REGIONE PIEMONTE

CSI your digital partner

WEBINAR
SICURI di essere **SICURI?**

NIS2 e Governance by Design: quando la sicurezza diventa una responsabilità di tutta l'azienda

La governance NIS2

Avv. Maria Livia Rizzo Studio Legale Stefanelli & Stefanelli

Avete, oggi, un Piano di gestione del rischio NIS2 approvato (e non solo visto) dal vostro organo di vertice?

La percezione diffusa (ed è quella sbagliata)

NIS2
Direttiva (UE) 2022/2555,
recepita in Italia con il **D.Lgs. 4 settembre 2024, n. 138**,
in vigore dal 16 ottobre 2024

SBAGLIATO

Cosa si pensa

«NIS2 = cosa fare quando succede un incidente»

CORRETTO

Cosa prevede la norma

«NIS2 = un sistema di gestione permanente: budget, calendario, responsabilità»

L'art. 23 del D.Lgs. 138/2024, in tre verbi

Organi di **amministrazione** e organi **direttivi** dei soggetti essenziali e importanti

APPROVANO

le modalità di attuazione delle misure di gestione del rischio

SOVRINTENDONO

all'implementazione degli obblighi previsti dal decreto

RISPONDONO — personalmente

incapacità a svolgere funzioni dirigenziali all’interno del medesimo soggetto – sospensione temporanea (art. 38, D.Lgs. 138/2024)

Undici decisioni e non undici scartoffie

Le Linee Guida ACN (settembre 2025) individuano undici documenti strategici da approvare formalmente.

Documento	Riferimento requisito
Organizzazione per la sicurezza informatica.	GV.RR-02 punto 1.
Politiche di sicurezza informatica.	GV.PO-01 punto 1.
Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete.	ID.RA-05 punto 3.
Piano di trattamento del rischio.	ID.RA-06 punto 3.
Piano di gestione delle vulnerabilità.	ID.RA-08 punto 4.
Piano di adeguamento.	ID.IM-01 punto 1.
Piano di continuità operativa.	ID.IM-04 punto 1.
Piano di ripristino in caso di disastro.	ID.IM-04 punto 1.
Piano di gestione delle crisi.	ID.IM-04 punto 1.
Piano di formazione.	PR.AT-01 punto 1.
Piano per la gestione degli incidenti di sicurezza informatica.	RS.MA-01 punto 2.

ACN aggiorna le FAQ su organi di amministrazione e direttivi

Nuove FAQ ODA.10, ODA.11, ODA.12 — integrate ODA.8 e ODA.9 · acn.gov.it/portale/faq/nis

Indelegabile (ODA.8–9)

L'approvazione dei documenti ex art. 23 resta competenza esclusiva dell'organo collegiale o monocratico; è delegabile solo **l'attuazione operativa** degli obblighi.

Strategico VS tecnico (ODA.10)

Serve approvazione del vertice solo per **indirizzi e pianificazione strategica** delle misure. **Procedure, istruzioni operative e manuali tecnici** li aggiornano le strutture competenti, senza approvazione.

Libertà di forma (ODA.11–12)

Un **documento unico o più documenti** coordinati, a scelta del soggetto.

Fonte: Agenzia per la Cybersicurezza Nazionale, FAQ NIS — acn.gov.it/portale/faq/nis

Un sistema di gestione ha quattro caratteristiche

Ricorrenza

Non un progetto che si esaurisce ma un ciclo che si ripete ogni anno

Documentazione strutturata

Decisioni di governance, non allegati tecnici

Costo pianificabile

A budget pluriennale, non scoperto in emergenza

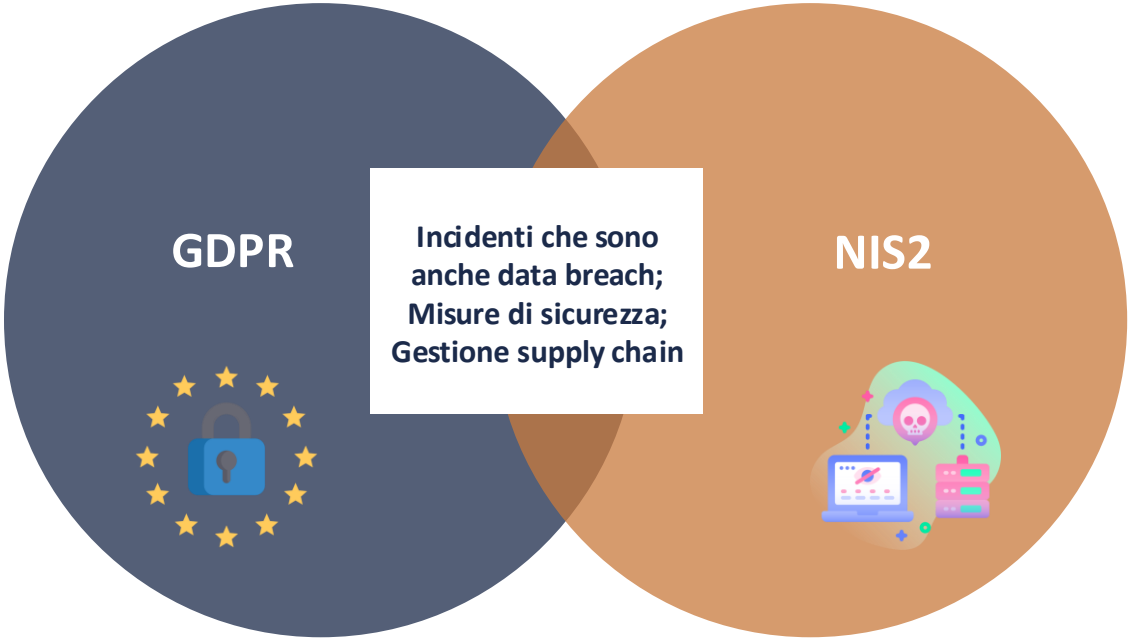
Ciclo di controllo

Si rivede, si misura, si aggiorna. Il ciclo si ripete ogni anno.

