



Politica della Sicurezza delle Informazioni

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

Rev. 0

Emissione 18/09/2026

Codice DSGI02

Politica della Sicurezza delle Informazioni

1	SCOPO E IMPEGNO DELLA DIREZIONE	pag. 4
2	CONTESTO E CAMPO DI APPLICAZIONE	pag. 4
3	PRINCIPI E OBIETTIVI	pag. 4
4	GOVERNANCE E RESPONSABILITÀ	pag. 5
5	IMPEGNI PER LA SICUREZZA DELLE INFORMAZIONI	pag. 5
5.1	Gestione dei rischi e degli asset	pag. 5
5.2	Persone e cultura della sicurezza	pag. 6
5.3	Controllo degli accessi e identità	pag. 6
5.4	Sicurezza fisica, ambientale e operativa	pag. 6
5.5	Crittografia e protezione delle comunicazioni	pag. 6
5.6	Acquisizione, sviluppo, manutenzione e vulnerabilità	pag. 6
5.7	Fornitori e catena di approvvigionamento	pag. 7
5.8	Incidenti, continuità e gestione delle crisi	pag. 7
5.9	Protezione dei dati personali	pag. 7
6	GESTIONE E NOTIFICA DEGLI INCIDENTI	pag. 7
7	CONFORMITÀ, VERIFICA E MIGLIORAMENTO	pag. 8

1. SCOPO E IMPEGNO DELLA DIREZIONE

RAFFMETAL S.P.A. considera la sicurezza delle informazioni un requisito essenziale per la continuità dei processi industriali, l'affidabilità verso clienti e partner, la protezione del patrimonio informativo e il conseguimento degli obiettivi aziendali.

La Direzione istituisce, mantiene e migliora continuamente un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) basato sul rischio e si impegna a:

- assicurare riservatezza, integrità, disponibilità e autenticità delle informazioni;
- soddisfare i requisiti legali, regolamentari, contrattuali e di settore applicabili (automotive);
- approvare gli indirizzi di sicurezza e obiettivi misurabili, mettendo a disposizione risorse, competenze e responsabilità adeguate;
- prevenire e ridurre l'impatto degli incidenti sulle attività, sui clienti, sui partner e sulle persone;
- valutare regolarmente efficacia, adeguatezza e proporzionalità delle misure adottate e promuovere il miglioramento continuo del SGSI.

2. CONTESTO E CAMPO DI APPLICAZIONE

RAFFMETAL S.P.A. opera nella produzione di leghe di alluminio da riciclo e serve, tra gli altri, il settore automotive. La gestione della sicurezza tiene quindi conto della natura industriale e multi-sito dell'organizzazione, dell'interconnessione fra tecnologie dell'informazione e tecnologie operative, della continuità produttiva, degli scambi informativi nella catena di fornitura e delle aspettative di clienti e altre parti interessate.

La presente Politica si applica a tutte le persone che operano per o per conto di RAFFMETAL S.P.A. e a processi, informazioni, asset e sedi inclusi nel campo di applicazione del SGSI formalmente approvato.

3. PRINCIPI E OBIETTIVI

Il SGSI persegue i seguenti principi e costituisce il quadro per definire e riesaminare gli obiettivi di sicurezza delle informazioni:

1. **Approccio basato sul rischio:** identificare, analizzare, valutare e trattare tempestivamente i rischi, assegnando priorità e responsabilità.

2. **Sicurezza proporzionata:** adottare misure tecniche, operative e organizzative adeguate al rischio, alla criticità dei processi e ai costi di attuazione.
3. **Information Security by Default:** integrare requisiti di sicurezza nella progettazione, nell'acquisizione, nello sviluppo, nella modifica e nella manutenzione di processi, impianti, prodotti e sistemi.
4. **Minimo privilegio e principio di necessità:** limitare gli accessi a quanto necessario per ruolo, attività e periodo, con autorizzazioni tracciabili e riesaminate periodicamente.
5. **Resilienza:** preparare la risposta a incidenti e crisi;
6. **Responsabilità condivisa:** richiedere a personale e terze parti comportamenti coerenti, segnalazioni tempestive e rispetto delle regole applicabili.
7. **Miglioramento continuo:** misurare efficacia ed efficienza, implementare azioni correttive e adattare il SGSI a minacce, tecnologie e requisiti in evoluzione.

