Per Mollificio Fede la sicurezza delle informazioni ha come obiettivo primario la sicurezza delle informazioni, della struttura tecnologica, fisica, logica e organizzativa, responsabile della loro gestione. Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, nel campo di applicazione definito dal SGSI, attraverso il rispetto delle seguenti proprietà:

- Riservatezza: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- Integrità: salvaguardare la consistenza dell'informazione dalle modifiche non autorizzate;
- Disponibilità: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali quando ne fanno richiesta;
- Controllo: assicurare che la gestione dei dati avvenga sempre attraverso processi sicuri e testati;
- Autenticità: garantire una provenienza affidabile dell'informazione;
- Privacy: garantire la protezione e il controllo dei dati personali.

Nell'ambito delle attività svolte dall'Organizzazione, attraverso la propria infrastruttura tecnologica, l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione del SGSI, assicura:

- Rispetto delle normative vigenti e degli standard di sicurezza;
- Soddisfazione del cliente;
- Miglioramento continuo;
- Elevata immagine aziendale.

Per questo motivo Mollificio Fede ha sviluppato un sistema di gestione per la sicurezza delle informazioni seguendo i requisiti specificati dalla norma 27001:2022 ed alle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.
L'Organizzazione si impegna inoltre, a ridurre l'impatto sul *climate change*, attraverso politiche volte al risparmio energetico, incentivazione alla comunicazione elettronica, gestione delle infrastrutture con misure di contenimento degli sprechi e sensibilizzazione del personale.

Mollificio Fede si adopera a perseguire la sicurezza delle informazioni:

- Utilizzando buone pratiche per proteggere le risorse informative dell'organizzazione da minacce alla sicurezza di informazioni interne ed esterne, intenzionali o accidentali.
- Allineando gestione della sicurezza delle informazioni con il contesto di gestione del rischio strategico dell'organizzazione.
- Fissando obiettivi di sicurezza delle informazioni e stabilendo direttive e principi per l'azione.
- Stabilendo criteri per la valutazione dei rischi e l'accettazione dei rischi, controllando l'accesso alle risorse informative, comprese le reti, in base alle esigenze di business e di sicurezza.
- Proteggendo le informazioni e i supporti fisici in transito.
- Proteggendo le informazioni associate con le informazioni di loro proprietà residenti presso la sede dell'organizzazione.
- Garantendo la protezione dei beni dei clienti e le informazioni di loro proprietà residenti presso la sede dell'organizzazione.
- Assicurando la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni a tutto il personale e per tutta la durata del rapporto di lavoro.
- Incoraggiando la consapevolezza delle problematiche relative alla sicurezza delle informazioni a tutto il personale e per tutta la durata del rapporto di lavoro.
- Osservando la politica della scrivania pulita per documenti e supporti di memorizzazione rimovibili.
- Osservando la politica dello schermo pulito per servizi di elaborazione delle informazioni.

- Implementando adeguati controlli crittografici per la protezione delle informazioni.
- Garantendo la protezione dei beni dell'organizzazione che sono accessibili dai fornitori.
- Proibendo l'uso dei software non autorizzato e rispettando le leggi sui diritti di proprietà intellettuale.
- Proteggendo dati organizzativi e di tutela della privacy.
- Gestendo in modo tempestivo gli incidenti relativi alla sicurezza delle informazioni.
- Predisponendo un piano di continuità che permetta di affrontare efficacemente un evento imprevisto garantendo il ripristino dei servizi secondo gli accordi contrattuali in essere.
- Proibendo l'uso di software non autorizzato e rispettando le leggi sui diritti di proprietà intellettuale.
- Proteggendo dati organizzativi e di tutela della privacy.
- Gestendo in modo tempestivo gli incidenti relativi alla sicurezza delle informazioni.
- Predisponendo copie di backup delle informazioni, del software e delle immagini di sistema e testandole regolarmente.
- Predisponendo un piano di continuità che permetta di affrontare efficacemente un evento imprevisto garantendo il ripristino dei servizi secondo gli accordi contrattuali in essere.
- Mantenendo registrazioni per un periodo adeguato prima di smaltirle con cura.
- Applicando azioni disciplinari e scoraggiando l'uso improprio dei servizi di informazioni e dati da parte del personale.
- Garantendo il rispetto delle disposizioni di legge, statuti, regolamenti o obblighi contrattuali ed ogni requisito inerente la sicurezza delle informazioni, compresi i requisiti enunciati nella norma UNI CEI ISO/IEC 27001:2022, riducendo al minimo i rischi di sanzioni, perdite di dati o danni alla reputazione.
- Riesaminando il Sistema di Gestione per la Sicurezza delle Informazioni ad intervalli regolari.
- Migliorando continuamente il Sistema di Gestione per la Sicurezza delle Informazioni.
- Disciplinando l'utilizzo dell'AI (Intelligenza Artificiale) in modo etico, equo, trasparente e conforme ai regolamenti vigenti.
- Incentivando strategie di gestione del rischio, un uso responsabile, supervisione umana e robustezza per un'IA affidabile.

Taceno, il 02/03/2026

La Direzione

Paolo Dell'Oro

F.to in originale