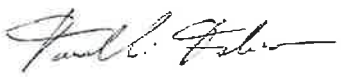
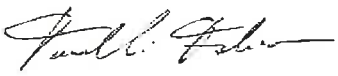
C4

asm vigevano lomellina s.p.a.

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

SISTEMA DI GESTIONE INTEGRATO

Codice documento	**SGSI01**
Versione	**1.5 del 09/10/2025**
Livello di confidenzialità	**PUBBLICO**

	Preparato	*Controllato*	*Approvato*
	Resp. Funzione Fabio Tonelli	**RGQ** Francesca Graziotin	**RDSGI** Fabio Tonelli
Firma			
Data	09/10/2025	09/10/2025	09/10/2025

Approvato con det. n. 86 del 10.12.2025

Registro delle modifiche

Data	Versione	Prodotta da	Descrizione delle modifiche
18/03/2020	1.0	Tonelli Fabio	Versione iniziale del documento
25/10/2021	1.1	Tonelli Fabio	Verifica e conferma del documento
30/11/2022	1.2	Tonelli Fabio	Verifica e conferma del documento
04/10/2023	1.3	Tonelli Fabio	Verifica e aggiornamento dei riferimenti normativi
29/08/2024	1.4	Tonelli Fabio	Verifica e aggiornamento normativo
09/10/2025	1.5	Reale Antonio	Integrazione Requisiti NIS 2

Sommario

Premessa e scopo del documento

La presente politica definisce il Sistema di Gestione per la Sicurezza delle Informazioni (di seguito, "SGSI"), di **ASM VIGEVANO** (di seguito, "Azienda") secondo i requisiti della norma ISO/IEC 27001 integrati con quanto previsto dalle Linee Guida ISO/IEC 27017 e ISO/IEC 27018 e dal D.Lgs 138/24 NIS 2 allo scopo di garantire la sicurezza e la protezione delle informazioni, patrimonio dell'organizzazione.

Si intende per Sistema di Gestione della Sicurezza delle Informazioni l'insieme delle politiche, procedure, documenti, registri, piani, linee guida, accordi, contratti, processi, pratiche, metodi, attività, ruoli, responsabilità, relazioni, strumenti , tecniche, tecnologie , risorse, e strutture che l'Azienda utilizza per proteggere e conservare le informazioni, per gestire e controllare i rischi di sicurezza delle informazioni e per raggiungere gli obiettivi aziendali di adeguatezza e conformità (security compliance).

I principi a cui si ispira la Politica riguardano la riservatezza, l'integrità e la disponibilità delle informazioni oggetto di trattamento e di comunicazione all'interno e all'esterno, e nel rispetto delle leggi nazionali ed europee vigenti con particolare attenzione alle disposizioni in merito al trattamento dei dati personali.

La sicurezza delle informazioni in azienda rappresenta un elemento di particolare rilievo soprattutto per quanto riguarda l'elaborazione di dati e informazioni che supera, oggi, oltre il 70% del trattamento unicamente su supporti e sistemi informatizzati, e per questo si rende necessario un controllo delle comunicazioni e trasmissioni sui diversi canali (web, internet, cloud) e sui diversi utilizzatori, interni ed esterni, per garantire protezione e sicurezza.

A ciò si aggiunge che il pericolo di "fuga di informazioni", compromissione o indisponibilità, incidentale o volontaria, che genera conseguenze negative sia per il business dell'azienda sia per la sua reputazione e immagine, con conseguenti gravi ripercussioni sulla sua stessa sopravvivenza.

A ciò si aggiungono anche le forti ricadute su un mancato adempimento a leggi e normative, alle quali corrispondono precise sanzioni penali e amministrative di notevole entità.

Scopo, quindi, della presente Politica è quello di fornire un'utile guida e visione di come l'azienda, coinvolgendo tutti gli attori che con essa partecipano, integri persone e processi in un Sistema di gestione e ne assicuri lo sviluppo e il mantenimento.

