Allegato D1.2-2
POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

(UNI CEI EN ISO/IEC 27001:2024 - UNI CEI EN ISO/IEC 27017:2021)

Ver.2	28/03/2025	Revisione per estensione a ISO/IEC27017 e conformità ISO/IEC27002: 2022/5.1	MG, MT	MT	CEO	Pubblico
REVISIONE	DATA	MODIFICA	REDATTO	VERIFICATO	APPROVATO	RISERVATEZZA

Camillo Ghelfi, CEO 40Factory

1. Scopo del documento

Il presente documento, approvato dalla Direzione, definisce le linee guida generali in base alle quali è stato definito l'intero Sistema di Gestione della Sicurezza delle Informazioni (SGSI) della società 40FACTORY, implementato in modo integrato con il Sistema di Gestione per la Qualità (SGQ). Ogni piano e procedura inerente al trattamento della sicurezza delle informazioni e degli asset che le gestiscono o che possa avere impatto con tale sicurezza deve uniformarsi alla politica delineata nel presente documento.

2. Il Sistema di Gestione Integrato dell'Azienda

40FACTORY è una PMI innovativa che opera in diversi settori industriali come fornitore di soluzioni tecnologiche pronte all'uso altamente configurabili e scalabili, basate sulle moderne tecnologie dell'*Industrial Internet of Things (IIoT)* e dell'*Artificial Intelligence (AI)*. L'Azienda ha un'offerta consolidata *di prodotto - consulenza strategica* che consente ai costruttori di macchine di adottare nuovi modelli di business e agli utilizzatori finali di accrescere la cultura digitale interna e di implementare produzioni più efficienti e sostenibili, mediante lo sfruttamento intelligente ed evoluto del "valore" che sono i dati delle macchine e dell'azienda.

Nel proprio processo di crescita, revisione e di miglioramento continuo l'Azienda 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 l'Azienda è il risultato della adozione integrata e certificata dei due sistemi di gestione della Qualità (SGQ) e della Sicurezza delle Informazioni (SGSI), conformi rispettivamente alle norme: ISO 9001:2015 e ISO/IEC 27001:2022 con estensione ISO/IEC 27017:2021 (recepite a livello europeo come norme EN e a livello nazionale italiano come norme UNI/CEI).

La Direzione è convinta che l'adozione, nell'attuazione di un SGI, dei concetti e i 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

[1] ISO 9001:2015
[2] ISO/IEC 27001:2022

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.

3. La Sicurezza delle Informazioni

3.1 L'importanza della Sicurezza delle Informazioni per l'Azienda

Il Patrimonio Informativo Aziendale - che include dati propri, dei clienti e dei fornitori - rappresenta la risorsa principale su cui si basano i processi di business dell'Azienda (dalla relazione con il mercato, allo sviluppo e gestione con qualità dei suoi prodotti e servizi, allo sviluppo del processo di innovazione continua, alla gestione di tutte le strutture interne, ai prodotti e servizi utilizzati dai clienti) e deve essere adeguatamente garantita la sua sicurezza con un costante bilanciamento tra due fattori: da una parte il livello di rischio accettato e la necessità di assicurare l'efficienza, l'efficacia e la continuità dei processi e dall'altra il grado di protezione da applicare con un complesso set di misure e controlli, non esclusivamente di natura tecnologica ma anche gestionale e di responsabilità personale.

Questa protezione oggi è sempre più necessaria, considerando i profondi e rapidi mutamenti degli scenari di rischio per la sicurezza informatica, dovuti alla crescente digitalizzazione e condivisione delle informazioni, attraverso le infrastrutture ITC e di cloud computing, che riguarda tutti gli stakeholder oltre che la propria struttura organizzativa e alla crescita delle minacce alla cybersecurity e alla privacy.

Data la natura delle proprie attività, la Direzione dell'Azienda considera la sicurezza del patrimonio Informativo gestito dall'azienda, nel rispetto di obblighi contrattuali e delle nuove leggi e regolamenti, un fattore irrinunciabile per la protezione del suo business, che oggi richiede di fornire garanzie non solo sulla qualità e innovazione dei prodotti e servizi erogati ma anche sul corretto trattamento delle informazioni.

La Direzione dell'Azienda ritiene quindi strategici gli investimenti nella gestione della sicurezza delle informazioni là dove richiesti 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.

