integrità

PA ABS si impegna a garantire l'integrità delle informazioni attraverso:

- **Controllo degli accessi** alle risorse informatiche da parte di personale autorizzato e competente esclusivamente;
- **Implementazione di meccanismi di hashing e firma digitale** per verificare l'integrità dei dati critici;
- **Gestione dei backup** dei dati e delle configurazioni dei sistemi informativi con periodicità definita e testati regolarmente;
- **Monitoraggio continuo** delle modifiche non autorizzate ai dati e ai sistemi;
- **Change management rigoroso** per le modifiche ai sistemi, con tracciamento completo e approvazione preventiva.

7.3 Protezione della Disponibilità

PA ABS si impegna a garantire la disponibilità delle informazioni e dei servizi attraverso:

- **Identificazione dei ruoli e delle funzioni** critiche per la continuità operativa;
- **Definizione dei diritti di accesso** alle informazioni e agli assets aziendali necessari per la gestione dei servizi;
- **Implementazione di sistemi ridondanti** e infrastrutture robuste per prevenire guasti singoli;
- **Piano di Business Continuity e Disaster Recovery** testato regolarmente, con obiettivi RTO/RPO definiti;
- **Monitoraggio 24/7** delle infrastrutture critiche e risposta rapida agli incidenti.

7.4 Coinvolgimento e Responsabilizzazione di Dipendenti e Terze Parti

PA ABS si impegna a garantire che:

- **Dipendenti, fornitori, partner, appaltatori e terze parti** coinvolte nel trattamento di informazioni che rientrano nel campo di applicazione del SGSI **accettino formalmente** gli obblighi e le responsabilità di propria pertinenza;
- **Clausole di riservatezza e di sicurezza** siano presenti in tutti i contratti con terze parti, con conseguenze chiare in caso di violazione;
- **Ogni persona** sia consapevole del proprio ruolo e dell'impatto delle proprie azioni sulla sicurezza delle informazioni e sulla conformità normativa.

7.5 Controllo degli Accessi

PA ABS si impegna a garantire che ogni accesso, di tipo fisico o informatico, sia:

- **Autorizzato in base al principio della "conoscenza minima"** (need-to-know): l'accesso è concesso al personale abilitato solo per le informazioni essenziali allo svolgimento delle proprie funzioni;
- **Autorizzato sulla base della funzione lavorativa**: l'accesso è correlato alle responsabilità specifiche assegnate;
- **Controllato mediante sistemi di log e audit** che registrano accessi, azioni, modifiche e anomalie;
- **Monitorato continuativamente** al fine di rilevare e contenere accessi non autorizzati o uso improprio;
- **Revocato tempestivamente** quando l'accesso non è più necessario (cambio di ruolo, cessazione del rapporto, ecc.).

L'accesso ai locali di PA ABS è autorizzato, controllato e monitorato in linea con la Politica Fisica di Sicurezza.

7.6 Formazione, Consapevolezza e Competenza

PA ABS si impegna a garantire che:

- **Ogni dipendente, fornitore, appaltatore e terza parte** sia consapevole del proprio ruolo, delle responsabilità e dell'impatto delle proprie azioni sulla sicurezza delle informazioni;
- **Ogni risorsa** sia adeguatamente formata e addestrata sulle politiche, le procedure e i protocolli relativi alla gestione della sicurezza delle informazioni, con periodicità definita e contenuti aggiornati;

- **Programmi di awareness** sulla cybersecurity, sulla privacy, sul phishing e su altre minacce siano erogati continuativamente;
- **Verifiche periodiche** della comprensione e dell'adesione alle politiche siano effettuate tramite quiz, test pratico e simulazioni.

