PROMOTICA
PEOPLE DRIVEN COMPANY

Politica Integrata Qualità e Sicurezza delle Informazioni

Policy

Società Promotica Spa

Versione 00

Data Sep 24, 2024

Rev.	Motivo revisione	Classificazione	Data revisione
00	Prima redazione documento	Public	Sep 24, 2024

Via Monte Baldo, 111
25015 Desenzano del Garda (BS)
+39 030.911.801
info@promotica.it
P.IVA e C.F.: 02394460980
promotica.it

Sommario

Introduzione

Il Sistema di Gestione Integrato di Promotica S.p.A. è sviluppato in conformità alle seguenti norme:

- ISO 9001:2015 - Sistema di Gestione per la Qualità (SGQ), che rappresenta un elemento centrale dell'organizzazione e dei processi aziendali, focalizzato alla soddisfazione del Cliente
- ISO/IEC 27001: 2022 - Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), al fine di garantire riservatezza, integrità e disponibilità delle informazioni utilizzate

L'ambito di applicazione delle norme sopra citate è così differenziato:

SCHEMA	CAMPO DI APPLICAZIONE	SETTORE
ISO 9001 **ISO/IEC 27001**	Ideazione, esecuzione e gestione di operazioni promozionali, di marketing e di servizi finalizzati all'incentivazione delle vendite e della fidelizzazione del cliente tramite l'utilizzo di software innovativi	

Dove il codice EA definisce il Settore di Certificazione: EA35: Altri servizi

Il presente documento fornisce un quadro di insieme delle politiche adottate per la realizzazione del Sistema di Gestione Integrato aziendale, con l'intento di promuoverne l'attuazione e la diffusione all'interno dell'azienda e di favorire il raggiungimento degli obiettivi previsti.

A supporto di quanto espresso nel presente documento, è stato elaborato dall'Alta Direzione della Società la politica integrata Qualità e Sicurezza delle informazioni che esprime principi, obiettivi, impegno e leadership, relativamente al sistema di gestione integrato 9001 e 27001.

Scopo

La presente politica è utilizzata quale strumento per sensibilizzare l'intera organizzazione su principi di qualità, sicurezza delle informazioni aziendali, gestione dei servizi e continuità operativa.

Campo di applicazione

La presente politica si applica, sotto il governo ed il supporto della Direzione, a tutto il personale aziendale e ai clienti e fornitori coinvolti nel campo di applicazione del Sistema di Gestione Integrato.

Acronimi e abbreviazione

Nel documento sono utilizzati i seguenti acronimi:

- GDPR: General Data Protection Regulation
- DVR: Documento di Valutazione dei Rischi
- SGI: Sistema di Gestione Integrato
- SGQ: Sistema di Gestione per la Qualità
- SGSI: Sistema di Gestione per la Sicurezza delle Informazioni

Descrizione della Politica

La presente politica aziendale integrata è stata sviluppata sulla base degli standard internazionali che forniscono i requisiti di Sistemi di Gestione per la Qualità - ISO 9001:2015, per la Sicurezza delle Informazioni - ISO/IEC 27001:2022

Tale scelta corrisponde, essenzialmente, alle seguenti esigenze:

- definire un sistema che consenta di implementare e governare l'insieme delle misure organizzative, fisiche e logiche necessarie a garantire la qualità del servizio, la protezione delle informazioni aziendali ivi compresi i dati personali e garantisca la sicurezza e disponibilità dei servizi offerti, nel rispetto di regole a tutela dell'ambiente e della salute e sicurezza sul lavoro del personale
- individuare e includere i diversi ambiti di cui si compone un sistema di gestione integrato.

Il documento delinea i principi strategici ai quali intende ispirarsi per raggiungere i propri obiettivi. Tali principi possono essere sintetizzati in:

- Focalizzazione sul Cliente
- Leadership
- Partecipazione attiva delle persone
- Approccio per processi
- Miglioramento continuo
- Analisi dei Rischi
- Gestione delle relazioni
- Garanzia di Riservatezza, Integrità e Disponibilità delle Informazioni
- Esercizio dei diritti degli interessati in ambito privacy
- Continuità nel fornire prodotti ed erogare servizi a livelli predefiniti
- Salvaguardia della salute e sicurezza sul lavoro delle risorse umane.