Riferimenti normativi

I principali riferimenti normativi che coinvolgono la sicurezza delle informazioni e la sua applicazione in contesti di tipo aziendale sono:

- √ ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection - Information security management systems - Requirements ";
- √ UNI CEI EN ISO/IEC 27002:2023 "Sicurezza delle informazioni, cybersecurity e protezione della privacy – Controlli di sicurezza delle informazioni";
- √ ISO/IEC 27017:2015 Information technology – Security techniques – Code of pratice for information security controls based on ISO/IEC 27002 for cloud services
- √ ISO/IEC 27018:2019 Information technology – Security techniques – Code of pratice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- √ Regolamento UE 679/2016 per la Protezione dei Dati Personali;
- √ D.lgs 196/2003 - Codice in materia di protezione dei dati personali;
- √ D. lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali
- √ D.lgs 81/2008 – Sicurezza Lavoro.
- √ D.lgs 138/24 – NIS2 e conseguenti determinazione ACN

Contesto dell'organizzazione

La partenza verso la Certificazione ISO/IEC 27001 è avvenuta a seguito di un'analisi del contesto in cui l'Azienda opera, degli attori coinvolti, delle opportunità e dei possibili rischi sul mancato adeguamento ad uno standard che permettesse di garantire la sicurezza delle informazioni.

Nel corso di svolgimento delle proprie attività organizzative e di business, l'Azienda vede interagire molti attori, definiti parti interessate, portatrici di interessi specifici (dipendenti, collaboratori, fornitori) e, per questo, in vario modo fonti anche di rischi sia a livello operativo che strategico (comunicazioni, accordi, accessi).

A cominciare da queste parti interessate, nonché dai fattori interni (competenze, processi, produttività) e esterni (mercati, competitors, innovazioni tecnologiche), il contesto in cui si inserisce la sicurezza è diventato un elemento di criticità e di assoluta importanza per affrontare i necessari cambiamenti.

Nel corso del 2024 l'azienda è diventata un soggetto importante NIS 2 e di conseguenza sono adottate e documentate politiche di sicurezza informatica per almeno i seguenti ambiti:

a) gestione del rischio;

b) ruoli e responsabilità;

c) affidabilità delle risorse umane;

d) conformità e audit di sicurezza;

e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;

f) gestione degli asset;

g) gestione delle vulnerabilità;

h) continuità operativa, ripristino in caso di disastro e gestione delle crisi;

i) gestione dell'autenticazione, delle identità digitali e del controllo accessi;

j) sicurezza fisica;

k) formazione del personale e consapevolezza;

l) sicurezza dei dati;

m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;

n) protezione delle reti e delle comunicazioni;

o) monitoraggio degli eventi di sicurezza;

p) risposta agli incidenti e ripristino.

Le Informazioni Aziendali

Le informazioni aziendali a cui fa riferimento la presente Politica, nell'ottica dello sviluppo di un Sistema di gestione SGSI, riguardano tutte le informazioni raccolte, conservate e trasmesse su qualsiasi supporto, cartaceo ed elettronico, per garantire l'operatività dell'azienda.

Ai fini del trattamento a cui possono essere sottoposte le informazioni aziendali, la garanzia della loro sicurezza tiene in considerazione le seguenti caratteristiche:

- √ il **Valore**, ossia l'importanza dell'asset informativo a livello di business e di strategia dell'organizzazione (ad esempio un brevetto o un piano di sviluppo):
- √ la **Cogenza,** in termini di proprietà valoriale insita nell'informazione stessa, da un punto di vista normativo e di conformità (ad esempio un regolamento, una policy);
- √ la **Criticità,** in termini di Riservatezza, Integrità e Disponibilità per cui la vulnerabilità ad attacchi e minacce ne comprometterebbero la sicurezza.

Leadership ed impegno

La Direzione è responsabile della definizione e revisione continua degli obiettivi del SGSI in relazione alle strategie di adeguatezza e sviluppo.

Essa garantisce anche il coinvolgimento di tutte le parti interessate comunicando prima di tutto la presente Politica del SGSI attraverso i canali interi tradizionali, quindi lo stato di applicazione del Sistema di Gestione, l'importanza del miglioramento continuo, l'impegno a sostenere e guidare tutti i processi a sostegno di tutti coloro che partecipano, direttamente e indirettamente, alla vita dell'azienda.