Il cortocircuito che vediamo più spesso

NIS2 non è «GDPR bis» — ma viene spesso gestita come se lo fosse.

NIS2 e GDPR: due mondi che si toccano, non si sovrappongono



Il confronto, in sintesi

	GDPR	NIS2
Interesse protetto	Dati personali delle persone fisiche	Resilienza di reti e sistemi informativi
Autorità competente	Garante per la protezione dei dati personali	Agenzia per la Cybersicurezza Nazionale (ACN)
Perimetro	Trattamento di dati personali	Sicurezza operativa, a prescindere dal trattamento dati
Sanzioni massime	20 mln € o 4% fatturato mondiale	10 mln €/2% (essenziali) — 7 mln €/1,4% (importanti)
Responsabile ex lege	Titolare del trattamento	Organi di amministrazione e direttivi (art. 23)

Tre modi sbagliati di organizzarsi

Solo IT

Tecnicamente corretto, ma il vertice non ne prende mai davvero possesso.

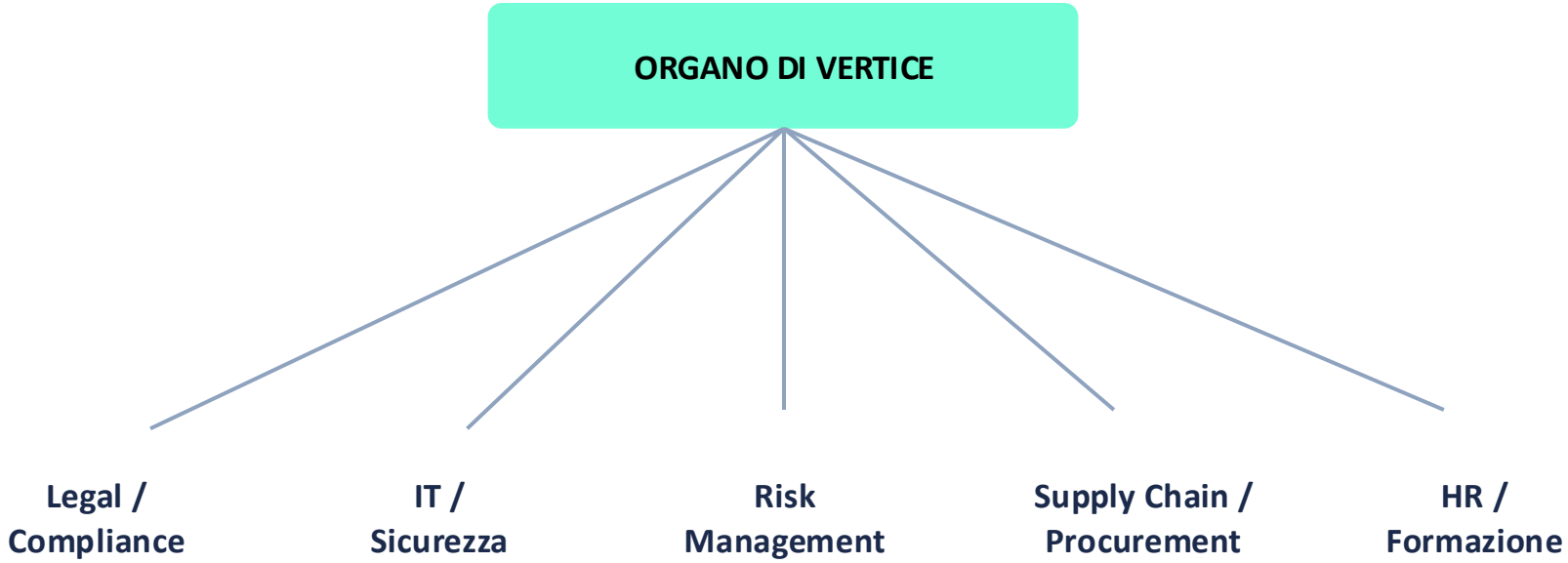
Solo DPO / privacy

Competenze costruite sul GDPR, non sulla continuità operativa e la sicurezza infrastrutturale.

«Tanto abbiamo già la privacy»

Il perimetro NIS2 è diverso e più ampio

Un presidio e non una delega



Quattro domande, prima della fine dell'estate

1 **PREVENZIONE**

Esiste un calendario annuale delle attività NIS2?

2 **RISORSE**

Chi sa leggere un incidente sia in chiave cyber sia in chiave data breach?

3 **ATTIVITÀ**

Chi fa cosa? E sopravvive al turnover?

4 **COSTI**

È a budget pluriennale, o si scopre in emergenza?

Il vantaggio non è la compliance

È la capacità di ridurre il numero e la gravità degli incidenti.

Grazie.