Nel dettaglio i principali processi identificati sono:

- gestione dei servizi erogati
- gestione degli asset
- gestione delle risorse umane, in particolare organizzazione
- gestione della comunicazione
- gestione dei fornitori
- sicurezza fisica ed ambientale
- gestione operativa delle risorse informatiche
- controllo accessi
- progettazione, sviluppo, controllo, riesame, produzione ed erogazione del prodotto/servizio
- soddisfazione del Cliente
- gestione degli incidenti di sicurezza
- conformità

Missione Aziendale

Promotica ha come obiettivo l'ottimizzazione della già ampia gamma di servizi che ruotano attorno alle campagne di marketing, mettendo in atto all'esecuzione delle strategie e dei piani di sviluppo e crescita al fine di garantire professionalità di alto livello nel campo della consulenza e della gestione di tutte le fasi del processo promozionale. L'aspirazione della società è quella di incrementare le vendite dei clienti attraverso la fidelizzazione del consumatore, migliorare la brand advocacy, aumentare lo share of wallet. Le attività di comunicazione, grafica, web design, media planning e pubbliche relazioni che sono già inquadrate da Promotica, puntano a diventare sempre più strutturate e coese al fine di individuare la categoria merceologica e il mix di vendita più adatti a comporre le campagne ad-hoc.

Risorse da salvaguardare

Le risorse che Promotica si impegna a salvaguardare sono tutte quelle che sottendono ai processi strategici e che sono attentamente elencate nell'asset inventory aziendale. Le categorie principali sono:

- dati/documenti interni di clienti e fornitori
- asset fisici
- asset logici
- servizi
- personale

Obiettivi

I principi base che guidano l'azione di Promotica sono:

- ottenere la massima soddisfazione del cliente e delle altre parti interessate, quali, ad esempio, i cittadini, nel rispetto delle loro aspettative ed esigenze, fornendo servizi di elevata qualità;
- offrire un adeguato livello di sicurezza dei dati e delle informazioni trattate durante la gestione dei processi di delivery di servizi, identificando, valutando e trattando i rischi ai quali i servizi stessi possono essere soggetti;
- garantire la protezione dei dati personali nei trattamenti gestiti sia in qualità di Titolare sia in qualità di Responsabile del Trattamento;
- garantire che i propri servizi siano sistematicamente rispondenti agli SLA (Service Level Agreement) concordati con i rispettivi clienti;
- assicurare la continuità dei servizi grazie ad una adeguata allocazione di risorse atte a garantire l'identificazione e l'impatto di potenziali perdite, il mantenimento dei piani e delle strategie di ripristino;
- predisporre luoghi di lavoro sicuri e salubri, migliorare la salute e sicurezza sul lavoro, eliminare i pericoli e minimizzare i rischi.

Con la presente politica Promotica intende formalizzare i seguenti obiettivi generali nell'ambito del sistema di gestione integrato:

- Fornire con regolarità servizi che soddisfino i requisiti del cliente e quelli cogenti e normativi applicabili.
- Facilitare le opportunità per accrescere la soddisfazione del cliente.
- Affrontare rischi ed opportunità associati al contesto e ai propri obiettivi.
- Dimostrare la conformità ai requisiti specificati dal Sistema di Gestione Integrato.
- Preservare al meglio l'immagine dell'azienda quale soggetto affidabile e competente.
- Fornire pieno supporto e commitment al fine di raggiungere la compliance dei requisiti cogenti in maniera di trattamento di dati personali (GDPR).
- Proteggere il proprio patrimonio informativo in modo che:
  - le informazioni siano protette da accessi non autorizzati tramite opportune politiche di accesso basate sui requisiti relativi alla sicurezza e all'attività dell'azienda;
  - le informazioni non vengano divulgate a personale non autorizzato a seguito di azioni deliberate o per incuria;
  - l'integrità delle informazioni sia protetta e salvaguardata da modifiche non autorizzate;
  - le risorse di supporto alle informazioni siano protette adeguatamente.
- Assicurare la protezione dei dati personali adempiendo agli obblighi dettati dal Regolamento Generale sulla Protezione dei Dati (GDPR) e la relativa normativa italiana attraverso:
  - l'elaborazione del registro delle attività di trattamento;
  - la valutazione di impatto sulla protezione dei dati, laddove applicabile;
  - l'applicazione di misure tecniche ed organizzative adeguate intese a garantire la sicurezza dei dati e assicurarne l'accountability e il rispetto dei principi di privacy by design e by default, in modo che i dati siano:
    - trattati in modo lecito, corretto e trasparente,
    - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità,

