La **Politica Aziendale** impone che, in coerenza con la mission aziendale, la gestione di tutti i processi aziendali sia impostata con le regole proprie dell'applicazione del Sistema di gestione secondo le norme **ISO/IEC 27001:2022 e UNI EN ISO 9001:2015**.

SCOPO E OBIETTIVI

La direzione di **Méthode S.r.l.** ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della Sicurezza delle Informazioni e della Qualità.
Lo scopo della presente policy è:

- garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27002 nelle loro ultime versioni.
- garantire un prodotto/servizio improntato alla massima soddisfazione dei propri clienti e, più in generale, di tutte le parti interessate.

CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'Azienda.
L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione (SGSDQ).
L'azienda consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

POLICY SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda.
È necessario assicurare:

- la confidenzialità delle informazioni: le informazioni devono essere accessibili solo da chi è autorizzato.
- l'integrità delle informazioni: proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.
- la disponibilità delle informazioni: che gli utenti autorizzati possano effettivamente accedere alle informazioni nel momento in cui ne hanno necessità.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti, nonché danni di natura economica e finanziaria.
Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.
L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo. La valutazione

del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.

I principi generali della gestione della sicurezza dei dati abbracciano vari aspetti:

- Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione dei dati e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso ai dati devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.
- Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali, dei dati e dei sistemi di gestione.
- Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
- È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza dei dati nei contratti con le terze parti.
- Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla mission aziendale.
- Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza dei dati, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

ATTENZIONE FOCALIZZATA SUL CLIENTE E SULLE PARTI INTERESSATE

L'organizzazione si impegna a comprendere le necessità dei clienti e pianifica le proprie attività per soddisfarle appieno. Allo stesso modo opera nel rispetto delle richieste e dei requisiti:

- del mercato di riferimento
- del paese in cui opera, adempiendo a leggi e regolamenti
- di tutte le parti coinvolte nei propri processi critici

Méthode S.r.l. si propone di assicurare competenza, continuità, diligenza, qualità, adeguati livelli di sicurezza e livello adeguato delle proprie prestazioni nel rispetto dell'etica professionale e nell'ottica di garantire nel tempo il miglioramento della Soddisfazione del Cliente. In particolare, la soddisfazione del cliente è perseguita attraverso momenti di verifica e di aggiornamento sui temi correlati alle prestazioni offerte. La soddisfazione del cliente viene perseguita offrendo e adeguando tutti i processi alle sue particolari esigenze implicite ed esplicite rilevate e monitorando sia gli sviluppi di acquisizione della cultura aziendale, sia il raggiungimento degli obiettivi concordati in fase contrattuale. Il cliente assume un ruolo centrale per il successo di Méthode S.r.l. Diventa, perciò, importante conoscerlo a fondo, erogare prestazioni rispondenti ai suoi bisogni e creare un'elevata customer satisfaction, in quanto fattore differenziante in un mercato fortemente competitivo.

APPROCCIO PER PROCESSI

L'organizzazione identifica le diverse attività dell'organizzazione come processi da pianificare, controllare e migliorare costantemente e attiva al meglio le risorse per la loro realizzazione.
L'organizzazione gestisce i propri processi perché siano univoci:

- gli obiettivi da perseguire e i risultati attesi
- le responsabilità connesse e le risorse impiegate.

LEADERSHIP

L'organizzazione si assume la responsabilità dell'efficacia del proprio SGSDQ, rendendo disponibili tutte le risorse necessarie e assicurandosi che gli obiettivi pianificati siano compatibili con il contesto e gli indirizzi strategici dell'organizzazione.
L'organizzazione comunica l'importanza del SGSDQ e coinvolge attivamente tutte le parti interessate, coordinandole e sostenendole.

VALUTAZIONE DEI RISCHI E DELLE OPPORTUNITÀ

L'organizzazione pianifica i propri processi con approccio risk-based thinking, al fine di attuare le azioni più idonee per:

- valutare e trattare rischi associati ai processi;
- sfruttare e rinforzare le opportunità identificate.

L'organizzazione promuove a tutti i livelli un adeguato senso di proattività nella gestione dei propri rischi.

COINVOLGIMENTO DEL PERSONALE E DEGLI STAKEHOLDER

L'organizzazione è consapevole che il coinvolgimento del personale e di tutti gli stakeholder, unito all'attiva partecipazione di tutti i collaboratori, sono un elemento strategico primario.
Promuove lo sviluppo delle professionalità interne e l'attenta selezione delle collaborazioni esterne al fine di dotarsi di risorse umane competenti e motivate.