3.2 Perché un Sistema di Gestione della Sicurezza delle Informazioni secondo gli standard

Per raggiungere questo obiettivo, l'approccio adottato è l'implementazione e manutenzione in azienda di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) integrato con il Sistema Qualità, che sia certificato da un ente internazionalmente qualificato e che si fonda su standard riconosciuti e metodologie consolidate. La scelta è ricaduta sull'ente di certificazione e consulenza Det Norske Veritas (DNV) e sull'impianto normativo ISO 27000, riconosciuto a livello internazionale.

In modo specifico, per le caratteristiche e il business dell'azienda, si sono individuate le seguenti norme e linee guida:

- La Norma "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements", oggetto della certificazione integrata con la ISO 9001:2015, che definisce i requisiti per impostare e gestire il SGSI e che include tutte le tre dimensioni della sicurezza delle informazioni: logica, fisica ed organizzativa.
- Le Linea guida "ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls" che costituiscono la raccolta delle "best practices" relative ai 114 controlli da adottare in funzione dei rischi sulla sicurezza delle informazioni, per soddisfare al meglio i requisiti della norma ISO/IEC 27001:2022.

- Le Linee guida "ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services" che consentono di estendere l'applicabilità della certificazione della sicurezza delle informazioni ISO/IEC 27001:2022, in modo specifico alle attività di gestione dei servizi cloud, sia come cliente che fornitore di servizi, in modo pienamente integrato nel SGSI aziendale.
- Le linee guida "ISO 31000:2018 Risk management - Guidelines" generali per il *risk management*, che fornisce un approccio comune alla gestione del rischio, personalizzabile in base all'organizzazione e contesto, che l'Azienda ha applicato alla gestione dei rischi per la sicurezza delle informazioni, basato sull'identificazione di asset, minacce e vulnerabilità (approccio *asset-base risk assesment*).

Nel SGSI aziendale, la sicurezza delle informazioni si ottiene, partendo da questa Politica generale e sulla base di un'analisi strutturata dei rischi del contesto dell'Azienda, mediante la selezione per applicabilità e implementazione del complesso set di controlli indicati dalle norme e linee guida, attraverso un insieme strutturato ed efficiente di *Politiche, Responsabilità, Processi, Procedure, Strutture organizzative, Funzionalità hardware e software*, *Report e Registrazioni per il monitoraggio,* che sono specifiche per argomento e aree di sicurezza, come definito nel Manuale del Sistema di Gestione Integrato (MSGI) e dei suoi allegati [3].

Nella definizione del SGSI l'azienda pone particolare attenzione a due temi considerati "*focal-point*" della sua certificazione normativa dalla sicurezza delle informazioni aziendali:

- tutto il ciclo di vita dei propri prodotti e servizi (progettazione, sviluppo, rilascio, manutenzione) che sono un bene primario dell'azienda;
- lo sviluppo e gestione dei propri servizi che utilizzano le tecnologie di cloud computing SaaS che operano sui dati e le informazioni critiche delle applicazioni dei clienti.

Inoltre, viene posta una specifica attenzione alle nuove modalità organizzative ed operative: l'adozione strutturale interna dello smart working e l'implementazione di un ecosistema integrato che coinvolge l'azienda, i clienti e i fornitori, basato sui servizi in cloud.

3.3 Definizione di Sicurezza delle Informazioni

L'obiettivo primario del SGSI è garantire la sicurezza delle informazioni che significa garantire i requisiti di base "CIA+A" per le informazioni classificate come critiche:

- Riservatezza (Confidentiality): le informazioni devono essere accessibili solo alle persone autorizzate;
- Integrità (Integrity): le informazioni devono deve essere modificabili solo ed esclusivamente da chi ne possiede il diritto per prevenire modifiche indebite o fraudolente con anche controlli che consentano di rilevare o prevenire le modifiche accidentali;
- Disponibilità (Availability): le informazioni devono essere accessibili e utilizzabili quando richiesto dai processi e dagli utenti che dispongono dei relativi privilegi, in tempi congruenti con le proprie esigenze operative.
- Autenticità (Authenticity): le informazioni devono essere autentiche e non alterate, false o contraffatte.