- adeguati, pertinenti e non sovrabbondanti,
- accurati e mantenuti aggiornati,
- non conservati più a lungo del necessario,
- trattati in conformità dei diritti dell'interessato,
- sicuri,
- non trasferiti all'estero senza adeguata protezione.

- Assicurare la continuità del business aziendale affinché le informazioni siano a disposizione degli utenti autorizzati quando ne abbiano necessità tramite:
  - predisposizione di sistemi di backup delle informazioni uniformemente gestito e monitorato;
  - redazione di piani per la gestione del servizio, tra cui piani della continuità, mantenuti costantemente aggiornati e controllati;
  - redazione di piani per la continuità dell'attività aziendale, opportunamente aggiornati, controllati e migliorati, ai fini di assicurare capacità di risposta a eventi disastrosi, resilienza e continuità dei servizi.
- Minimizzare i danni derivanti da attività esterne, interne, accidentali o intenzionali mediante:
  - controlli opportuni per l'accesso alle informazioni o agli asset dell'azienda da parte di terzi;
  - mantenimento della sicurezza dell'informazione e del software scambiato all'interno dell'azienda con qualunque parte esterna;
  - procedure per le necessarie autorizzazioni a portarefuori dall'azienda informazioni critiche, apparati e/o software;
  - procedure per la sicurezza degli apparati all'esterno dell'azienda stabilendo le modalità di assegnazione degli accessi.
- Rispondere e reagire tempestivamente ad eventi che possano ridurre la sicurezza delle informazioni mediante:

- redazione di procedure per la comunicazione tempestiva e per la gestione degli incidenti in caso di minaccia alla sicurezza dell'informazione, in modo che siano immediatamente individuabili i responsabili e le azioni correttive da intraprendere;
- comunicazioni tempestive a chi di dovere relativamente a violazioni della sicurezza delle informazioni.

- Rispondere pienamente alle indicazioni della normativa vigente e cogente.
- Aumentare, nella propria organizzazione, il livello di sensibilità e la competenza sui temi di sicurezza attraverso:
  - comunicazioni aggiornate e adeguata formazione per tutto il personale, circa l'attuazione del SGSI;
  - programmi formativi di dettaglio sulla sicurezza delle informazioni per tutto il personale interno e per tutto il personale esterno che opera per periodi prolungati all'interno dell'azienda.
- Fornire opportunità di miglioramento continuo.
- Definire e mantenere sotto controllo, per quanto riguarda l'erogazione di servizi in modalità cloud:
  - le modalità di erogazione del servizio in cloud: SaaS, IaaS e PaaS;
  - la gestione degli accessi ai servizi erogati in modalità cloud, secondo la Politica degli Accessi Logici di Promotica Spa;
  - le comunicazioni ai customer in caso di change e agli interessati in caso di data breach
  - il ciclo di vita degli account, definito nelle note operative relative ai servizi erogati in modalità cloud;
  - il recepimento nell'analisi del rischio dei rischi aggiuntivi derivanti dall'erogazione di una infrastruttura cloud: l'analisi del rischio ISO/IEC 27001 viene effettuata includendo gli asset relativi ai servizi in cloud;
  - l'applicazione dei requisiti cogenti derivati dal Regolamento Europeo per la Protezione dei Dati Personal (GDPR).

Leadership e commitment

L'Alta Direzione di Promotica Spa, ponendo il SGI quale base prioritaria e strategica per il conseguimento degli obiettivi a carattere generale individuati, intende mostrare la propria leadership e il proprio impegno concreto.

