POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Le informazioni sono risorse che, al pari di altri elementi e asset aziendali, sono strategiche ed essenziali per l'attività delle Organizzazioni e di conseguenza devono essere adeguatamente protette, in particolare in un mondo sempre più interconnesso e digitalizzato.

Marval SPA considera la Sicurezza delle Informazioni un'esigenza primaria e un preciso impegno nei confronti dei clienti e degli altri stakeholders.

Il Sistema di Gestione della Sicurezza Informazioni (ISMS) della Marval SPA copre tutti i processi aziendali, è integrato con gli altri Sistemi di Gestione ed è organizzato attraverso una robusta infrastruttura IT e una specifica configurazione documentale.
Esso è sviluppato conformemente ai requisiti della Norma UNI CEI EN ISO/IEC 27001 in vigore ed è implementato e mantenuto attivo per garantire:
1. Riservatezza – accessibilità esclusivamente ai soggetti e/o ai processi autorizzati;
2. Integrità – salvaguardia del contenuto e della forma dell'informazione da modifiche non autorizzate o da deterioramento/distruzione;
3. Disponibilità – facilità di accesso alle informazioni necessarie;
4. Controllo - garanzia che i processi e gli strumenti per la gestione dei dati siano sicuri e testati ai fini dell'adeguatezza;
5. Autenticità - provenienza affidabile dell'informazione;
6. Privacy – garanzia di protezione dei dati personali.

I domini di sicurezza volti a garantire la salvaguardia delle informazioni in tutte le attività, si appoggiano a specifici ed adeguati controlli organizzativi/logici, controlli relativi alle risorse umane, controlli fisici e controlli tecnologici.

L'insieme dei dati e informazioni della Marval SPA, patrimonio da salvaguardare, è localizzato nella sede centrale di Castellamonte, in tutti gli stabilimenti produttivi dell'azienda e presso i Data Center ove sono gestiti i dati aziendali.

Il Management ha definito ruoli e responsabilità per lo sviluppo e il mantenimento del ISMS ed è impegnato a:

- valutare periodicamente l'esposizione ai rischi e alle minacce per la sicurezza delle informazioni, provvedendo ad attuare idonee azioni di prevenzione e mitigazione dei rischi;
- garantire la disponibilità e allocazione di opportune risorse economiche, umane e tecnologiche necessarie per la gestione e protezione degli asset aziendali ai fini di un'efficace sicurezza delle informazioni;
- garantire che i requisiti del ISMS e i controlli previsti siano attuati efficacemente;

- garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi attuando, ove necessario, le opportune azioni correttive;
- diffondere la cultura, consapevolezza e sensibilizzazione alla sicurezza dei dati e delle informazioni tra i propri dipendenti, collaboratori, fornitori e terze parti coinvolte affinché in tutte le attività lavorative, anche quotidiane, si pongano le necessarie attenzioni e le misure personali più efficaci;
- monitorare l'infrastruttura IT, in collaborazione con il gestore di servizi IT;
- garantire la continuità operativa, anche in caso di disastri, in collaborazione con il gestore di servizi IT;
- mantenersi aggiornato rispetto all'evolversi delle tecnologie, dei tools, delle minacce;
- garantire la conformità ai requisiti di legge applicabili (in primis il GDPR in materia di privacy);
- riesaminare periodicamente gli obiettivi e la Politica per la Sicurezza delle Informazioni per accertarne continua adeguatezza e attuabilità, individuando azioni di miglioramento continuo.

Castellamonte, 28/04/25

La Direzione

V. Nunziata