7.7 Conformità Normativa e Contrattuale

PA ABS si impegna a garantire che:

- **I trattamenti delle informazioni, delle attività, delle risorse e delle soluzioni** inerenti la protezione delle informazioni di PA ABS o gestiti per conto dei propri clienti siano **conformi a**:
    - Leggi e regolamenti cogenti (GDPR, NIS2, Perimetro di Sicurezza Nazionale Cibernetica, normative settoriali, ecc.);
    - Obblighi contrattuali derivanti da contratti con clienti e partner;
    - Standard internazionali volontariamente adottati (ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018).
- **Verifiche di conformità** periodiche siano effettuate al fine di assicurare l'aderenza continua;
- **Adeguamenti normativi** siano implementati tempestivamente quando norme nuove o modificate diventano applicabili.

7.8 Protezione e Classificazione delle Risorse

PA ABS si impegna a garantire che:

- **Ogni attività, risorsa e informazione** pertinente all'ambito del SGSI sia protetta contro i problemi legati a riservatezza, integrità e disponibilità;
- **Il livello di protezione** sia proporzionato al valore, alla sensibilità e alla criticità della risorsa;
- **La classificazione** di dati, sistemi e processi sia eseguita, documentata e mantenuta aggiornata;
- **Procedure di smaltimento sicuro** dei dati e delle risorse a fine vita siano implementate e verify.

7.9 Responsabilizzazione di Tutto il Personale

PA ABS si impegna a garantire che tutto il personale sia responsabilizzato e tenuto a:

a) Rispetto della Normativa

Garantire il rispetto delle norme, leggi e regolamenti vigenti di natura cogente, contrattuale e volontaria rese applicabili negli ambiti del SGSI (GDPR, ISO 27001, normative locali e settoriali).

b) Protezione del Patrimonio Informativo

Proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite da PA ABS, inclusa la proprietà intellettuale e il patrimonio informativo aziendale o affidato da clienti.

c) Custodia dei Beni Materiali

Avere cura e responsabilità dei beni materiali, dei sistemi informatici e delle risorse di PA ABS, prevenendone il furto, il danneggiamento e l'uso improprio.

d) Gestione Appropriata delle Informazioni

Salvaguardare e gestire in modo appropriato ogni informazione, dato e documento afferenti le attività di propria competenza, seguendo le procedure stabilite.

e) Segnalazione di Violazioni

Contattare tempestivamente la Direzione, il Responsabile della Sicurezza delle Informazioni (RSI) e/o altre autorità competenti (es. Garante Privacy, Autorità competenti) in caso di:

- Effettive violazioni della sicurezza (data breach, accessi non autorizzati, ecc.);
- Sospette violazioni (comportamenti anomali, tentative di accesso, ecc.);
- Debolezze o vulnerabilità nei sistemi e nei processi.

f) Proposte di Miglioramento

Segnalare qualsiasi necessità di modifiche, adeguamenti o miglioramenti alle procedure relative alla gestione della sicurezza delle informazioni e dei sistemi informativi.

---

8. Riesame e Aggiornamento della Politica

Questa Politica della Qualità e della Sicurezza delle Informazioni è sottoposta a **riesame almeno annuale** dalla Direzione al fine di assicurare:

- Il suo continuo miglioramento e l'efficacia del SGSI;
- L'allineamento con l'evoluzione del contesto normativo, tecnologico e commerciale;
- La rispondenza alle esigenze delle parti interessate e agli esiti delle valutazioni dei rischi;
- L'inclusione di nuovi requisiti contrattuali o legali;
- L'incorporazione di lezioni apprese da incidenti, audit e valutazioni esterne.

Ogni revisione materiale della Politica è comunicata formalmente a tutto il personale, ai clienti e ai partner attraverso canali ufficiali (email, intranet, sito web, riunioni).

---

9. Sottoscrizione e Approvazione

Documento	Politica della Qualità e della Sicurezza delle Informazioni
Revisione	Rev. 0 - Anno 2025
Data di Emissione	01 luglio 2025

Responsabile dell'Approvazione	Responsabile della Sicurezza delle Informazioni (RSI) / Direzione
Destinatari	Tutto il personale, clienti, partner, fornitori, terze parti

Firma Digitale della Direzione:

Responsabile della Sicurezza delle Informazioni

Data: 01 luglio 2025
