Politica integrata | Qualità, Sicurezza dei Dati delle Informazioni e Cybersecurity di BIG DIGITAL

Riferimenti Normativi: ISO 9001:2015 | ISO/IEC 27001:2022

1. Visione e Impegno della Direzione

Big Digital riconosce che la qualità dei propri servizi digitali e la protezione delle informazioni proprie e dei propri clienti sono pilastri inscindibili del proprio successo commerciale e della propria reputazione.

La Direzione si impegna a fornire le risorse necessarie per mantenere un **Sistema di Gestione Integrato (SGI)** volto al miglioramento continuo e alla piena soddisfazione dei requisiti legali, contrattuali e normativi.

2. Obiettivi Strategici per la Qualità (ISO 9001)

Per garantire l'eccellenza nei processi di trasformazione digitale, Big Digital si pone i seguenti obiettivi:

- **Customer Centricity:** Comprendere le esigenze dei clienti per offrire soluzioni tecnologiche che superino le loro aspettative.
- **Efficienza Operativa:** Ottimizzare i processi interni per ridurre sprechi e tempi di consegna (Time-to-Market).
- **Coinvolgimento delle persone:** Valorizzare le competenze del team attraverso la formazione continua e un ambiente di lavoro stimolante.
- **Rapporti con i Partner:** Selezionare fornitori che condividano i medesimi standard di qualità e affidabilità.

3. Obiettivi Strategici per la Sicurezza delle Informazioni (ISO 27001)

Data la natura del business, la protezione dei dati è una priorità assoluta. Big Digital garantisce:

- **Riservatezza:** L'accesso alle informazioni è consentito solo ai soggetti autorizzati.
- **Integrità:** Salvaguardia dell'accuratezza e della completezza delle informazioni e dei metodi di elaborazione.

- **Disponibilità:** Garantire che gli utenti autorizzati abbiano accesso alle informazioni e ai beni associati quando richiesto.
- **Gestione del Rischio:** Identificare preventivamente le minacce informatiche e fisiche, implementando controlli per mitigare i rischi a un livello accettabile.

4. Principi Cardine dell'SGI

1. **Approccio per Processi e Risk-based Thinking:** Ogni decisione è guidata dall'analisi dei rischi e delle opportunità.
2. **Compliance:** Rispetto rigoroso del GDPR e delle normative vigenti in ambito cyber-security.
3. **Miglioramento Continuo:** Il sistema non è statico; viene periodicamente revisionato tramite audit interni e riesami della Direzione per garantirne l'efficacia.
4. **Consapevolezza:** Ogni collaboratore è formato e consapevole del proprio ruolo nel proteggere il valore aziendale e la privacy dei dati trattati.

Bologna, 29/05/2026