

# Cybersecurity e NIS2

L'impatto su PMI e Attività Professionali

*Come proteggere la tua impresa nella nuova era normativa*

Team PAC: Privacy • Artificial Intelligence • Cybersecurity

# Cosa Vedremo Oggi

- 1. La NIS2: cosa cambia e chi è coinvolto**
- 2. L'impatto concreto su PMI e professionisti**
- 3. Le sfide che affrontate ogni giorno**
- 4. Come individuare rischi e calcolare impatti**
- 5. L'approccio integrato del Team PAC**
- 6. Passare da compliance formale a protezione reale**

# NIS2: La Direttiva che Cambia Tutto



## La NIS2 in breve

- Direttiva UE 2022/2555
- Recepimento Italia: **entro ottobre 2024**
- Estende obblighi cyber a **molte più aziende**
- Introduce **responsabilità diretta del management**
- Sanzioni fino a **10 milioni € o 2% fatturato**



## Chi è coinvolto?

### Settori essenziali:

Energia, trasporti, banche, sanità, PA digitale, ICT

### Settori importanti:

Servizi postali, gestione rifiuti, food, manifattura chimica, digitale, ricerca

### Fornitori di servizi digitali:

Cloud, datacenter, CDN, DNS, marketplace

# NIS2: Non Solo Grandi Aziende



**Soglie dimensionali:** Aziende con  $\geq 50$  dipendenti o  $\geq 10\text{M€}$  fatturato

## Piccola Impresa

10-49 dipendenti

Fatturato  $< 10\text{M€}$

✓ Coinvolta se settore  
essenziale/importante

## Media Impresa

50-249 dipendenti

Fatturato  $< 50\text{M€}$

✓ Sicuramente coinvolta

## Grande Impresa

$\geq 250$  dipendenti

Fatturato  $\geq 50\text{M€}$

✓ Sempre coinvolta

# Cosa Richiede Concretamente la NIS2

## Misure Tecniche

- Gestione rischi e sicurezza reti
- Gestione incidenti e business continuity
- Crittografia e backup
- Controllo accessi e autenticazione

## Misure Organizzative

- Policy di sicurezza delle informazioni
- Formazione personale obbligatoria
- Gestione supply chain (fornitori)
- Notifica incidenti entro 24-72h

## Responsabilità Management

- **Gli amministratori** rispondono personalmente
- Approvazione misure di sicurezza
- Supervisione implementazione
- Formazione obbligatoria dirigenti

## Sanzioni Severe

Fino a **10 milioni €**  
o **2% fatturato annuo mondiale**

- + Sospensione certificazioni
- + Esclusione da gare pubbliche

# Il Problema delle PMI e Professionisti

## Non so da dove iniziare

*"Quali sistemi devo proteggere? Dove sono i dati sensibili? Chi ha accesso? Quali sono le vulnerabilità critiche? Non ho visibilità."*

## Budget limitati

*"Un penetration test costa 10-20k€. Un avvocato privacy, un tecnico cyber, un consulente ISO... costi impossibili per una PMI."*

## Tempo e coordinamento

*"Devo gestire l'azienda. Non posso passare settimane a coordinare consulenti diversi che parlano linguaggi diversi e chiedono le stesse cose."*

## Compliance formale vs reale

*"Ho policy bellissime e documenti perfetti. Ma nella realtà backup su chiavetta USB, password su post-it, nessun piano di disaster recovery."*

# Le Tre Domande a cui Dovete Rispondere

**1. DOVE** sono i rischi nella mia azienda?

**2. QUANTO** impattano sul mio business?

**3. COME** mi proteggero tecnicamente e organizzativamente?

# La Risposta: Il Team PAC

*Privacy • Artificial Intelligence • Cybersecurity*

**Un team integrato di 5 specialisti che lavorano coordinati:**

- ✓ **Identifica TUTTI i rischi** (tecnici, legali, organizzativi, AI)
- ✓ **Calcola l'IMPATTO reale** sul vostro business con scoring oggettivo
- ✓ **Definisce PIANI di protezione e remediation** (progetta il percorso)
- ✓ **Implementa PROTEZIONI concrete** (non solo documenti)
- ✓ **Si coordina DA SOLO** — voi avete un unico referente
- ✓ **Garantisce COERENZA** tra documenti e realtà operativa

# I Partner del Team PAC



## Studio Legale Carozzi e Associati

Coordinamento legale • GDPR • NIS2 • Audit legali •  
Contratti DPA



## Risk Solver Srl

CyberAudit • Cybersecurity • MSSP • AI Act  
consulting



## Programma Radon Srl

Privacy • Sicurezza lavoro • ISO • Formazione  
accreditata



## Mainlab Srl

Remediation IT • Infrastrutture sicure • Backup •  
Network security



## Carosella Group

Motore GRC • Analisi rischi • Scoring compliance •  
Valutazione impatti business

