

Lo scopo della direttiva NIS2 è l'introduzione di requisiti di base di sicurezza informatica per tutti i settori produttivi più critici, con lo scopo di ottenere un sistema economico e sociale resiliente alle perturbazioni esterne



## OT cybersecurity e Direttiva NIS2

Foto: Shutterstock

Schmersal Italia, con i suoi servizi di OT cybersecurity, accompagna i suoi clienti verso l'adeguamento alla Direttiva NIS2 e al Regolamento Macchine

Francesco Astolfo

**P**er 80 anni Schmersal è stata sinonimo di qualità e affidabilità nel settore della Sicurezza Macchine, fornendo prodotti sempre all'avanguardia e servizi, tramite il dipartimento 'tec.nicum', di formazione, consulenza, ingegneria e integrazione. Da quando il tema della sicurezza informatica applicata all'ambiente industriale si è posto con forza all'attenzione dei fabbricanti di macchine e system integrator, Schmersal Italia ha inserito nella propria offerta servizi specifici per la cybersecurity, soprattutto nell'ottica dei nuovi requisiti richiesti dal 20 gennaio 2027 per la marcatura CE dei macchinari dal Regolamento Macchine. Ma senza aspettare il 2027, un'altra scadenza più urgente ci interpella: la registrazione sul portale di ACN - Agenzia per la Cybersecurity Nazionale, dei soggetti che rientrano nel perimetro di applicazione della direttiva NIS2. Lo scopo di questa direttiva europea, recepita dall'Italia con il dlgs n°138/2024, è l'introduzione di requisiti di base di sicurezza informatica per tutti i settori produttivi più critici, con lo scopo di ottenere un sistema economico e sociale resiliente alle perturbazioni esterne. I soggetti interessati, medie e grandi aziende, tranne casi particolari, si possono individuare facilmente, e naturalmente i soggetti essenziali

che insistono su settori altamente critici avranno requisiti più stringenti rispetto ai soggetti importanti. Sostanzialmente le piccole e micro-imprese risultano quasi totalmente escluse dal perimetro (salvo poi rientrare in relazione alla catena di approvvigionamento), mentre per alcuni settori l'identificazione dei soggetti è legata al codice Ateco: ad esempio, nel settore della 'fabbricazione' sono inclusi tutti i codici Ateco dal 26 al 30. I soggetti interessati dovrebbero essersi già registrati sul portale di ACN, dove si trovano tutte le informazioni necessarie per portare a termine la procedura; dal 1° gennaio al 28 febbraio 2026 si apre la registrazione 2026, dove i soggetti pubblici e privati per cui i presupposti di ingresso nel perimetro NIS si sono verificati nel 2025, devono designare il punto di contatto e registrarsi sul portale dei servizi ACN. In questo periodo anche i soggetti già registrati devono confermare o modificare i dati già inseriti nel 2025. Per i nuovi soggetti è da sottolineare, in particolare per i gruppi di imprese, la possibilità di applicare la clausola di salvaguardia (art.3 comma 4 del decreto) per richiedere la valutazione separata della singola azienda, in modo che possa essere valutata come piccola impresa e quindi tendenzialmente esterna al perimetro NIS.



## sicurezza nei sistemi di automazione

| Settore                                                                 | Dettaglio                | Grandi imprese                | Medie imprese           | Piccole/micro imprese     |
|-------------------------------------------------------------------------|--------------------------|-------------------------------|-------------------------|---------------------------|
| SETTORI ALTAMENTE CRITICI                                               |                          |                               |                         |                           |
| Energia (con nuovi sottosettori/tipologie di soggetti)                  | 19 tipologie di soggetto | Essenziali                    | Importanti <sup>1</sup> | Fuori ambito <sup>2</sup> |
| Trasporti                                                               | 10 tipologie di soggetto |                               |                         |                           |
| Settore bancario                                                        | DORA Lex specialis       |                               |                         |                           |
| Infrastrutture dei mercati finanziari                                   |                          |                               |                         |                           |
| Settore sanitario (con nuovi sottosettori/tipologie di soggetti)        |                          |                               |                         |                           |
| Acqua potabile                                                          | 1 tipologia di soggetto  |                               |                         |                           |
| Acque reflue                                                            | 1 tipologia di soggetto  |                               |                         |                           |
| Infrastrutture digitali (con nuovi sottosettori/tipologie di soggetti)  | 9 tipologie di soggetto  |                               |                         |                           |
| Gestione dei servizi TIC (b2b)                                          | 2 tipologie di soggetto  |                               |                         |                           |
| Spazio                                                                  | 1 tipologia di soggetto  |                               |                         |                           |
| SETTORI CRITICI                                                         |                          |                               |                         |                           |
| Servizi postali e di corriere                                           | 1 tipologia di soggetto  |                               |                         |                           |
| Gestione dei rifiuti                                                    | 1 tipologia di soggetto  |                               |                         |                           |
| Fabbricazione, produzione e distribuzione di sostanze chimiche          | 1 tipologia di soggetto  |                               |                         |                           |
| Produzione, trasformazione e distribuzione di alimenti                  | 1 tipologia di soggetto  |                               |                         |                           |
| Fabbricazione                                                           | 6 tipologie di soggetto  |                               |                         |                           |
| Fornitori di servizi digitali (con nuovi sottosettori/tip. di soggetti) | 4 tipologie di soggetto  |                               |                         |                           |
| Ricerca                                                                 | 2 tipologie di soggetto  |                               |                         |                           |
| ULTERIORI TIPOLOGIE DI SOGGETTI                                         |                          |                               |                         |                           |
| Pubblica Amministrazione centrale                                       | 4 categorie di PA        | Identificazione dell'Autorità |                         |                           |
| Pubblica Amministrazione regionale e locale                             | 11 categorie di PA       |                               |                         |                           |
| Ulteriori tipologie di soggetti                                         | 4 tipologie di soggetti  |                               |                         |                           |

