Politica per la sicurezza dei sistemi informativi, di rete e delle informazioni

Costamp Group S.p.a.
Via Verdi, 6 - 23844 Sirone (LC) | +39.031.875195 | info@costampgroup.it
P.I. IT 01763310354 | REA 325890 CCIAA di Lecco

www.costampgroup.com

Versione	1.0
Data di emissione	6/07/2026
Classificazione	Pubblico
Autore	CIO

1 Contesto normativo e ambito di riferimento

Il Decreto Legislativo 4 settembre 2024, n. 138 (di seguito, il "Decreto NIS2") ha recepito nell'ordinamento nazionale la Direttiva (UE) 2022/2555 ("Direttiva NIS2"), definendo un quadro armonizzato di obblighi in materia di sicurezza delle reti e dei sistemi informativi, gestione del rischio informatico, notifica degli incidenti e supervisione da parte delle autorità competenti.

L'Agenzia per la Cybersicurezza Nazionale (ACN) è individuata quale Autorità nazionale competente per l'attuazione e la vigilanza. La Società, in ragione delle attività svolte nell'ambito della filiera della mobilità sostenibile — incluse le funzioni di progettazione, produzione e fornitura di componenti strategici per il settore automotive — è stata inclusa nell'elenco dei soggetti destinatari degli obblighi previsti dal Decreto, in qualità di soggetto rilevante ai sensi dell'art. 3 del medesimo.

La presente Politica per la sicurezza dei sistemi informativi e di rete (di seguito, la "Politica") è adottata in attuazione dell'art. 21, par. 2, lett. a) della Direttiva NIS2 e dell'art. 24 del Decreto, che prevedono l'obbligo per i soggetti destinatari di definire e mantenere una politica documentata in materia di sicurezza delle reti e dei sistemi informativi.

La Politica si applica all'intero perimetro organizzativo, tecnologico e informativo della Società, inclusi i sistemi produttivi, i sistemi informativi gestionali, le infrastrutture di rete, le applicazioni software, i dati aziendali e le infrastrutture tecnologiche, indipendentemente dalla modalità di gestione (on-premise, cloud, ibrida o in outsourcing). Sono destinatari della presente Politica tutti i soggetti che, a qualsiasi titolo, accedano o trattino i sistemi informativi e di rete della Società, incluse le parti esterne nei limiti dei rispettivi rapporti contrattuali.

2 Finalità e natura della presente Politica

La Politica definisce i principi, gli obiettivi e le responsabilità in materia di sicurezza informatica, costituendo il quadro di riferimento per la progettazione, l'attuazione, il monitoraggio e il miglioramento continuo delle misure di sicurezza adottate dalla Società. Essa rappresenta il fondamento del sistema di gestione della sicurezza delle informazioni e delle relative procedure operative.

La presente Politica costituisce un documento di indirizzo strategico e di governo, volto a definire il quadro dei principi, degli impegni e delle priorità entro cui le misure di sicurezza devono essere progettate e attuate. La declinazione operativa dei suoi contenuti è demandata a politiche tematiche e procedure attuative, adottate dai competenti livelli di responsabilità.

La Politica ha carattere vincolante per l'intera organizzazione e si configura come un documento dinamico, soggetto a revisione periodica almeno annuale, nonché ogniqualvolta si verifichino incidenti significativi o mutamenti rilevanti nel contesto operativo o nel profilo di rischio della Società.

3 Impegno per la sicurezza

3.1 Stakeholder

La Società riconosce che la gestione del rischio informatico costituisce un elemento fondamentale per la protezione dei servizi erogati, la tutela degli interessi dei propri clienti e partner, nonché per la continuità operativa delle attività produttive e di fornitura. la Società dipende in misura crescente dalla disponibilità, integrità e riservatezza dei propri sistemi informativi.