A cui si aggiunge in specifici contesti la Non ripudiabilità: le azioni sui dati degli utenti e dei processi devono essere tracciate in un modo non ripudiabile.

[3] Manuale del Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni- 40FACTORY

3.4 Obiettivi della Sicurezza delle Informazioni

Con la presente politica della sicurezza delle informazioni, in conformità con quanto già attuato nell'ambito del sistema di gestione della qualità, la Direzione definisce i seguenti obiettivi aziendali:

- Proteggere al meglio il patrimonio informativo proprio e dei propri clienti;
- Rispondere pienamente alle indicazioni delle normative vigenti;
- migliorare la trasparenza dei propri servizi anche nell'utilizzo delle nuove tecnologie cloud, per facilitare la definizione e gestione di solidi e sicuri contratti, nel rispetto degli obblighi giuridici applicabili.
- Ottimizzare i processi di gestione del ciclo di vita dei propri prodotti e servizi.
- Preservare al meglio l'immagine dell'azienda quale partner tecnologico affidabile e competente, anche nell'ambito della sicurezza delle informazioni;
- Incrementare l'integrazione digitale sicura con gli stakeholder
- Aumentare la resilenza dell'azienda alle minacce di cybersecurity del contesto
- Aumentare il livello di sensibilità, competenza e responsabilità su temi di sicurezza, del proprio personale.

3.5 Principi fondamentali della sicurezza delle informazioni

Poiché l'obiettivo generale dell'Azienda è garantire in tutti i processi la corretta gestione di tutte le informazioni generate o trattate, sia di proprietà interna che esterna, l'organizzazione ha impegnato tutte le funzioni e i livelli aziendali, a partire dal top management, nell'implementazione, nel suo *Sistema di Gestione della Sicurezza delle Informazioni* certificato, delle misure e i controlli degli standard ISO 27000 relative ai principi fondamentali della sicurezza delle informazioni:

1. FORMAZIONE E CONSAPEVOLEZZA - Tutti i dipendenti, a partire dal momento della selezione e per tutta la durata del rapporto di lavoro, e le terze parti interessate devono essere periodicamente istruiti e resi consapevoli del valore e delle minacce alla sicurezza delle informazioni e formati, con specifici formazioni e training sulla base di ruoli e responsabilità, sulla politica e le procedure specifiche di sicurezza delle informazioni stabilite dall'organizzazione.
2. GESTIONE DEL PERSONALE - Devono essere definite procedure, in conformità con le leggi, i regolamenti e comportamenti etici, per lo screening di tutti i dipendenti e il personale di terze parti che accedono regolarmente ai locali dell'organizzazione, in modo proporzionato ai rischi di sicurezza delle informazioni gestite. Inoltre, tutti i dipendenti e il personale di terze parti devono firmare accordi di non divulgazione prima di avere qualsiasi interazione con le informazioni dell'organizzazione e il loro contratti devono richiedere il rispetto delle politiche dell'organizzazione.
3. GESTIONE DEI FORNITORI - Tutti i fornitori, ed eventuali loro subappaltatori, con cui vengono scambiate informazioni critiche dell'Azienda devono essere contrattualmente vincolati ad essere a conoscenza e rispettare le politiche di sicurezza delle informazioni aziendali applicabili, consentendo l'esecuzione di verifiche. Deve essere costantemente monitorato, mediante l'uso di procedure formali, il rispetto delle clausole di sicurezza aziendali e dei livelli di servizio di sicurezza alle informazioni.
4. CONTATTI ESTERNI E COMUNICAZIONI - L'organizzazione deve sviluppare, in modo sistematico, un'attività di sorveglianza con sufficienti contatti, sia con le autorità competenti al fine di reagire rapidamente ed efficacemente alle minacce diffuse in modo coordinato a livello nazionale e sia con gruppi specialistici di interesse, forum o associazioni, al fine di ottenere informazioni sulle correnti minacce alla sicurezza delle informazioni e le best practice da adottare per evitarle o combatterle.
5. REQUISITI LEGALI E CONTRATTUALI – Tutti i requisiti applicabili in materia di sicurezza delle informazioni derivanti da normative nazionali, internazionali o settoriali applicabili devono essere

tenuti sotto costante controllo così come quelli derivanti da contratti con terze parti, con particolare attenzione alla protezione dei dati personali e confidenziali e a quelli relativi ai servizi in cloud utilizzati o forniti.

