

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

Standard ISO 27001:2013

History

Version	Date	Author	Modifications
1.0	31/01/2020	Alessio Zanforlin	
2.0	01.06.2021	Valerio Savino - CISO	Approvazione Politica da parte del CISO di recente nomina

Approval

Approved by	Date
Enrico Bazzi	01.06.2021

Data classification

Type	Date
Internal	01.06.2021

Contesto

Jakala S.p.A. è una realtà internazionale che nasce dall'unione di Jakala Marketing Solutions, specializzata nel mondo dei c.d. "marketing services", Seri System S.p.A., società specializzata nello sviluppo di strategie di marketing personalizzate, basate su programmi di fidelizzazione e strategie digitali in diversi settori, Value Lab, società di management consulting, analytics e information technology e Volponi S.p.A. società italiana specializzata in soluzioni di comunicazione integrata a supporto delle attività di fidelizzazione della "customer base" (di seguito anche "Jakala").

La diffusione di Jakala in tutto il mondo nel settore del loyalty, engagement, marketing services advisory, data & analytics e CRM evoluto, offre ai clienti supporto in ambito strategico, analitico, digitale e tecnologico per la gestione multicanale di clienti, canali e forza vendita, al fine di aiutarli a massimizzare le proprie vendite attraverso la trasformazione dei dati in ricavi aggiuntivi.

Questa attività core viene realizzata con un modello integrato che unisce la capacità di analizzare e interpretare i dati, di sviluppare e integrare piattaforme di engagement e di gestire i contenuti in grado di influenzare l'interazione tra brand, canali e consumatori con un modello di remunerazione legato anche ai risultati generati.

In questo contesto, Jakala ha di fatto una posizione privilegiata avendo nel proprio "portfolio" tutti gli assets necessari a sostenere la competizione, con un know-how diversificato ed integrato, dando origine ad un modello che è un "unicum" sul mercato. Data la natura delle attività, particolare attenzione è garantita alla sicurezza delle informazioni, fattore fondamentale anche per assicurare ai propri clienti la tutela, la riservatezza e la disponibilità del loro patrimonio informativo.

La presente politica si applica durante tutto il ciclo di progettazione e sviluppo dei progetti di Jakala, ove sono adottate misure sia tecniche che organizzative, secondo regole e criteri previsti dalle "best practice" internazionali e dagli standard internazionali di riferimento.

Scopo

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da Jakala al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

Ambito di applicazione

La politica per la sicurezza delle informazioni di Jakala si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

Politica

Jakala intende garantire la sicurezza delle informazioni trattate, proteggendole dalle possibili minacce, interne o esterne, intenzionali o accidentali, che possano comprometterne la disponibilità,

l'integrità o la riservatezza. Inoltre, è obiettivo primario dell'organizzazione assicurare la continuità dei servizi erogati.

Le politiche di sicurezza delle informazioni, si applicano a tutte le attività di analisi, progettazione, sviluppo e manutenzione dei prodotti e servizi, ed ai dati ad esse collegati.

La gestione della sicurezza delle informazioni è basata sui seguenti principi:

- valutare il livello di sicurezza delle informazioni gestite, al fine di poter stabilire gli adeguati livelli di protezione da garantire;
- adottare un processo di valutazione e gestione del rischio;
- garantire l'attuazione di adeguate misure di sicurezza, a livello fisico, tecnologico e organizzativo;
- assicurare che gli incidenti aventi ripercussioni sulla sicurezza delle informazioni siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione, al fine di minimizzare l'impatto sul business;
- identificare periodicamente gli obiettivi dell'organizzazione relativi alla sicurezza delle informazioni, stabilire i piani per il loro raggiungimento e controllarne lo stato di attuazione;
- garantire l'adeguatezza del Sistema di Gestione della Sicurezza delle Informazioni in caso di cambiamenti del contesto interno o esterno dell'organizzazione;
- assicurare la conoscenza da parte del personale della politica e degli obiettivi per la sicurezza delle informazioni e del loro contributo all'efficacia del sistema;
- assicurare la competenza e l'adeguata formazione del personale;
- garantire l'attuazione degli adeguati livelli di sicurezza da parte di fornitori, partner, etc.;
- monitorare e migliorare in modo continuo le prestazioni e l'efficacia del sistema;
- assicurare la conformità a tutte le normative e i regolamenti applicabili all'organizzazione e a tutti i contratti stipulati, ed in particolare alla normativa nazionale e comunitaria in materia di tutela dei dati personali.

Responsabilità della politica di sicurezza delle informazioni

Il Chief Information Security Officer è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.

