**POLITICA PER LA SICUREZZA DEI SISTEMI DI INFORMAZIONE (SSI)**

**Brambati SpA** considera la Sicurezza dei Sistemi di Informazione (SSI) un elemento strategico per la tutela dei propri dati, processi e relazioni con clienti, fornitori e stakeholder. La presente Politica è coerente con i principi delle Direttive Europee NIS2 e REC, si ispira alle migliori pratiche della norma ISO/IEC 27001 e integra i requisiti del Sistema di Gestione Integrato aziendale.

**Principi fondamentali**

I principi fondamentali che guidano la gestione della sicurezza delle informazioni in **Brambati SpA** si basano su:

* Disponibilità → garantire che i sistemi e le informazioni siano accessibili e utilizzabili quando richiesto dai processi aziendali e dagli utenti autorizzati;
* Integrità → assicurare l’accuratezza, la completezza e l’affidabilità dei dati e delle informazioni lungo l’intero ciclo di vita;
* Confidenzialità → proteggere le informazioni da accessi non autorizzati, garantendo che solo i soggetti legittimati possano accedervi e trattarle.

**Gestione dei rischi**

**Brambati SpA** adotta un approccio sistematico di Analisi dei Rischi e delle Opportunità per identificare, valutare e mitigare le minacce alla sicurezza delle informazioni, considerando anche l’impatto dei cambiamenti climatici e di eventi estremi sulla continuità dei sistemi ICT. In particolare, vengono analizzati:

* Cyber attacchi (malware, ransomware, phishing, accessi non autorizzati);
* Guasti tecnici, blackout e indisponibilità dei sistemi critici;
* Eventi naturali e climatici che possono compromettere infrastrutture e data center;
* Rischi derivanti da fornitori esterni, partner e supply chain digitale;
* Errori umani e mancanza di consapevolezza del personale.

Le opportunità individuate comprendono:

* Adozione di tecnologie innovative e sicure (cloud resiliente, AI, blockchain);
* Sviluppo di una cultura aziendale della cyber security attraverso formazione continua;
* Maggiore fiducia di clienti e stakeholder grazie a sistemi sicuri e affidabili;
* Resilienza organizzativa e capacità di risposta rapida a incidenti e crisi.

**Impegni della Direzione**

La Direzione di **Brambati SpA** si impegna a:

* Assicurare la conformità alle leggi, regolamenti e direttive applicabili (NIS2, REC, GDPR, Codice Privacy);
* Definire obiettivi e programmi di miglioramento della sicurezza delle informazioni;
* Garantire risorse, ruoli e responsabilità per la gestione della sicurezza;
* Riesaminare periodicamente la presente Politica e il sistema di sicurezza delle informazioni per verificarne efficacia e adeguatezza;
* Integrare i principi di sicurezza by design e by default nello sviluppo e nella gestione di processi e sistemi informativi;
* Promuovere la sensibilizzazione e la formazione di tutto il personale in materia di sicurezza delle informazioni.

**Obiettivi operativi**

Gli obiettivi operativi che **Brambati SpA** si pone in materia di SSI comprendono:

* Proteggere i dati personali, industriali e proprietari da accessi e trattamenti non autorizzati;
* Garantire continuità operativa e capacità di ripristino rapido tramite piani di Business Continuity e Disaster Recovery;
* Monitorare costantemente i sistemi per rilevare e rispondere tempestivamente a incidenti di sicurezza;
* Gestire correttamente gli accessi, le identità digitali e i privilegi degli utenti;
* Effettuare regolarmente backup sicuri e test di ripristino;
* Valutare e monitorare i fornitori critici e i servizi in outsourcing per garantirne l’allineamento agli standard di sicurezza aziendali.

**Monitoraggio e miglioramento**

**Brambati SpA** garantisce un monitoraggio costante e il miglioramento continuo della sicurezza dei sistemi di informazione tramite:

* Definizione e tracciamento di KPI (incidenti gestiti, tempi medi di ripristino, % formazione effettuata, disponibilità sistemi critici);
* Audit interni ed esterni per verificare la conformità alle politiche e agli standard di sicurezza;
* Analisi periodica delle minacce e aggiornamento delle contromisure tecniche e organizzative;
* Coinvolgimento attivo della Direzione e dei responsabili operativi nei processi decisionali legati alla SSI.

**Integrazione sull'uso dell'Intelligenza Artificiale (IA)**

**Brambati SpA**, pur non sviluppando sistemi di Intelligenza Artificiale, ne fa uso in alcuni processi gestionali, produttivi e di supporto. Per questo motivo, l’azienda riconosce l’importanza di garantire che tali strumenti siano utilizzati in modo sicuro, responsabile e conforme alla normativa europea, in particolare al Regolamento (UE) AI Act e al GDPR.

In relazione all’utilizzo di strumenti di IA, **Brambati SpA** si impegna a:

* Applicare i principi fondamentali di disponibilità, integrità e confidenzialità anche ai dati e agli algoritmi utilizzati dai sistemi di IA;
* Valutare e mitigare i rischi legati a bias, discriminazioni algoritmiche e opacità delle decisioni automatizzate;
* Verificare la conformità dei fornitori di soluzioni IA alle normative europee e agli standard etici di settore;
* Garantire trasparenza e accountability nell’uso degli strumenti di IA, assicurando che le decisioni critiche non siano mai affidate esclusivamente a sistemi automatizzati;
* Integrare l’IA nei processi di formazione, audit e monitoraggio della sicurezza dei sistemi informativi.

La presente Politica per la Sicurezza dei Sistemi di Informazione è diffusa a tutto il personale, resa disponibile agli stakeholder e pubblicata sul sito web aziendale. Essa rappresenta l’impegno formale di **Brambati SpA** a proteggere i propri asset informativi, garantendo disponibilità, integrità e confidenzialità, e a perseguire un miglioramento continuo in materia di sicurezza informatica.

 Data Direzione **Brambati SpA**

Codevilla, 01/09/2025 ………………………………….