6. TUTELA DELLA PROPRIETA' INTELLETTUALE – Devono essere definite e attuate procedure adeguate a garantire il rispetto dei requisiti legislativi, normativi e contrattuali sull'uso di materiale coperto da diritti di proprietà intellettuale e sull'uso di prodotti software proprietari.
7. SICUREZZA FISICA E AMBIENTALE - È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali dell'organizzazione e ai suoi sistemi dove sono gestite le informazioni, mediante punti di accesso ridotti al minimo e dotati di barriere fisiche protette con sistemi di controllo accessi. Inoltre, tali locali e sistemi devono essere dotati di protezioni fisiche contro i danni causati da cause naturali o da qualsiasi altro tipo di calamità naturale o provocata dall'uomo (come il fuoco, l'umidità e i terremoti).
8. GESTIONE DEGLI ASSET - Deve essere istituito e mantenuto un inventario centralizzato, costantemente aggiornato degli asset Aziendali, con le loro caratteristiche, informazioni gestite, tracciabilità in tutto il loro ciclo di vita, procedure operative di utilizzo sicuro, con le proprietà e le responsabilità chiaramente identificate, documentate, accettate e attuate (gestione di tutti i beni assegnati ai dipendenti o a terzi).
9. CLASSIFICAZIONE ETICHETTATURA E TRATTAMENTO DELLE INFORMAZIONI - Le informazioni devono essere classificate, etichettate e trattate nella loro riservatezza, disponibilità ed integrità, in base al loro valore per l'organizzazione e la legislazione vigente (e quindi la loro criticità), da tutti i proprietari delle informazioni dell'organizzazione.
10. SICUREZZA DELLE RETI - Le reti ICT, incluse le reti virtuali cloud, devono essere implementate e verificate (se necessario con sistemi di Vulnerability Assessment e Penetration test) in modo da limitare la possibilità di intercettazioni o alterazioni del traffico, anche limitando le comunicazioni autorizzate al necessario e bloccando tutte le altre non autorizzate. I servizi, gli utenti e i sistemi informatici dovrebbero essere opportunamente segmentati e segregati all'interno le diverse aree di rete con requisiti di sicurezza omogenei, per definire compartimenti stagni con diversi livelli di sicurezza capaci di isolare e confinare le eventuali minacce, utilizzando firewall e sistemi hardware e software specifici.
11. CLOUD COMPUTING – L'organizzazione, in qualità di cliente di servizi cloud e cloud provider definisce che: gli applicativi rilasciati possono essere forniti in ambiente cloud, le informazioni memorizzate nell'ambiente di cloud computing possono essere soggette ad accesso e gestione da parte del fornitore di servizi cloud; i processi possono essere eseguiti su un servizio cloud multi-tenant e virtualizzato; gli amministratori del servizio cloud del cliente del servizio cloud possono avere accesso privilegiato; sono definite le aree geografiche delle risorse cloud. Inoltre l'organizzazione definisce i requisiti di sicurezza delle informazioni di base applicabili alla progettazione e all'implementazione del servizio cloud, i rischi da parte di addetti ai lavori autorizzati, l'accesso alle risorse dei clienti del servizio cloud da parte del personale del fornitore di servizi cloud, le procedure di controllo degli accessi come l'autenticazione forte per l'accesso amministrativo ai servizi cloud, i requisiti di sicurezza della virtualizzazione, le modalità di accesso e protezione dei dati dei clienti del servizio cloud; la gestione del ciclo di vita degli account dei clienti dei servizi cloud.
12. SICUREZZA DEGLI ASSET - Tutti gli asset, inclusi si asset virtuali in cloud, che portano dati o di supporto a servizi informativi devono essere ubicati in modo da essere protetti da minacce accidentali e ambientali e sempre collegati con adeguate utenze di supporto sia all'interno che all'esterno dei locali dell'organizzazione. Tutte le apparecchiature devono essere mantenute nel contesto del piano di sicurezza delle informazioni dell'organizzazione. L'accesso ai sistemi di informazione per la manutenzione deve essere definito e controllato. Le apparecchiature non

presidiate devono essere sempre lasciate con un'adeguata protezione sia contro l'accesso fisico non autorizzato e il furto sia contro l'accesso informatico: tutte le sessioni devono essere bloccate quando si lascia qualsiasi apparecchiatura o in grado di disconnettersi automaticamente dopo un periodo di inattività definito e configurato. Nessun supporto di memoria deve essere lasciato incustodito in un luogo di lavoro.