Tra l'altro, la Leadership si impegna a:

- garantire il rispetto delle normative vigenti e i requisiti della norma;
- rendere disponibili le risorse, umane e tecniche, necessarie al perseguimento degli obiettivi della sicurezza delle informazioni;
- comunicare regole, procedure, policy e altra documentazione per la gestione del SGSI;
- sviluppare e garantire la consapevolezza e la conoscenza alle persone, interne ed esterne, che interagiscono con la sicurezza;
- fissare obiettivi sempre aggiornati e condivisi, e riesaminare annualmente l'intero Sistema.

Gli obiettivi del SGSI

L'Azienda ha individuato gli obiettivi per la Sicurezza delle informazioni che sono qui sinteticamente elencati (si rimanda al Piano degli Obiettivi per un maggiore dettaglio):

- √ sviluppare competenze in ciascuna figura professionale in tema di Sicurezza delle informazioni;
- √ attivare a proposito un Piano della Formazione che intervenga con corsi ad hoc sulla tematica;
- √ sviluppare un Piano della Comunicazione in cui siano inseriti eventi e campagne di sensibilizzazione;
- √ assegnare le necessarie risorse per tutti gli aspetti della sicurezza, fisica, logica e organizzativa;

- √ sviluppare la documentazione di supporto e integrarla con documenti già presenti e di valido utilizzo per la gestione del SGSI;
- √ individuare le figure professionali già impegnate per la sicurezza e ridefinirne i profili secondo competenze e responsabilità proprie dei ruoli stabiliti per la Sicurezza delle informazioni;
- √ migliorare l'attuale gestione di incidenti o eventi dannosi attraverso lo sviluppo di un processo di gestione e controllo adeguati;
- √ gestire l'intero Sistema di gestione SGSI da un punto di vista del rischio e tutte le sue articolazioni (pianificazione, valutazione, gestione contromisure, rischio accettato).

Ruoli e responsabilità

La Leadership, o Alta Direzione, assegna ruoli e responsabilità a figure professionali ben definite e li comunica al personale e ai collaboratori attraverso i canali tradizionali interni all'azienda.

Sono inoltre stati definiti i ruoli e le responsabilità previste dalla NIS 2

La sicurezza degli asset informativi (gestione degli asset)

Le Informazioni, o asset informativi, sono un patrimonio fondamentale per l'organizzazione, e la loro sicurezza e protezione è irrinunciabile.

Gli Asset Informativi si dividono in due categorie di appartenenza:

1. Asset Primari
   - Riguardano dati, processi e attività di business, informazioni aziendali, che riguardano tutti i dati, quelli di mercato e vendita, del personale, di procedure, aspetti amministrativi, ecc.
2. Asset di Supporto
   - Sistemi IT (ci sono anche le reti, le infrastrutture, i dispositivi)
   - Software
   - Personale
   - Network
   - Sedi e Aree Riservate
   - Struttura organizzativa

La Sicurezza delle informazioni garantita dal Sistema di gestione SGSI avviene nel rispetto dei tre requisiti base citati in premessa, cioè la Riservatezza, l'Integrità e la Disponibilità delle informazioni (R.I.D.):

- √ **Riservatezza**: si tratta di non divulgare informazioni ai non autorizzati, individui, entità o processi, quindi ci deve essere un processo di autorizzazioni che indichi chi può e chi non può accedere alle informazioni;
- √ **Integrità**: riguarda la conservazione e protezione da danni o modifiche delle informazioni, quindi alla loro salvaguardia e alla completezza delle informazioni;
- √ **Disponibilità**: le informazioni sono rese disponibili solo a entità autorizzate, si ritorna alla definizione di processi di autorizzazione per cui un'informazione può essere Pubblica o Riservata.

L'obiettivo è quello di identificare gli asset dell'organizzazione e definire adeguate responsabilità per la loro protezione.