4. GOVERNANCE E RESPONSABILITÀ

L'alta Direzione:

- approva la presente Politica, gli obiettivi e le modalità di attuazione delle misure di gestione del rischio;
- sovrintende alla loro implementazione; assicura risorse adeguate; riceve informazioni periodiche sullo stato del SGSI e informazioni tempestive sugli incidenti rilevanti. Gli organi di amministrazione e direttivi esercitano le responsabilità previste dai requisiti applicabili e partecipano a una formazione adeguata in materia di sicurezza informatica.

Il comitato di Sicurezza coordina l'attuazione della Politica, la gestione dei rischi, il programma di miglioramento, il monitoraggio e il reporting alla Direzione.

I responsabili di processo, asset e rischio classificano e proteggono le informazioni e gli asset affidati, collaborano alla valutazione dei rischi e assicurano l'attuazione delle azioni concordate. Tutto il personale e le terze parti coinvolte devono conoscere e rispettare le regole, proteggere credenziali e informazioni e segnalare senza ritardo eventi, vulnerabilità, anomalie, perdite o sospetti incidenti attraverso i canali definiti.

5. IMPEGNI PER LA SICUREZZA DELLE INFORMAZIONI

5.1 Gestione dei rischi e degli asset

- Mantenere inventari aggiornati di informazioni, applicazioni, infrastrutture, dispositivi e componenti IT e OT rilevanti, con proprietari e livelli di criticità definiti.
- Classificare ed etichettare le informazioni e stabilire regole coerenti per creazione, accesso, uso, trasferimento, conservazione, restituzione e distruzione sicura.
- Riesaminare i rischi periodicamente e in occasione di cambiamenti significativi, incidenti, nuove minacce, variazioni normative, organizzative, tecnologiche o di sito.

5.2 Persone e cultura della sicurezza

- Verificare, nei limiti di legge, identità e idoneità per i ruoli sensibili e definire obblighi di riservatezza e sicurezza prima, durante e dopo il rapporto di lavoro o incarico.
- Fornire formazione e sensibilizzazione iniziale, periodica e basata sul ruolo;
- Documentare la partecipazione e verificare l'efficacia della formazione.

5.3 Controllo degli accessi e identità

- Gestire l'intero ciclo di vita delle identità e dei diritti di accesso, con approvazione, minimo privilegio, segregazione dei compiti, riesami periodici e revoca tempestiva.
- Applicare autenticazione robusta e, ove opportuno o richiesto dal rischio, autenticazione a più fattori; proteggere gli accessi privilegiati, remoti e ai sistemi industriali.
- Registrare e monitorare le attività rilevanti nel rispetto della legge e proteggere i log da alterazioni e accessi non autorizzati.

5.4 Sicurezza fisica, ambientale e operativa

- Proteggere siti, aree, impianti, sale tecniche, supporti e apparecchiature mediante perimetri, autorizzazioni, controlli degli accessi e misure ambientali proporzionate.
- Definire configurazioni sicure, gestione delle modifiche, protezione da software malevolo, aggiornamenti, monitoraggio, capacità e manutenzione per sistemi IT e OT.
- Segregare le reti e gli ambienti secondo il rischio.

5.5 Crittografia e protezione delle comunicazioni

- Definire criteri per l'uso della crittografia e della cifratura, la gestione delle chiavi e la protezione dei dati in transito e a riposo in funzione di classificazione, rischio e requisiti contrattuali.

- Utilizzare canali autorizzati e protetti per lo scambio di informazioni con clienti, fornitori e partner, applicando accordi di riservatezza quando richiesto.