13. CONTROLLO DEGLI ACCESSI E GESTIONE DEL CICLO DI VITA - Ogni accesso ai sistemi e alle reti dell'organizzazione deve essere sottoposto a un'appropriata procedura di identificazione, autorizzazione e autenticazione, periodicamente sottoposte a revisione, che consente un accesso alle sole informazioni e funzioni pertinenti, differenziato in base al ruolo e alla mansione (principio del minimo privilegio). Gli utenti dei sistemi e dei servizi devono essere identificati in modo univoco attraverso una procedura formale di registrazione e cancellazione per la concessione e la revoca dei privilegi di accesso, verificati periodicamente. Le credenziali per autenticarsi e i sistemi che le verificano devono essere sufficientemente robusti da ridurre al minimo l'accesso di personale non autorizzato (mediante la gestione di firme elettroniche con autenticazione a due fattori o firme digitali dove richieste da norme e standard specifici). Vengono inclusi i controlli necessari alla definizione degli accessi del personale addetto alla gestione dell'infrastruttura cloud ed il ciclo di vita per il rilascio, modifica, cancellazione degli accessi.
14. GESTIONE SUPPORTI DI MEMORIA - Devono essere definite e implementate restrizioni specifiche per la gestione di tutti i supporti rimovibili e portatili. Inoltre, i supporti dei sistemi informatici contenenti informazioni devono essere protetti contro l'accesso non autorizzato, l'uso improprio o la distruzione in caso di trasferimento al di fuori dei locali dell'organizzazione. Devono essere definite procedure rigorose per la riassegnazione o lo smaltimento sicuro dei supporti, al fine di rendere irrecuperabili i dati precedentemente memorizzati.
15. PROTEZIONE CONTRO I MALWARE - Adeguati sistemi hardware e software di cybersecurity, per la protezione dai malware devono essere installati e mantenuti costantemente aggiornati su tutte le risorse informatiche che possono essere infettate.
16. TRASFERIMENTO DELLE INFORMAZIONI - Nel trasferimento e gestione delle informazioni, devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e dei requisiti e principi inerenti alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione. Le informazioni trasferite tramite la messaggistica elettronica e piattaforme informatiche devono essere selezionate e configurate per garantire la riservatezza e rilevare gli attacchi su questi canali. Deve essere ridotte al minimo con controlli di sicurezza il trasferimento di informazioni con supporti rimovibili.
17. CRITTOGRAFIA – Se necessario devono essere sviluppati, documentati, implementati, mantenuti e rivisti dei controlli crittografici con algoritmi "robusti" per garantire la riservatezza delle informazioni critiche sia nelle trasmissioni che a riposo. Le chiavi crittografiche devono essere utilizzate, protette e conservate secondo procedure rigorose e documentate durante l'intero ciclo di vita. Tale fondamento si applica ai servizi offerti dall'organizzazione e ai fornitori dell'organizzazione stessa.
18. CONFIGURAZIONE E GESTIONE SICURA DEGLI ASSET INFORMATICI E DEGLI END POINT - Devono essere definite delle procedure per l'utilizzo sicuro degli asset informatici, tra i quali i dispositivi di end point, con definite procedure di configurazione.
19. DISPOSITIVI MOBILI E LAVORO A DISTANZA - I dispositivi mobili utilizzati per scopi lavorativi devono essere configurati in modo sicuro e rigorosamente controllati. Gli strumenti di lavoro a distanza devono essere sviluppati con protezioni di sicurezza aggiuntiva per evitare fughe di informazioni e

usi impropri e malware. Gli accessi remoti utilizzati a tal fine devono essere rafforzati contro l'accesso non autorizzato.