Inoltre, è stato preso in considerazione anche il loro ciclo di vita naturale, a partire dalla implementazione, protezione, gestione, manutenzione, per poi passare alla dismissione Ciò implica che il Sistema di gestione SGSI viene impostato per orientare più efficacemente il valore e i rischi in ciascuna delle fasi di gestione dell'Asset

Le procedure per la gestione prevedono per tutti gli Asset informativi la classificazione e l'etichettatura su cui è prevista la predisposizione di un'apposita politica (Information Security Policy) che ne definisce requisiti e criteri. Il Sistema SGSI, infatti, prevede un processo di classificazione ed etichettatura delle informazioni che rispecchi funzionalità e uso nelle varie occasioni di fruizione, in funzione delle attività e dell'utenza che ne effettua elaborazione e trattamento.

La Direzione è responsabile dell'approvazione delle responsabilità affidate alle figure di ruolo individuate per la gestione degli Asset informativi, oltretutto classificati per gruppi in modo da agevolare il monitoraggio e il controllo come richiesto dalla ISO/IEC 27001.

Sicurezza fisica dei sistemi informatici

A protezione degli asset sono definite apposite procedure che limitano l'accesso fisico agli asset al personale autorizzato

Sicurezza dei dati degli accessi logici

L'accesso logico ai dati dei sistemi informatico è protetto adottando sistema di accesso nominativi, policy di complessità ed in base alla valutazione del rischio sistemi di autenticazioni avanzanti quali MFA

Sono adotti molteplici livelli di protezione quali (firewall, vpn, mail relay, ecc) al fine di proteggere gli asset e le comunicazioni

Gestione delle vulnerabilità

I sistemi informativi sono aggiornanti periodicamente, inoltre vengono effettuati vulnerability assesment e penetration test periodici per verificare il livello di vulnerabilità del sistema.

Quanto rilevato dai VA e da PT viene usato per predisporre un piano di remedation al fine di ridurre il rischio.

Continuità operativa

Sono predisposte, verificare annualmente e aggiornare procedure di business continuity, disaster recover ed incident management

Azioni per la gestione di rischi e opportunità

Secondo la metodologia adottata dall'Azienda, dopo aver definito un elenco dei rischi ed effettuato una valutazione del loro impatto sulla gestione degli Asset informativi, la correlazione tra questi ultimi e i rischi avviene considerando le vulnerabilità con impatto sulla Riservatezza, Integrità e Disponibilità.

Questa metodologia permette di condurre una valutazione del rischio partendo dalle specifiche vulnerabilità insite nell'Asset informativo, dalle minacce rilevate e loro frequenza, e dalle probabilità di manifestarsi.

Questo conduce il Sistema SGSI ad effettuare un vero e proprio trattamento del rischio decidendo le quattro strategie su cui viene anche formulato un apposito Piano di Trattamento del Rischio. Questo l'elenco delle strategie che sono messe in atto:

1. **Evitare i rischi** – modificare o non intraprendere attività per fare in modo che non si presentino;
2. **Controllare/Mitigare i rischi** – ridurre la probabilità o l'impatto, o entrambi, con contromisure appropriate;
3. **Accettare il rischio** – decidere di non intervenire sugli effetti del rischio in quanto troppo costoso;
4. **Trasferire il rischio** – esternalizzare il rischio a terze parti. Non previsto per i rischi rientranti nella NIS 2

Dalla gestione del rischio e il suo trattamento secondo la logica dei controlli forniti dalla ISO/IEC 27002, e da effettuare per tutti i gruppi di Asset informativi, deriva un altro importante documento adottato dal Sistema di gestione SGSI: la Dichiarazione di Applicabilità, o SOA (Statement of Applicability). Esso stabilisce il perimetro

di attuazione del Sistema SGSI attraverso la scelta dei controlli con cui intervenire nei vari processi per garantire la sicurezza delle informazioni.

Gestione del rischio della catena di approvvigionamento

L'azienda effettua un'analisi sulla criticità delle forniture in base ai seguenti parametri:

- livello degli standard di sicurezza adottato dal fornitore
- criticità del servizio/attività erogata dal fornitore
- privilegi di accesso assegnati al fornitore

Gestione del personale

Sono state previste ed implementate procedure per la gestione del personale nelle fasi di ingresso, gestione e uscita.