Le principali azioni in tal senso sono:

COMMITMENT	MODALITÀ DI ATTUAZIONE
Assicurare che le Politiche e gli obiettivi del SGI siano stabiliti in modo adeguato	• Definizione della Politica del Sistema di Gestione Integrato • Riesame della Direzione • Azioni di mitigazione dei rischi • Mantenimento di risorse adeguate • Intervento in caso di violazione delle Politiche del Sistema di Gestione Integrato.
Assicurare un'adeguata integrazione dei processi del SGI nei processi di business dell'organizzazione	• Attività di formazione e consapevolezza • Attribuzione di adeguati ruoli, responsabilità e autorità.
Rendere disponibili adeguate risorse per il SGI.	• Azioni di mitigazione dei rischi • Piano di miglioramento del SGI
Comunicare l'importanza dell'efficacia del SGI e del conformarsi ai relativi requisiti	• Attività di formazione e consapevolezza.
Assicurare che il SGI raggiunga gli obiettivi stabiliti	• Monitoraggio, misurazione e analisi delle azioni di mitigazione dei rischi.
Dirigere e supportare il personale nel contribuire all'efficacia del SGI.	• Attività di formazione e consapevolezza.
Promuovere il miglioramento continuo.	• Attività di formazione e consapevolezza • Piano di miglioramento del SGI.
Supportare i responsabili di processo nel consolidamento della leadership nelle attività di loro pertinenza.	• Riunioni periodiche di pianificazione e comunicazione dei risultati

Assicurare che il SGI promuova e persegua la completa responsabilizzazione (accountability).	• Rispetto dei requisiti di legge, dei regolamenti, delle direttive (locali, nazionali e comunitarie) applicabili alla realtà dell'azienda, nel rispetto di tutte le parti interessate e delle esigenze dalle stesse espresse durante l'erogazione del servizio • Garanzia di efficacia ed efficienza dei processi aziendali • Disponibilità del presente documento a tutte le parti interessate, tramite adeguati canali di comunicazione al proprio interno e verso l'esterno • Monitoraggio e miglioramento costante dei propri Sistemi di Gestione, definendo obiettivi per il miglioramento e verificandone il raggiungimento e dandone opportuna comunicazione a tutto il personale • Introduzione e costante aggiornamento delle • procedure di gestione e sorveglianza per il costante controllo dell'incolumità del personale, dell'ambiente e delle prestazioni energetiche, al fine di programmare opportuni interventi nel caso si riscontrino situazioni non conformi, anomalie o emergenze • Potenziamento dell'attività di informazione e formazione di tutti gli operatori, garantendo lo sviluppo professionale degli stessi in quanto risorsa strategica, rendendoli consapevoli dei loro obblighi individuali, dell'importanza di ogni loro azione per il raggiungimento dei risultati attesi e della loro responsabilità in materia di ambiente, responsabilità sociale, salute e sicurezza sui luoghi di lavoro • Considerazione dei Clienti quali elemento fondamentale del proprio successo, lavorando per la loro soddisfazione anche riguardo alle regole di Responsabilità Sociale • Considerazione dei propri fornitori come partner, non solo per la realizzazione delle attività ma anche per quanto riguarda la Responsabilità Sociale • Identificazione di rischi, opportunità e pericoli derivanti dallo svolgimento delle attività, tramite valutazione preventiva di rischi per il personale per le attività in essere e per ogni nuova attività e/o processo, in modo da adottare soluzioni in grado di prevenire infortuni, patologie professionali, impatti sull'ambiente e sprechi energetici, e minimizzare, per quanto possibile, l'accadimento e l'estensione di tali eventi • Conduzione periodica di audit interni; analisi e monitoraggio di eventuali non conformità

Analisi dei rischi

La Direzione ha istituito ed attua un approccio basato sulla valutazione quantitativa e qualitativa dei rischi associati alle risorse esistenti in azienda, ai processi e agli obiettivi definiti nel sistema. Tale metodo consente di determinare valori oggettivi che permettono di definire le relative contromisure che devono essere adottate per abbattere e rendere accettabile il valore del rischio residuo associato al bene. In tal senso vengono adottati strumenti informatici e metodi deterministici che permettono, oltre che di implementare e gestire l'inventario degli asset aziendali, il registro dei trattamenti dei dati personali, misurare l'efficacia dell'applicazione delle azioni e soprattutto la replicabilità della valutazione, in ottica di garantire il processo di miglioramento. Inoltre, l'analisi dei rischi costituisce strumento fondamentale a supporto delle decisioni dell'organizzazione, al fine di evitare rischi e cogliere opportunità.