20. BACKUP, RIDONDANZA, BUSINESS CONTINUITY - Devono essere definite e implementate procedure per un'adeguata creazione e test di copie di backup dei software e delle informazioni. Le strutture di elaborazione delle informazioni devono essere progettate ed implementate in modo di garantire una ridondanza sufficiente a soddisfare i requisiti di disponibilità anche in situazioni di guasto. Deve essere predisposto un piano di continuità (*business continuity*) che consenta all'Azienda di affrontare efficacemente un evento imprevisto, garantendo, mediante i sistemi di backup e di ridondanza, il ripristino dei servizi critici in tempi e con modalità che minimizzano le conseguenze negative sulla sicurezza delle informazioni e sui processi, obiettivi e interessi all'azienda e agli stakeholder (clienti collaboratori fornitori, istituzioni, ecc.).
21. GESTIONE DEGLI INCIDENTI - Devono essere definiti ed applicate procedure per il controllo, registrazione, e la pronta gestione e comunicazione, degli incidenti alla sicurezza delle informazioni e della loro *escalation*, in base a specifiche responsabilità approvate e stabilite dalla direzione e con interazioni con le autorità nazionali incaricate e indicate dalle normative, qualora necessario. Le modalità di affronto e se necessario le procedure, devono essere adattate in base alla conoscenza acquisita dall'analisi e dalla soluzione degli incidenti (*incident lesson learned*) e dall'analisi di eventuali punti deboli della sicurezza segnalati dagli utenti, osservati o sospettati. L'organizzazione ha definito un processo di comunicazione delle violazioni e linee guida alla condivisione delle informazioni per aiutare le indagini e le indagini forensi verso enti esterni, tale processo è conforme alle norme vigenti e agli standard applicati dall'organizzazione.
22. MONITORAGGIO E REGISTRAZIONE DEGLI EVENTI - Gli eventi maggiormente rilevanti per la sicurezza delle informazioni devono essere monitorati ed archiviati in modo sicuro, protetti da modifiche e devono essere soggetti a regolare revisione. Tutte le attività degli amministratori di sistema e degli operatori devono essere registrate così come i loro accessi/disconnessioni riuscite e tentate.
23. SVILUPPO SICURO - Gli aspetti di sicurezza devono essere inclusi by-design in tutte le fasi del ciclo di vita dei sistemi e dei servizi informatici: progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione. Tutti i progetti dell'organizzazione dovrebbero includere considerazioni sulla sicurezza delle informazioni. Sicurezza dei servizi applicativi - I sistemi informativi utilizzati per sviluppare prodotti e fornire servizi devono essere protetti dagli attacchi attraverso configurazioni sicure e rinforzate con controlli di sicurezza aggiuntivi e costantemente monitorate e protette mediante dispositivi di sicurezza dedicati, in proporzione alla loro esposizione al rischio. Protezione del ciclo di vita dello sviluppo di applicazioni e servizi informatici - Le organizzazioni devono integrare i criteri per la sicurezza delle informazioni nel ciclo di vita dello sviluppo delle loro applicazioni, al fine di ridurre al minimo le vulnerabilità della loro sicurezza. Tra questi criteri vanno considerati: la separazione degli ambienti di sviluppo e di test; i criteri di sicurezza da implementare nei test di sviluppo e di accettazione per i nuovi sistemi informatici, i loro aggiornamenti e manutenzioni; l'applicazione delle patch alle vulnerabilità del software messe a disposizione dai fornitori.
24. SEGREGAZIONE DELLE INFORMAZIONI DEI CLIENTI NEGLI AMBIENTI CLOUD – L'organizzazione ha processi che garantiscono e monitorano la segregazione dei dati dei clienti negli ambienti cloud, requisito fondamentale per i servizi offerti dall'azienda.
25. CHANGE MANAGEMENT - Tutte le modifiche all'organizzazione, ai processi o ai sistemi aziendali e informativi che influiscono sulla sicurezza delle informazioni devono essere registrate, debitamente approvate e testate. Le modifiche al sistema e al software devono essere consentite solo al personale autorizzato. Vengono gestiti i processi di informazione e comunicazione verso i clienti per le attività di aggiornamento e modifiche delle soluzioni cloud.

26. AUDIT E ASSESSMENT - I sistemi di sicurezza delle informazioni devono essere riesaminati periodicamente da revisori indipendenti. I manager devono garantire che tutte le procedure di sicurezza all'interno della loro area di responsabilità siano eseguite correttamente per ottenere la conformità alle politiche e agli standard di sicurezza. I sistemi informatici dovrebbero essere riesaminati periodicamente per garantire la conformità continua agli standard di implementazione della sicurezza.