5.6 Acquisizione, sviluppo, manutenzione e vulnerabilità

- Integrare requisiti di sicurezza nelle specifiche, nella selezione dei fornitori, nello sviluppo, nei collaudi, nell'accettazione e nelle modifiche di sistemi e servizi.
- Individuare, valutare, prioritizzare e trattare le vulnerabilità in tempi coerenti con il rischio; governare le eccezioni e predisporre misure compensative.
- Applicare procedure di change management formalizzate, con valutazione dell'impatto, autorizzazione, test, verifica successiva e possibilità di ripristino.

5.7 Fornitori e catena di approvvigionamento

- Valutare il rischio dei fornitori e dei servizi esterni prima dell'affidamento e durante il rapporto, considerando criticità, vulnerabilità e dipendenze.
- Inserire nei contratti requisiti proporzionati relativi agli aspetti di information security rilevanti.
- Monitorare prestazioni e conformità dei fornitori critici e gestire tempestivamente scostamenti e cambiamenti rilevanti.

5.8 Incidenti, continuità e gestione delle crisi

- Mantenere processi per rilevare, segnalare, classificare, contenere, analizzare, risolvere e documentare eventi e incidenti, preservando le evidenze e apprendendo dalle cause.
- Definire ruoli, escalation, reperibilità e comunicazioni interne ed esterne, coordinando sicurezza delle informazioni, continuità operativa, gestione delle crisi, obblighi normativi e contrattuali.
- Predisporre e testare backup e piani di continuità operativa.

5.9 Protezione dei dati personali

- Integrare nel SGSI i requisiti applicabili in materia di protezione dei dati personali, coordinando la gestione dei rischi di sicurezza con i principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza e limitazione della conservazione.
- Adottare misure tecniche e organizzative adeguate al rischio per i diritti e le libertà delle persone e applicare protezione dei dati fin dalla progettazione e per impostazione predefinita nei nuovi trattamenti e nei cambiamenti rilevanti.

- Coordinare la gestione delle violazioni di dati personali con la risposta agli incidenti, assicurando valutazione, escalation, documentazione e notifiche o comunicazioni nei termini applicabili.

6. GESTIONE E NOTIFICA DEGLI INCIDENTI

RAFFMETAL S.P.A. mantiene un processo di gestione degli incidenti che consente di effettuare senza ingiustificato ritardo le segnalazioni e le notifiche alle autorità competenti, ai clienti e alle altre parti interessate, rispettando criteri, termini e modalità previsti dai requisiti applicabili. Il processo assicura escalation tempestiva, valutazione della significatività, aggiornamenti sullo stato dell'incidente e una relazione conclusiva sulle cause, sugli impatti e sulle misure adottate.

La qualificazione dell'incidente, le comunicazioni ai destinatari dei servizi, alle autorità, ai clienti e alle altre parti interessate sono coordinate da funzioni autorizzate e tengono conto degli impatti operativi, economici, legali, contrattuali, reputazionali e sui diritti delle persone. Nessun dipendente o fornitore comunica autonomamente all'esterno informazioni su incidenti salvo autorizzazione o obbligo di legge.

7. CONFORMITÀ, VERIFICA E MIGLIORAMENTO

RAFFMETAL S.P.A. mantiene un registro dei requisiti applicabili derivanti dalla strategia aziendale, da leggi e regolamenti, dagli accordi con clienti e partner e dai criteri TISAX pertinenti. La conformità a politiche e procedure è verificata secondo un programma definito mediante controlli di linea, indicatori, verifiche tecniche, audit interni e riesami indipendenti, conservandone evidenze e risultati.

Le non conformità, gli esiti degli audit, gli incidenti, i risultati dei test e le variazioni del rischio generano, quando necessario, azioni correttive con responsabile, priorità e scadenza. L'efficacia delle azioni è verificata e riferita alla Direzione. Gli obiettivi di sicurezza sono misurabili ove praticabile e includono almeno riduzione dei rischi oltre la soglia accettata, tempestività delle correzioni, completamento della formazione, risultati dei test di continuità e gestione degli incidenti.

Direttore Generale

Roberta Niboli



Per ulteriori informazioni, scrivi a:
info@raffmetal.it