Le analisi dei rischi e i relativi piani di trattamento sono presentati e valutati ad ogni riesame della Direzione al fine di individuare opportunità di miglioramento e definire misure di sicurezza. Tali misure di sicurezza hanno lo scopo di "contrastare", "prevenire", "dissuadere", "rilevare", "attenuare", "ripristinare" o "correggere" le minacce che possono incombere sui sistemi informativi aziendali. Esse dovranno essere attuate secondo le modalità descritte all'interno di specifiche procedure operative e/o istruzioni operative.

Responsabilità e violazioni

Responsabilità

La presente politica è stata formulata dal Consulente in collaborazione con Responsabile del SGQ e del SGI, che, su incarico della Direzione, estende la responsabilità su tutti i sistemi di gestione.

Essa verrà riesaminata almeno annualmente ad ogni riesame della Direzione e comunque al verificarsi di cambiamenti significativi.

I responsabili dell'attuazione della presente politica sono:

- La Direzione de Promotica Spa, che stabilisce i criteri di accettazione e i livelli di accettabilità del rischio e fornisce le risorse necessarie per garantire la corretta applicazione dei processi del Sistema di Gestione Integrato, assicura lo svolgimento di audit interni e garantisce il pieno supporto nell'attuazione della presente politica, affidando alle diverse funzioni compiti di implementazione, gestione e monitoraggio dell'efficacia ed efficienza del sistema, assegna opportuni ruoli e responsabilità per la gestione per la qualità, la gestione per la sicurezza dell'informazione, la gestione del servizio e per la continuità operativa.
- Il Titolare per il Trattamento dei dati personali ha la responsabilità di qualsiasi trattamento di dati personali che effettui direttamente o che altri effettuino per suo conto. In particolare, mette in atto misure adeguate ed efficaci, così da essere in grado di dimostrare la conformità delle attività di trattamento con il GDPR, compresa l'efficacia delle misure, che tengono conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.
- Il Responsabile del SGI, che facilita l'attuazione della presente politica attraverso norme e procedure appropriate.
- Tutto il personale di Promotica Spa, a cui sono assegnati precisi ruoli e responsabilità. Esso deve avere un'adeguata competenza per svolgere i compiti richiesti. Pertanto, deve essere informato e formato adeguatamente riguardo agli obiettivi dell'azienda in tema di qualità,

sicurezza delle informazioni, protezione dei dati personali, gestione dei servizi, continuità operativa, salute e sicurezza sul lavoro, gestione ambientale. Sono definite e mantenute registrazioni sull'istruzione, formazione, abilità, esperienze e qualifiche. Tutto il personale ha la responsabilità di reagire tempestivamente agli incidenti contro la sicurezza e/o non conformità del prodotto/servizio e a segnalare alla Direzione qualsiasi punto debole individuato nel sistema.

- Clienti e Fornitori coinvolti nella gestione dei prodotti/servizi implementati, che rientrano nel perimetro di applicazione del Sistema di Gestione Integrato. Essi sono tenuti al rispetto della Politica Integrata di Promotica Spa.

Violazioni

L'Alta Direzione è coinvolta in prima persona nel rispetto e nell'attuazione di questi principi e si impegna ad assicurare che la presente politica sia compresa, condivisa, implementata e attuata da tutti i propri dipendenti e collaboratori ed allo stesso tempo si impegna a condividerla con tutti gli stakeholder.

Ritenendo di fondamentale importanza la realizzazione degli obiettivi fissati, il Sistema di Gestione Integrato è costantemente monitorato e si dà atto che ogni azione non conforme alla presente politica aziendale verrà esaminata e potrà dare origine all'adozione di provvedimenti in coerenza con le disposizioni di legge e con i previsti regimi contrattuali applicabili caso per caso.