RESPONSABILITÀ DI OSSERVANZA E ATTUAZIONE

L'osservanza e l'attuazione delle policy sono responsabilità di:

1. Tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è coinvolto nel trattamento di dati rientranti nel campo di applicazione del Sistema di Gestione. Il personale è responsabile della tempestiva segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza. Il raggiungimento di tali obiettivi è garantito attraverso un'adeguata formazione, finalizzata a consentire lo svolgimento consapevole dei compiti assegnati e al miglioramento continuo delle prestazioni, al fine di soddisfare in modo sempre più efficace le esigenze dei clienti. A tal fine, l'azienda assicura un supporto formativo e informativo continuo, nonché la definizione e l'attuazione di un Piano di Formazione e Aggiornamento strutturato, coerente e orientato alla crescita professionale del personale. Il rispetto di questi principi è altresì garantito mediante il controllo dell'osservanza, da parte dei collaboratori, degli obblighi di segreto e di riservatezza professionale, nonché degli impegni contrattuali, sia espliciti che impliciti, cui essi sono tenuti.
2. Tutti i soggetti esterni che intrattengono rapporti di collaborazione con l'azienda sono tenuti a garantire il rispetto dei requisiti previsti dalla presente politica. Il conseguimento di tale obiettivo è assicurato attraverso la verifica che i partner, i fornitori, i collaboratori e gli eventuali professionisti coinvolti possiedano adeguati requisiti di qualità, affidabilità, competenza e responsabilità, nonché idonee misure a tutela della sicurezza dei dati.
3. Tutti i soggetti esterni che intrattengono rapporti di collaborazione con l'azienda sono tenuti a rispettare i requisiti stabiliti dalla presente policy. Il raggiungimento di tale obiettivo è garantito attraverso la selezione e la verifica di collaboratori, partner e professionisti esterni in possesso di adeguati requisiti di qualità, affidabilità, competenza e responsabilità, nonché della capacità di assicurare un adeguato livello di sicurezza dei dati.
4. Il Responsabile del Sistema di Gestione che, nell'ambito del Sistema di Gestione e attraverso norme e procedure appropriate, deve:
   - condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio;
   - stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali;
   - verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi;
   - organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza dei dati;
   - verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e, in tal modo, provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

MIGLIORAMENTO CONTINUO

L'adozione di sistemi di monitoraggio interni all'azienda, permette una sorveglianza continua dell'attività aziendale, per consentire di individuare in modo preventivo possibili scostamenti dai propri obiettivi. L'obiettivo viene garantito attraverso un controllo costante in tutte le fasi di

realizzazione delle stesse e nel rispetto delle normative vigenti, migliorando l'immagine e la credibilità sul mercato.
La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'attività di **Méthode S.r.l.**, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti, nonché danni di natura economica, finanziaria e di immagine.
L'impegno della direzione si attua tramite la definizione di una struttura organizzativa adeguata a:

- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSDQ;
- controllare che il SGSDQ sia integrato in tutti i processi aziendali e che le procedure e i controlli siano sviluppati efficacemente;
- monitorare l'esposizione alle minacce per la sicurezza dei dati;
- attivare programmi per diffondere la consapevolezza e la cultura sulla sicurezza dei dati.

L'organizzazione si pone come obiettivo permanente il miglioramento delle prestazioni dei propri Sistemi di Gestione. La preliminare valutazione dei rischi e delle opportunità connessi ai processi aziendali, le attività di verifica, interna ed esterna, e il riesame della Direzione sono gli strumenti che l'organizzazione mette in atto per migliorarsi costantemente. L'obiettivo viene garantito attraverso:

- Professionalità delle prestazioni
- Trasparenza dei comportamenti
- Diligenza nello svolgimento degli incarichi professionali
- Correttezza professionale
- Riservatezza
- Disponibilità totale nei confronti del Cliente
- Senso di Responsabilità
- Spirito Costruttivo nella risoluzione dei problemi

RIESAME

L'organizzazione si pone come obiettivo permanente il miglioramento delle prestazioni del proprio SGSDQ. La preliminare valutazione dei rischi e delle opportunità connessi ai processi aziendali, le attività di verifica, interna ed esterna, e il riesame della Direzione sono gli strumenti che l'organizzazione mette in atto per migliorarsi costantemente.

La Direzione verificherà periodicamente e regolarmente, o in concomitanza di cambiamenti significativi, l'efficacia e l'efficienza del Sistema di Gestione, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.
Il Responsabile del Sistema di Gestione ha la responsabilità del riesame della politica.
Il riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica.
Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio dell'azienda alla gestione della sicurezza dei dati, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e i risultati dei precedenti riesami. Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza dei dati.

IMPEGNO DELLA DIREZIONE

La Direzione sostiene attivamente la sicurezza dei dati e della qualità aziendale attraverso un chiaro orientamento strategico, un impegno concreto, l'assegnazione esplicita di incarichi e il riconoscimento delle relative responsabilità.

Tale impegno si concretizza mediante una struttura organizzativa dedicata, con i seguenti compiti:

- Identificare gli obiettivi relativi alla sicurezza dei dati e della qualità, assicurando che siano allineati ai requisiti aziendali e normativi;
- Definire ruoli e responsabilità per lo sviluppo, il mantenimento e il miglioramento continuo del Sistema di Gestione della Sicurezza dei Dati e della Qualità (SGSDQ);
- Garantire risorse adeguate per la pianificazione, implementazione, gestione, controllo, revisione e miglioramento del SGSDQ;
- Assicurare l'integrazione del SGSDQ nei processi aziendali, sviluppando procedure e controlli efficaci;
- Approvare e promuovere iniziative volte al miglioramento della sicurezza dei dati e della qualità aziendale;
- Favorire la diffusione della cultura della sicurezza e della qualità attraverso programmi di sensibilizzazione e formazione.

La Direzione si impegna, inoltre, a garantire il rispetto delle normative di riferimento e a promuovere un approccio orientato al miglioramento continuo, affinché la sicurezza dei dati e la qualità siano elementi centrali della strategia aziendale.

San Vendemiano, 11/12/2025

RSGSDQ _____