La sicurezza dei sistemi informativi e di rete non costituisce un ambito esclusivamente interno, ma incide direttamente sulla fiducia e sulle legittime aspettative di una pluralità di portatori di interesse, tra cui:

- i clienti e partner della filiera automotive, nei confronti dei quali la Società ha obblighi di riservatezza industriale, continuità della fornitura e protezione dei dati tecnici e progettuali condivisi;
- il personale dipendente e i collaboratori, che operano quotidianamente sui sistemi informativi aziendali e rappresentano al contempo un presidio operativo e un potenziale vettore di rischio;
- la Direzione e le strutture di governance della Società, cui compete la responsabilità ultima della supervisione delle misure di sicurezza;
- le Autorità competenti e di vigilanza, in primo luogo l'ACN e il CSIRT Italia, nonché gli altri organismi di controllo cui la Società è soggetta;
- i fornitori, i prestatori di servizi e i partner tecnologici che accedono ai sistemi informativi della Società o ne trattano i dati, la cui catena di approvvigionamento costituisce un vettore di rischio da presidiare;
- gli enti certificatori e organismi di audit, nei confronti dei quali la Società è tenuta a dimostrare la conformità dei propri processi.

3.2 Obiettivi

La presente Politica esprime l'impegno della Società a tutelare le aspettative di tutti i portatori di interesse, mediante l'adozione di un livello di sicurezza adeguato, proporzionato e verificabile. A tal fine, la Società si impegna a perseguire i seguenti obiettivi:

- garantire la riservatezza, l'integrità e la disponibilità delle informazioni e dei sistemi rilevanti per lo svolgimento delle attività aziendali, inclusi i dati tecnici, progettuali, produttivi e commerciali;
- gestire in modo sistematico i rischi connessi alla sicurezza dei sistemi informativi e di rete, attraverso un approccio multirischio e proporzionato che tenga conto dello stato dell'arte, della probabilità e della gravità degli incidenti, nonché del loro potenziale impatto economico e operativo;

- rafforzare la resilienza complessiva della Società, intesa come la capacità di prevenire, resistere, assorbire e ripristinare le proprie funzioni a fronte di eventi avversi che colpiscano i sistemi informativi e di rete;
- rafforzare le capacità di prevenzione, rilevazione, contenimento e risposta agli incidenti di sicurezza, garantendo il rispetto degli obblighi di notifica tempestiva alle Autorità competenti;
- ridurre la superficie di attacco dei sistemi informativi e di rete, adottando misure tecniche e organizzative adeguate allo stato dell'arte, incluse pratiche di igiene informatica, gestione delle vulnerabilità e principi di sicurezza by design e by default;
- garantire la sicurezza della catena di approvvigionamento, valutando e gestendo i rischi derivanti dalle relazioni con i fornitori diretti e i prestatori di servizi;
- promuovere una cultura diffusa della sicurezza informatica a tutti i livelli dell'organizzazione, attraverso programmi di sensibilizzazione e formazione continua;
- assicurare la governance della sicurezza informatica al più alto livello decisionale, garantendo il coinvolgimento diretto della Direzione;
- garantire il rispetto dei requisiti normativi e regolamentari applicabili, con particolare riferimento alla Direttiva NIS2 e al Decreto di recepimento.

3.3 Risorse

La Direzione della Società, nell'approvare la presente Politica, assume formalmente l'impegno a garantire la disponibilità delle risorse necessarie per la sua piena ed efficace attuazione, attraverso:

- la disponibilità di personale sufficiente, dotato delle competenze richieste o messo nelle condizioni di acquisirle mediante percorsi formativi mirati, per l'esercizio dei ruoli e delle funzioni di sicurezza; ove necessario, la Società valuterà il ricorso a figure professionali dedicate o a competenze esterne qualificate;
- la previsione, nei documenti di programmazione economico-finanziaria, delle risorse necessarie a sostenere gli investimenti in sicurezza informatica, coerentemente con i risultati della valutazione del rischio e gli obblighi normativi vigenti;
- la definizione, documentazione e aggiornamento dei processi organizzativi e delle procedure operative necessari a tradurre i principi della presente Politica in azioni concrete, misurabili e verificabili;
- la dotazione di infrastrutture tecnologiche adeguate al livello di sicurezza richiesto, garantendone aggiornamento e manutenzione nel tempo.