Tali procedure prevedono:

in ingresso

la valutazione del personale in fase di ingresso al punto d vista delle competenze, dell'affidabilità e della riservatezza

in gestione

la formazione del personale e la verifica delle competenze per il ruolo e gli accessi forniti

in uscita

la chiusura degli accessi e la riservatezza dei dati

Monitoraggio e risposta agli eventi di sicurezza

E' stato predisposto un sistema di monitoraggio degli eventi si sicurezza XDR

L'azienda inoltre ha predisposto un piano di gestione degli eventi si sicurezza per il loro contenimento ed ove previsto eventuale comunicazione alle autorità, al garante ed al CSIRT.

Comunicazione

L'Azienda considera la comunicazione come uno strumento strategico per la diffusione e la conoscenza della sicurezza delle informazioni per tutte le finalità che detto sistema si pone, ossia la messa in opera di operatività a garanzia del suo funzionamento e l'assicurazione del raggiungimento dei suoi obiettivi.

Questo documento della Politica del Sistema di gestione SGSI mette in luce la funzione chiave del processo di Comunicazione: esso da un lato permette lo sviluppo della consapevolezza e delle responsabilità, dall'altro scandisce accordi e doveri che sono imprescindibili per una corretta conduzione e funzionamento del sistema stesso.

La comunicazione si muove su tre assi:

- √ **Comunicazione interna:** tutto il personale e i collaboratori sono raggiunti da informazioni aggiornate e da strumenti per lo sviluppo della consapevolezza e conoscenza delle regole e procedure con cui trattare le informazioni classificate secondo uno schema abilitante e utilizzando strumenti propri dell'organizzazione (posta elettronica, intranet, riunioni, ecc.);
- √ **Comunicazione con i Fornitori e Clienti:** accordi contrattuali e autorizzazioni discendono sistematicamente nelle relazioni con fornitori e clienti affinché le disposizioni del Sistema siano estese anche a loro e al rapporto di business che li vincola;
- √ **Comunicazione con il pubblico:** promozioni e campagne di marketing avvengono nell'ottica della divulgazione di una cultura della sicurezza che accresce la credibilità dell'azienda e ne rinforza immagine e reputazione, veicolando l'interesse per il suo business e aumentandone la competitività.

Informazioni documentate

Le informazioni documentate sono il supporto alle attività svolte per la gestione del Sistema SGSI.

La progettualità e pianificazione del Sistema SGSI prevede una fondamentale gestione di Informazioni documentate anche perché costituiscono un riferimento per lo svolgimento di tutti i processi, e l'evidenza della messa in opera del Sistema.

Ogni documento deve essere valutato e autorizzato, revisionato ed approvato dalla Direzione sulla base della sua funzione strategica (Piano, politica, progetto, obiettivo), o da un Responsabile in caso di documentazione operativa all'interno di un processo.

La gestione delle Informazioni documentate ingloba anche documenti di supporto alla gestione, come registrazioni, report di misurazione e monitoraggio, analisi dei risultati, grafici, ecc.

È utile che le Informazioni documentate siano codificate, quindi archiviate, aggiornate, distribuite e accessibili a riprova di quanto svolto ed eseguito in conformità al Sistema di gestione SGSI.

Controllo delle informazioni

La sicurezza delle informazioni si ottiene impostando un insieme di controlli costituiti da politiche, processi, procedure, regolamenti e sistemi IT affidati alla tecnologia informatizzata.

I controlli sono stabiliti, attuati, monitorati, riesaminati e migliorati per assicurare il raggiungimento degli obiettivi di sicurezza e si abbinano alle informazioni a seconda del loro livello di classificazione e grado di rischio.

Valutazioni delle prestazioni

Il Sistema di gestione SGSI prevede un continuo monitoraggio e misurazione delle prestazioni dei processi inerenti alla sicurezza delle informazioni al fine di misurare l'efficacia e l'adeguatezza del Sistema stesso, intervenire su non conformità ed errori, identificare opportunità per il miglioramento e trarre così vantaggio dalle correzioni.

Per questo il Sistema di gestione SGSI prevede un riesame con cui valutare la continua idoneità, adeguatezza ed efficacia dell'approccio dell'azienda alla gestione della sicurezza delle informazioni.

La responsabilità del riesame è sempre della Direzione che ne effettua l'esecuzione e la valutazione dei risultati.