3.6 Assegnazione delle responsabilità

La Direzione è inoltre consapevole che la corretta gestione della sicurezza delle informazioni riguarda tutti gli aspetti della vita dell'Azienda 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 coinvolti nella gestione delle informazioni.

Per il conseguimento di tale obiettivo di coinvolgimento responsabile, la Direzione si impegna a far sì che la presente politica sia distribuita, compresa e accettata e attuata, attraverso l'impianto di politiche e procedure particolari definito dal SGSI, da tutto il personale, interno ed esterno, che a qualsiasi titolo collabora con l'azienda e in qualsiasi modo coinvolto con le informazioni che rientrano nel campo di applicazione del SGSI: *personale interno, stagisti, collaboratori esterni, consulenti, fornitori sotto contratto*.

In particolare, tutto il personale è tenuto a:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e delle risorse intellettuali dell'Azienda o affidate all'Azienda da terze parti, anche con la sottoscrizione formale di *un patto di riservatezza*;
- proteggere ogni informazione, attività, beni materiali, i sistemi informatici e risorsa dell'Azienda sotto la propria responsabilità o affidati all'Azienda da terze parti;
- confermare in modo formale di aver ricevuto, compreso ed accettato la presente politica, ove applicabile:
- segnalare al Supervisore della Sicurezza delle Informazioni o al Management Team, le anomalie, i punti deboli e le violazioni della sicurezza effettive o presunte di cui si viene a conoscenza, anche non formalmente codificate, per poter prevenire e gestire in modo tempestivo eventuali incidenti.
- segnalare al Supervisore della Sicurezza delle Informazioni o al Management Team qualsiasi modifica che si ritiene necessaria dei requisiti di sicurezza, degli standard, della politica e delle politiche e procedure specifiche.

Specifiche responsabilità sono attribuite come definito dal MSGI[4], dal mansionario[5] e organigramma[6] e dal regolamento[7] ai diversi ruoli: Direzione (CEO), Management Team (MT), Supervisore della Sicurezza delle Informazioni (SSI), il Personale.

Nell'ottica del coinvolgimento responsabile viene promossa l'assegnazione dello sviluppo, revisione e l'approvazione delle politiche/procedure relative ad argomenti specifici della sicurezza delle informazioni, ai collaboratori, in modo pertinente al ruolo, livello di autorità e competenza tecnica, pur mantenendo la Direzione il ruolo di approvatore finale.

[4] Manuale del Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni- 40FACTORY
[5] D1.2-5 – Mansionario aziendale
[6] D1.2-4 - Organigramma nominativo
[7] S4.2-6 - Regolamento e policy per la sicurezza informatica

La violazione dei principi e dei comportamenti a tutela della sicurezza delle informazioni saranno perseguite dall'Azienda, in misura proporzionata alla gravità delle infrazioni commesse ed in linea con quanto stabilito nel regolamento aziendale[8].

3.7 Riesame della politica e delle politiche specifiche per argomento

Le attività periodiche di riesame del SGSI - audit interni, riesame della Direzione e sorveglianza annuale da parte dell'ente accreditato per il mantenimento della certificazione - consentono il controllo del sistema, la sua revisione e il suo miglioramento continuo, in risposta a modifiche significative del contesto dell'Azienda: la strategia aziendale; fattori interni all'organizzazione;, norme nazionali e internazionali, regolamenti, statuti e contratti; rischi per la sicurezza delle informazioni dovuti a fattori interni ed esterni; lezioni apprese da eventi e incidenti di sicurezza delle informazioni.

4. Conformità Direttiva (UE) n. 2022/2555NIS2

A seguito dell'attività di notifica da parte dell'Azienda, la stessa è stata riconosciuta dall'autorità di riferimento europeo per l'Italia ACN come soggetto "*non in ambito NIS2*". Nonostante ciò, l'Organizzazione ha definito gli obiettivi aziendali per soddisfare i requisiti del regolamento NIS2 per il supporto dei propri clienti che ricadono nell'ambito NIS2 come soggetti importanti o essenziali.

5. Conformità protezione dei dati personali: Regolamento (UE) 2016/679 GDPR e ISO/IEC 27001:2022

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.

[8] D1.2-7 - Regolamento e policy aziendale