L'adeguatezza delle risorse allocate sarà oggetto di riesame periodico da parte della Direzione, sia in occasione della revisione annuale della Politica, sia a fronte di cambiamenti significativi nel profilo di rischio o nel quadro normativo.

3.4 Strategia

La Società riconosce la sicurezza informatica quale condizione abilitante per il perseguimento della propria missione industriale e assume la conformità alla Direttiva NIS2 come obiettivo strategico, da perseguire mediante un approccio progressivo, strutturato e sostenibile, fondato sulla valorizzazione delle iniziative già intraprese e sullo sviluppo di una cultura organizzativa orientata alla sicurezza.

La presente Politica si inserisce organicamente nel sistema dei documenti di governo e di programmazione strategica della Società, della quale costituisce il complemento per i profili attinenti alla sicurezza informatica.

3.5 Classificazione delle informazioni

La Società adotta e mantiene uno schema di classificazione delle informazioni che costituisce uno degli elementi fondanti per l'applicazione differenziata delle misure di protezione in funzione del valore e della sensibilità delle informazioni trattate.

4 Gestione del Rischio

4.1 Identificazione, analisi e valutazione del rischio

La Società adotta un approccio alla sicurezza fondato sulla valutazione del rischio, calibrato sulle proprie specificità industriali, sulla natura dei servizi e prodotti erogati e sul contesto delle minacce rilevanti per il settore automotive e della mobilità sostenibile. I rischi sono identificati, analizzati e valutati con cadenza almeno annuale e ogniqualvolta si verifichino cambiamenti significativi nell'organizzazione, nelle infrastrutture tecnologiche o nel panorama delle minacce. La valutazione considera sia la probabilità di accadimento degli eventi avversi sia la gravità del loro potenziale impatto sulla riservatezza, integrità e disponibilità delle informazioni, nonché sulla continuità operativa.

A ciascun asset sono associati il livello di classificazione, il responsabile e il profilo di rischio derivante anche dall'analisi delle minacce e delle vulnerabilità pertinenti.

I rischi residui che eccedono le soglie di accettabilità formalmente approvate dalla Direzione sono oggetto di trattamento documentato nel Piano di trattamento del rischio.

4.2 Proporzionalità e adeguatezza delle misure

Le misure di sicurezza adottate sono proporzionate al grado di esposizione al rischio rilevato. La Società garantisce un equilibrio efficace tra il livello di protezione assicurato e la sostenibilità organizzativa ed economica degli interventi, privilegiando quelli con maggiore efficacia nella riduzione del rischio residuo.

4.3 Trattamento del rischio

A seguito della valutazione dei rischi, per ciascun rischio identificato la Società definisce e attua una strategia di trattamento che può includere: la riduzione del rischio mediante misure di sicurezza tecniche e organizzative, l'accettazione consapevole del rischio residuo entro soglie predefinite, il trasferimento del rischio anche tramite strumenti assicurativi, oppure l'eliminazione della fonte di rischio. Le decisioni sono documentate nel Piano di trattamento del rischio e sottoposte all'approvazione della Direzione.

4.4 Riesame e miglioramento continuo

I risultati della valutazione del rischio e l'efficacia delle misure di trattamento adottate sono oggetto di riesame almeno annuale nell'ambito del ciclo di gestione del SGSI, per assicurare che la postura di sicurezza della Società rimanga adeguata all'evoluzione del contesto interno ed esterno.