I Riesami sono previsti con cadenza pianificata, solitamente ad ogni modifica o variazione, e comunque con cadenza almeno annuale in corrispondenza della revisione globale di tutto il Sistema e le sue parti.

Monitoraggio, misurazione e valutazione del SGSI

Il Sistema di gestione SGSI è oggetto di monitoraggio con cadenza almeno annuale con cui la Direzione verifica le politiche, le procedure organizzative e le registrazioni opportunatamente aggiornate dai relativi responsabili.

Il processo con cui si effettua il monitoraggio e la valutazione del Sistema è l'Audit interno. È uno strumento con cui misurare il livello di sicurezza del sistema, ma è anche un'indagine strutturata e metodica poiché ispeziona ogni elemento oggetto di rischio con l'ausilio dei controlli specifici disposti dalla norma. È, in termini più ampi, un processo di verifica sistematico e documentato, che si avvale di verifiche anche sul campo e di registrazioni da cui detrarre evidenze oggettive per determinare il grado di conformità alle politiche, alle procedure o alla norma stessa.

L'Audit interno mira a:

- √ individuare eventuali vulnerabilità che rendono il Sistema inefficiente;
- √ verificare e assicurare le conformità a politiche, norme o leggi;
- √ rivedere e migliorare il sistema e i processi;
- √ verificare il reale raggiungimento degli obiettivi della sicurezza.

L'Audit viene condotto da personale interno qualificato e competente (Internal Auditor), in grado di rilevare le criticità e i punti di forza del Sistema di gestione per poi esporle in un report che funga da guida per la Direzione nel formulare nuove strategie e nuovi traguardi per la sicurezza delle informazioni.

Il risultato di un Audit, infatti, può portare alla scoperta di non conformità, come criticità o vulnerabilità di un servizio o di un processo, quindi dover intervenire con opportune azioni correttive.

Sono inoltre effettuate periodicamente verifiche di conformità ed audit di sicurezza quali VA e o PT

Miglioramento

Il miglioramento è uno dei più importanti processi per la sicurezza delle informazioni in quanto è mirato ad accrescere la capacità del Sistema SGSI di soddisfare i requisiti della norma.

Esso procede «a valle» e «a monte» delle attività del Sistema di gestione SGSI, ossia agisce sui risultati ottenuti alla fine del periodo o percorso predefinito della gestione e quindi, dopo aver effettuato correzioni, rivede, riesamina e ripropone nuovi obiettivi e strategie per migliorare tali risultati.

Il miglioramento si attua attraverso strategie, tecniche e strumenti quali:

- √ impegno della Direzione;
- √ formazione a tutti i livelli;
- √ partecipazione dei membri dell'organizzazione in attività di gruppo dedicate al tema della sicurezza delle informazioni;
- √ sviluppo del processo di miglioramento mediante metodologie, tecniche e strumenti opportuni.

Gli obiettivi del miglioramento per la gestione della sicurezza delle informazioni sono:

- √ soddisfare i requisiti del cliente e accrescerne la soddisfazione;
- √ garantire il miglioramento dei requisiti, attuali e futuri, della sicurezza delle informazioni;
- √ correggere, prevenire o ridurre gli effetti indesiderati dei rischi connessi alle informazioni;

- √ adoperarsi per il miglioramento dei risultati di prestazioni (risorse e strumenti) e dell'efficacia dei processi del Sistema di gestione SGSI.

Miglioramento Continuo

L'Azienda ha tra i suoi obiettivi principali anche il miglioramento continuo del proprio Sistema di Gestione di Sicurezza delle Informazioni.

Mentre il miglioramento interviene sulle non conformità e sulla loro correzione per riportare il Sistema di gestione SGSI nella giusta direzione, e quindi sui risultati, il miglioramento continuo si prefigge degli obiettivi di lungo termine che incidono sulle prestazioni più che sui risultati, ed è un'attività ricorrente che non si ferma mai, anche quando il Sistema di gestione SGSI non mostra grandi criticità.

Tali obiettivi riguardano:

- √ idoneità;
- √ adeguatezza;
- √ efficacia del SGSI.