# Come Funziona: Fase 1-Assessment Integrato

## FOTOGRAFIAMO LA SITUAZIONE REALE

### Scansione Perimetro Cyber

Risk Solver: scansione esterna vulnerabilità, porte aperte, credenziali compromesse, configurazioni non sicure, superficie d'attacco

### Questionario GDPR/NIS2

35-118 domande calibrate su dimensione aziendale: mappatura processi, trattamenti dati, conformità normativa, misure organizzative

### Analisi Rischi e Scoring GRC

Carosella Group: calcolo scoring compliance oggettivo, valutazione impatti business quantificati, prioritizzazione rischi con analisi costi-benefici

### Audit Legale e Contrattuale

Studio Carozzi: analisi contratti con fornitori/clienti, policy interne, gap normativi GDPR/NIS2, rischi legali, DPA e nomine

# Fase 2: Gap Analysis e Report Integrato

IL TEAM PRODUCE UN DOCUMENTO UNICO COORDINATO

## Report che contiene:

- ✓ Vulnerabilità Cyber critiche e loro impatto su continuità operative
- ✓ Gap di conformità GDPR/NIS2 con potenziali sanzioni quantificate
- ✓ Carenze organizzative e procedurali (formazione, policy, gestione accessi)
- ✓ Scoring di rischio oggettivo calcolato in base a Standard ISO31000
- ✓ Priorità di intervento con analisi costi-benefici e ROI stimato
- ✓ Piano di remediation dettagliato con tempistiche e responsabilità

# Fase 3: Remediation Coordinata

**OGNI SPECIALISTA NEL SUO CAMPO, MA SINCRONIZZATI**

## **Mainlab Srl**

Messa in sicurezza IT: firewall configurati, backup cifrati automatici, MFA implementata, logging centralizzato, segmentazione rete, configurazioni hardened

## **Studio Legale Carozzi**

Documenti legali: policy aggiornate, contratti DPA con fornitori, nomine DPO, procedure data breach, compliance NIS2, audit legali periodici, aggiornamenti normativi

## **Programma Radon Srl**

Coordinamento privacy: implementazione SGP, formazione GDPR dipendenti, documentazione completa, supporto certificazioni ISO 27001

## **Risk Solver Srl**

Monitoraggio continuo sistemi ICT, Sistemi di protezione Cyber, check cyber periodici, programmi verifica fornitori, supporto negoziazione assicurazioni cyber, consulenza AI Act



## **Carosella Group**

Consulenza Risk Analysis & Compliance, Sviluppo motori GRC, Risk Scoring, Valutazione impatti di business, Gestione crisi d'impresa

# I Vantaggi Concreti per la Vostra Azienda



## Visibilità Totale

Sapete esattamente DOVE sono i rischi, QUANTO impattano sul business con scoring oggettivo, COSA fare per proteggervi con priorità chiare



## Un Solo Referente

Non coordinate 5 consulenti diversi. Il team PAC si coordina internamente, voi avete una sola persona di contatto e un solo report



## Protezione Vera, Non Carte

Implementazione tecnica reale: firewall configurati, backup cifrati funzionanti, MFA attiva, disaster recovery testato. Conformità NIS2 operativa



## Costi Ottimizzati

Zero duplicazioni. Ogni attività produce valore per più ambiti: stesso assessment serve per GDPR, NIS2 e ISO. Efficienza massima

# Prima e Dopo il Team PAC

## ✗ PRIMA

- Consulenti scollegati
- Stesse informazioni chieste 3 volte
- Nessuno si parla
- Documenti bellissimi, realtà scadente
- Gap invisibili tra IT e legale
- Voi fate da tramite
- Costi duplicati
- Nessuna visione d'insieme
- In caso di ispezione: panico
- Non sapete se siete protetti

## ✓ DOPO

- Team coordinato dal primo giorno
- Un solo assessment completo
- Linguaggio comune pre-stabilito
- Documenti = Realtà operativa
- Coerenza totale IT-Legale
- Un solo referente per voi
- Efficienza massima
- Visione 360° dei rischi
- In caso di ispezione: tranquillità
- Protezione reale verificata

# Una iniziativa interessante per gli Studi Professionali

---

Il Servizio PAC è la base documentale per consulenze professionali  
in privacy, AI e cybersecurity



**REGISTRATEVI PER ATTIVARE  
LA PARTNERSHIP**

[www.conformitadigitale.it/studi\\_professionali](http://www.conformitadigitale.it/studi_professionali)

Riceverete:

- ✓ Materiale informativo per i vostri clienti
- ✓ Pricing partner personalizzato
- ✓ Supporto commerciale e tecnico

✉ [info@conformitadigitale.it](mailto:info@conformitadigitale.it)

*Grazie per l'attenzione*

# Non Siete Soli

La NIS2 e la cybersecurity sono sfide complesse.

Ma con il team giusto — specializzato e coordinato —  
la vostra azienda può essere protetta davvero.

**Team PAC**

*Il team che identifica i rischi, calcola gli impatti  
e protegge il vostro business per voi*