5 Implementazione di misure di sicurezza tecniche e organizzative

In conformità con quanto previsto dall'art. 21 della Direttiva (UE) 2022/2555 e dal relativo Decreto Legislativo di recepimento, la Società si impegna ad adottare misure tecniche e organizzative adeguate e proporzionate, volte a gestire i rischi per la sicurezza dei sistemi informativi e di rete e a prevenire o ridurre al minimo l'impatto di eventuali incidenti. La selezione e il dimensionamento delle misure seguono i criteri di proporzionalità definiti nella presente Politica e sono oggetto di revisione periodica.

5.1 Misure Tecniche

5.1.1 Gestione degli asset

La Società mantiene inventari aggiornati dell'hardware, del software, dei servizi e dei sistemi gestiti, inclusi quelli erogati da fornitori terzi. Tali inventari costituiscono strumenti essenziali per la valutazione dei rischi e per l'adozione mirata delle misure di protezione, e coprono l'intero perimetro degli ambienti IT e OT aziendali.

5.1.2 Gestione delle vulnerabilità

La Società identifica, analizza e registra sistematicamente le vulnerabilità dei sistemi informativi e di rete, attuando un piano strutturato di gestione che ne stabilisce le priorità in coerenza con la valutazione del rischio, assicura l'installazione tempestiva degli aggiornamenti di sicurezza e definisce processi chiari per la ricezione, l'analisi e il trattamento delle segnalazioni di vulnerabilità.

5.1.3 Gestione dell'autenticazione, delle identità digitali e del controllo degli accessi

La Società garantisce che tutte le utenze, incluse quelle con privilegi amministrativi e quelle destinate all'accesso remoto, siano censite, approvate e, ove possibile, individuali. I permessi sono assegnati secondo i principi del privilegio minimo e della separazione delle funzioni. Le modalità

di accesso remoto sono definite, documentate e adeguatamente protette, con impiego dell'autenticazione a più fattori per i sistemi rilevanti.

5.1.4 Protezione delle reti e delle comunicazioni

La Società protegge le proprie reti mediante sistemi perimetrali e di segmentazione aggiornati, configurati e mantenuti in modo coerente con il profilo di rischio. Le attività consentite da remoto sono definite e documentate, con un elenco aggiornato dei sistemi accessibili da remoto e delle relative misure di protezione.

5.1.5 Sicurezza dei dati

La Società adotta misure per proteggere i dati memorizzati su dispositivi e sistemi aziendali, inclusa la cifratura per i dati sensibili e i supporti rimovibili. I protocolli di trasmissione dei dati verso l'esterno sono costantemente aggiornati e considerati sicuri. I backup dei dati e delle configurazioni sono eseguiti con regolarità, conservando copie offline per i sistemi rilevanti e verificandone periodicamente l'integrità.

5.1.6 Configurazione, manutenzione e dismissione dei sistemi

La Società si impegna a utilizzare software per il quale è garantita la disponibilità continuativa di aggiornamenti di sicurezza. Gli accessi remoti e privilegiati sono registrati e i log conservati in modo sicuro per un periodo determinato dalla valutazione del rischio. Lo sviluppo di software viene commissionato a società esterne nel rispetto di pratiche di sviluppo sicuro lungo l'intero ciclo di vita, secondo il principio di security by design.

5.1.7 Sicurezza fisica

La Società adotta misure di sicurezza fisica commisurate al rischio, al fine di prevenire accessi non autorizzati alle infrastrutture tecnologiche e garantire la protezione dei sistemi informativi e di rete rilevanti, con particolare attenzione agli ambienti produttivi e ai centri elaborazione dati.

5.1.8 Monitoraggio degli eventi di sicurezza e rilevamento degli incidenti

La Società mantiene capacità tecniche aggiornate per il rilevamento tempestivo degli eventi di sicurezza e degli incidenti significativi, definendo i livelli di servizio attesi e adottando sistemi di protezione e monitoraggio per il rilevamento e il contenimento di codice malevolo e comportamenti anomali.

