

**Corso - 08/06/2026**

## **Direttiva NIS 2 per i costruttori di macchine industriali**

**Corso di formazione sui requisiti tecnici, organizzazione interna, supply chain e gestione degli incidenti.**

### **Obiettivi**

- Comprendere in modo approfondito il quadro normativo e gli impatti operativi della Direttiva NIS 2 nel contesto industriale;
- tradurre gli obblighi normativi in azioni concrete di compliance e gestione organizzativa;
- rafforzare la resilienza aziendale e la capacità di risposta agli incidenti cyber;
- integrare gli aspetti legali e tecnici nella cybersecurity della supply chain.

### **Programma**

#### **Parte 1: Organizzazione delle risorse interne, compiti e ruoli per la conformità aziendale**

Introduzione e contesto normativo:

- obblighi generali di governance;
- focus su articoli più rilevanti: (Art. 20, 21 e 23).

La gestione delle risorse interne secondo NIS 2:

- politiche interne e piani di cybersecurity;
- la responsabilità del management e il ruolo del CISO (Chief Information Security Officer);
- risorse umane e sicurezza: formazione, access control, policy di autenticazione;
- mappatura degli obblighi delle principali figure professionali.

#### **Parte 2: La gestione degli incidenti cyber: obblighi normativi e misure tecniche da adottare**

##### **Quadro legale: gestione degli incidenti in NIS 2**

Normativa di riferimento:

- le misure di gestione del rischio;
- gli obblighi di notifica degli incidenti;
- le responsabilità del management.

Definizione di incidente e "Incidente significativo".

Obblighi interni:

- la predisposizione di piani di risposta;cCompiti e responsabilità delle principali figure coinvolte (CISO, DPO (Data Protection Officer), management).

Rapporti esterni:

- comunicazioni a CSIRT, autorità competenti e utenti;
- interazione con il GDPR (violazione dati personali).

##### **Aspetti tecnici: misure tecniche da adottare**

- misure previste a livello organi di amministrazione e direttivi.
- obblighi ex. Artt. 24, e 25;
- framework nazionale per la Cybersecurity e la Data Protection;
- standard di riferimento;
- determinazioni dell'Agenzia Cybersecurity Nazionale. Modalità e specifiche di base e relativi ambiti per soggetti importanti e essenziali.

### **Parte 3: La gestione della supply chain: aspetti legali e tecnici**

#### **Introduzione e inquadramento normativo**

- Supply chain nella NIS 2.
- Obblighi per soggetti essenziali e importanti.
- Responsabilità del management e accountability.
- Rapporti con altri atti UE: Cyber Resilience Act, GDPR.

#### **Contratti e governance legale della supply chain**

- Clausole contrattuali tipiche per la cybersecurity:  
"Right to audit" e verifiche di sicurezza;  
obblighi di notifica degli incidenti;  
subfornitura e cascading obligations;  
certificazioni e attestazioni di conformità.
- Integrazione con i sistemi di gestione (ISO 27001, ISO 9001).

#### **Aspetti tecnici della supply chain cybersecurity**

- Determinazione ACN modalità e specifiche di base relative alla supply chain;
- fattispecie di servizi acquisiti rilevanti in ambito NIS2;
- declinazione delle modalità e specifiche di base ACN per tali servizi;
- casi tipici e modalità di gestione.

#### **Ulteriori informazioni**

La quota di partecipazione è comprensiva di materiale didattico in formato digitale e attestato di partecipazione.  
Si intendono aziende associate quelle aderenti alle associazioni: ACIMAC, ACIMALL, AMAPLAST, FEDERTEC E UCIMA.

#### **Destinatari**

Direttori generali, responsabili compliance e risk management; responsabili IT; responsabili legali; responsabili tecnici, responsabili qualità e supply chain, responsabili formazione e HR.

#### **Durata**

11 ore

#### **Quota di adesione:**

**600,00 € + IVA a persona per le aziende associate**

750,00 € + IVA a persona per le aziende non associate

#### **Date e Sedi di svolgimento**

08/06/2026 14.00-17.00 - ONLINE

15/06/2026 14.00-18.00 - ONLINE

18/06/2026 09.00-13.00 - ONLINE