Fonte sito ACN

I soggetti interessati, quali medie e grandi aziende, tranne casi particolari, si possono individuare correttamente nella tabella proposta da ACN

### La risposta

Dopo la nuova registrazione, entro aprile 2026 ACN risponderà con la valutazione definitiva dell'azienda, tra essenziale, importante oppure fuori ambito. I soggetti già registrati entro il 31 dicembre 2025, hanno potuto procedere alla designazione del referente Csirt per l'interlocuzione con il Csirt Italia secondo le modalità rintracciabili nel sito di ACN. Il referente, in possesso di competenze tecniche così come i suoi sostituti, sarà responsabile della notifica tempestiva degli incidenti rilevanti, quelli cioè che hanno provocato un grave danno economico per l'azienda o le persone, furto di informazioni oppure un blocco della filiera: questo obbligo scatta da gennaio 2026 e diventa la prima vera scadenza operativa per le aziende. La notifica, sempre ad ACN, va eseguita in tempi rapidi: 24 ore per la segnalazione e 72 ore per la notifica definitiva. Queste tempistiche rapide richiedono che l'azienda possieda già una politica di cybersecurity della cui attuazione si occupano in prima persona gli organi di gestione della società, come sottolinea il decreto all'articolo 23.

Chi gestisce la società deve preoccuparsi, obbligatoriamente, di capire cosa sia la cybersecurity e come impatti sulla continuità aziendale e i relativi risultati economici; tale formazione di base va estesa a tutto il personale, soprattutto in virtù del fatto che il fattore umano è il primo elemento di rischio per la sicurezza.

### Misure tecniche

La politica di sicurezza informatica comprende delle specifiche misure tecniche, che vengono richiamate esplicitamente dalla direttiva, per un sistema multi-rischio: non solo formazione, non solo misure tecniche, non solo gestione operativa ma l'insieme di tutto questo. Tecnicamente, Enisa - Agenzia per la Cybersecurity Europea, nella guida all'implementazione, richiama esplicitamente la ISO/IEC 27001, standard internazionale per la gestione della sicurezza delle informazioni. Considerato che la NIS2 impatta maggiormente i settori produttivi sarà d'obbligo includere la norma di riferimento per la OT Cybersecurity, ISA/IEC 62443, serie internazionale di standard che affrontano la sicurezza informatica

per la tecnologia operativa nei sistemi di automazione e controllo. Il legislatore ha correttamente impostato i requisiti secondo i principi di proporzionalità e adeguatezza, al fine di richiedere uno sforzo economico per l'implementazione della politica di cybersecurity compatibile con le dimensioni aziendali e la valutazione del rischio. Il decreto, infine, si conclude con il capitolo delle sanzioni, notevoli per chi non si adegua: non è questo, comunque, il senso di una direttiva che non mira a colpire le aziende ma, bensì, a renderle consapevoli dei pericoli a cui sono esposte, soprattutto su macchinari e impianti dove l'attenzione alla cybersecurity non è sempre stata così elevata.

### Un partner affidabile

Schmersal Italia è al fianco delle aziende che vogliono affrontare questo percorso. La proposta è differenziata per system integrator, fabbricanti di macchine e aziende manifatturiere. Per i system integrator, molto spesso piccole o micro imprese, propone innanzitutto un assessment sulla postura dell'azienda, in particolare per la grande criticità che assume l'ufficio di produzione del software nei confronti dei clienti (collaudi, assistenze da remoto, ecc.). Di seguito, attività di formazione mirata e differenziata, in modo che la progettazione hardware e software soddisfi i requisiti richiesti dalle norme internazionali, soprattutto la ISA/IEC 62443. Per i fabbricanti di macchine, il percorso è simile, con la possibilità di assessment dedicati su macchine o modelli di macchine standard, per validare la loro configurazione, anche in vista dei nuovi requisiti richiesti dal Regolamento Macchine. Infine, le aziende manifatturiere: l'esperienza di Schmersal nella Sicurezza Macchine e nei temi dell'automazione consente di migliorare il lato più critico di queste organizzazioni, vale a dire il reparto produttivo, dove spesso si mescolano attrezzature recenti con macchinari antiquati dove sistemi operativi obsoleti non possono essere aggiornati.

Schmersal Italia - [www.schmersal.it](http://www.schmersal.it)