5.1.9 Risposta agli incidenti e ripristino

La Società definisce, attua e aggiorna periodicamente un piano di gestione degli incidenti di sicurezza informatica, comprensivo delle procedure di notifica al CSIRT Italia, delle modalità di comunicazione interna ed esterna, incluso il coinvolgimento della Direzione, e delle azioni necessarie per il ripristino del normale funzionamento dei sistemi.

5.1.10 Continuità operativa, disponibilità e ripristino da disastro

La Società assume il seguente impegno in materia di continuità operativa e disponibilità dei sistemi informativi:

La Società identifica e mantiene aggiornato l'elenco dei servizi IT e OT critici per la continuità operativa, tenendo conto del loro impatto sul business (*Business Impact Analysis*, BIA). Ai sistemi critici sono assegnati gli obiettivi di disponibilità richiesta:

- **Obiettivi di ripristino (RTO e RPO)**: per ciascun servizio o sistema IT critico identificato sono definiti e formalmente approvati il *Recovery Time Objective* (RTO) e il *Recovery Point Objective* (RPO), in proporzione alla criticità del servizio e all'impatto atteso di un'interruzione sulle attività produttive e sulla sicurezza delle informazioni.

La Società predispone, mantiene e verifica periodicamente un Piano di Continuità Operativa e Ripristino per i servizi e sistemi IT critici. I piani includono strategie alternative per la comunicazione, l'archiviazione e l'alimentazione elettrica. I piani sono approvati dalla Direzione e sottoposti a test almeno annuale.

Le strategie di backup per i sistemi critici sono definite in coerenza con gli RTO e RPO approvati, con verifica periodica dell'integrità e della recuperabilità delle copie, incluse quelle offline.

6 Revisione della Politica e miglioramento continuo

La Società si impegna a sottoporre la presente Politica a revisione periodica, tenendo conto degli aggiornamenti della valutazione del rischio, delle modifiche normative, delle raccomandazioni dell'ACN o dell'ENISA, delle buone pratiche di settore, dei risultati degli audit e degli incidenti occorsi.

7 Comunicazione, diffusione e riconoscimento

La Società si impegna a pubblicare la presente Politica nei canali informativi interni aziendali.

8 Riferimenti normativi e di indirizzo

La presente Politica è redatta in conformità al seguente quadro normativo e di indirizzo:

Normativa europea

- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione ("Direttiva NIS2"), e in particolare l'art. 21, par. 2, lett. a);
- Regolamento di esecuzione (UE) 2024/2690 della Commissione, del 17 ottobre 2024, recante le modalità di applicazione della Direttiva NIS2 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza;

Normativa nazionale di recepimento

- Decreto Legislativo 4 settembre 2024, n. 138, recante il recepimento della Direttiva (UE) 2022/2555 nell'ordinamento italiano, e in particolare gli artt. 24, 25 e 26;

Atti delle Autorità competenti

- Determinazione del Direttore Generale dell'ACN del 14 aprile 2025, n. 136117, recante le Specifiche per l'adozione delle misure di sicurezza per i soggetti di cui all'articolo 3 del decreto NIS2;
- Linee guida dell'ACN — dicembre 2025 — per la definizione del processo di gestione degli incidenti di sicurezza informatica;

Linee guida e standard di riferimento

- ENISA, Technical Implementation Guidance on Cybersecurity Risk Management Measures, versione 1.0, giugno 2025;
- VDA, ISA v.6.0.3;
- NIST Cybersecurity Framework (CSF) 2.0.

Direzione	CIO
Data	Data
07/07/2026	07/07/2026

Costamp Group S.p.a.
Via Verdi, 6 - 23844 Sirone (LC) | +39.031.875195 | info@costampgroup.it
P.I. IT 01763310354 | REA 325890 CCIAA di Lecco

www.costampgroup.com