Allegato D1.2-2

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

(UNI CEI EN ISO/IEC 27001:2024)

Ver.1	05/09/2024	1° Rilascio	MG	Management Team	CEO	Pubblico
REVISIONE	DATA	MODIFICA	REDATTO	VERIFICATO	APPROVATO	DISTRIBUZIONE

Camillo Ghelfi, CEO 40Factory

40Factory srl
Via San Giacomo 17B, 27029 Vigevano (PV)
P.IVA 02708730185

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

Il Sistema di Gestione Integrato dell'Azienda

Nel proprio processo di crescita, revisione e di miglioramento continuo la 40-FACTORY ha deciso di istituire un Sistema Integrato di Gestione (SIG) per la qualità e la sicurezza delle informazioni, che copra interamente le attività caratteristiche dell'Azienda.

Il SIG comprende tutte le fasi del ciclo di vita dei prodotti applicativi software MAT e Wilson e relativi servizi: progettazione, produzione, commercializzazione, installazione e supporto ed erogazione di servizi informatici quali ad esempio la distribuzione in modalità SaaS (Software as a Service) degli applicativi.

Il SIG di cui si è dotata 40FACTORY è il risultato della adozione integrata dei due sistemi di gestione della Qualità (SGQ) e della Sicurezza delle Informazioni (SGSI), conformi rispettivamente alle norme:

- UNI EN ISO 9001:2015 - Sistemi di gestione per la qualità – Requisiti.
- UNI CEI EN ISO/IEC 27001:2024 - Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni – Requisiti *(che richiama la norma ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements).*

La Direzione è convinta che l'adozione, nell'attuazione di un SGI, dei concetti ei principi che stanno alla base di tali norme porta all'Azienda importanti I benefici:

- migliorare "la capacità di fornire con regolarità prodotti e servizi che soddisfino i requisiti del cliente e quelli cogenti applicabili" (1) e delle parti interessate rilevanti, in un sistema economico produttivo sempre più competitivo,
- "affrontare rischi e opportunità associati al suo contesto e ai suoi obiettivi" (1) caratterizzato da rapidi cambiamenti e da evoluzioni e innovazioni
- migliorare la capacità di preservare "la riservatezza, l'integrità e la disponibilità dalle informazioni mediante l'applicazione di un processo di gestione del rischio" (2) per far fronte alle sfide emergenti della sicurezza informatica in un contesto di crescente interconnessione tecnologica, data driven;
- garantire "la conformità ai requisiti specificati del sistema di gestione per la qualità" (1) e ai requisiti legali e normativi applicabili alla gestione delle informazioni;
- costruire una solida base per realizzare all'interno dei propri obiettivi di business, delle strategie di sviluppo sostenibile e resiliente.

Per raggiungere questi obiettivi del SGI, di qualità e di sicurezza delle informazioni, in modo efficiente ed efficace e perseguendo un continuo miglioramento del sistema stesso, le attività del SGI sono state definite e strutturate all'interno di un insieme di processi correlati, gestiti utilizzando il ciclo "Plan-Do-Check-Act" (PDCA) con una pianificazione basata su un'analisi del contesto (fattori interni, esterni ed esigenze degli stakeholder) e applicando un approccio sistematico di tipo preventivo basato sull'analisi del rischio" che minimizza le azioni correttive e il verificarsi di problematiche.

La Sicurezza delle Informazioni

Poiché l'obiettivo generale dell'Azienda è garantire la gestione corretta, in tutti i processi, di tutte le informazioni generate o trattate, di proprietà interna ed esterna, l'organizzazione con il suo SGI è impegnata a promuovere, con tutte le funzioni e i livelli Aziendali pertinenti, i principi generali della gestione della sicurezza delle informazioni, che abbracciano i seguenti aspetti, considerati i più significativi:

1. Deve essere manutenuto un **catalogo costantemente aggiornato degli asset Aziendali** con le loro caratteristiche e responsabilità e **una classificazione delle informazioni stesse** con il loro livello di criticità, in modo da essere gestite con livelli di riservatezza, disponibilità ed integrità coerenti ed appropriati.

2. **Ogni accesso ai sistemi deve essere sottoposto a un'appropriata procedura d'identificazione e autenticazione (**periodicamente sottoposte a revisione), che consente un accesso alle sole informazioni e funzioni pertinenti, differenziato in base al ruolo e alla mansione.

3. Devono essere definite **delle procedure per l'utilizzo sicuro dei beni Aziendali, in particolare quelli informatici, e delle informazioni** e dei loro sistemi di gestione.

4. Con specifiche attività, deve essere **promossa e 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.

5. Per poter gestire in modo tempestivo gli incidenti, tutti devono **notificare qualsiasi problema relativo alla sicurezza delle informazioni.** Ogni incidente deve essere gestito come indicato nelle procedure.

6. È **necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali Aziendali dove sono gestite le informazion**i e deve essere garantita **la sicurezza delle apparecchiature che le gestiscono.**

7. I processi implementati devono **garantire la *riservatezza, integrità, disponibilità* delle informazioni di impatto critico**. Inoltre, deve essere **implementata la caratteristica di *non ripudiabilità del dato***, (ottenuta mediante la gestione di firme elettroniche o digitali che deve essere documentata dove richiesto da norme e standard specifici.

8. Deve essere assicurata **la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni, nei contratti con le terze parti.**

9. Deve essere predisposto un **piano di continuità (*business continuity*) c**he consenta all'Azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che minimizzano le conseguenze negative sulla sicurezza delle informazioni agli attori del suo contesto (clienti collaboratori fornitori, istituzioni, ecc.) e sulla missione Aziendale.

10. **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.**

11. **Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla sicurezza delle informazioni**, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

In questo impegno e promozione, l'Azienda ha una specifica attenzione alle nuove modalità organizzative ed operative adottate: outsourcing dei servizi SaaS, adozione strutturale interna dello smart working, implementazione di un ecosistema integrato di prodotti e servizi che coinvolge clienti e fornitori.

La Direzione della 40-Factory ritiene strategici gli investimenti nella gestione della sicurezza delle informazioni (ove richiesto dal contesto applicativo, in quanto aspetti fondamentali per assicurare, oltre alla sostenibilità del business e la conformità legale, il mantenimento di una reputazione di impresa affidabile, verso tutti gli stakeholder.

La Direzione è inoltre consapevole che la corretta gestione della sicurezza delle informazioni riguarda tutti gli aspetti della vita societaria e richiede la partecipazione attiva di tutti gli attori coinvolti, ed è quindi attivamente impegnata a perseguire il coinvolgimento competente e responsabile di tutti i collaboratori dell'Azienda e, per quanto possibile, dei Soggetti Terzi interessati.

Protezione dei dati personali

Riguardo alla politica per la protezione dei dati personali, l'Azienda fornisce ai propri dipendenti, collaboratori, fornitori o consulenti, istruzioni organizzative e tecniche che consentano l'osservanza degli obblighi di legge relativi alla protezione dei dati personali. Per questi obblighi delinea il quadro di sicurezza adottato per il sistema informativo, e definisce tutte le misure per garantire l'affidabilità delle componenti hardware e software ai fini della tutela dei dati personali trattati. Inoltre, provvede a informare gli utenti di prodotti e servizi delle misure messe in atto per proteggere e conservare i dati personali attraverso le apposite informative.