
NIS2, Governance e Compliance

**Focus sulla ultime novità introdotte da ACN**

02 luglio 2026

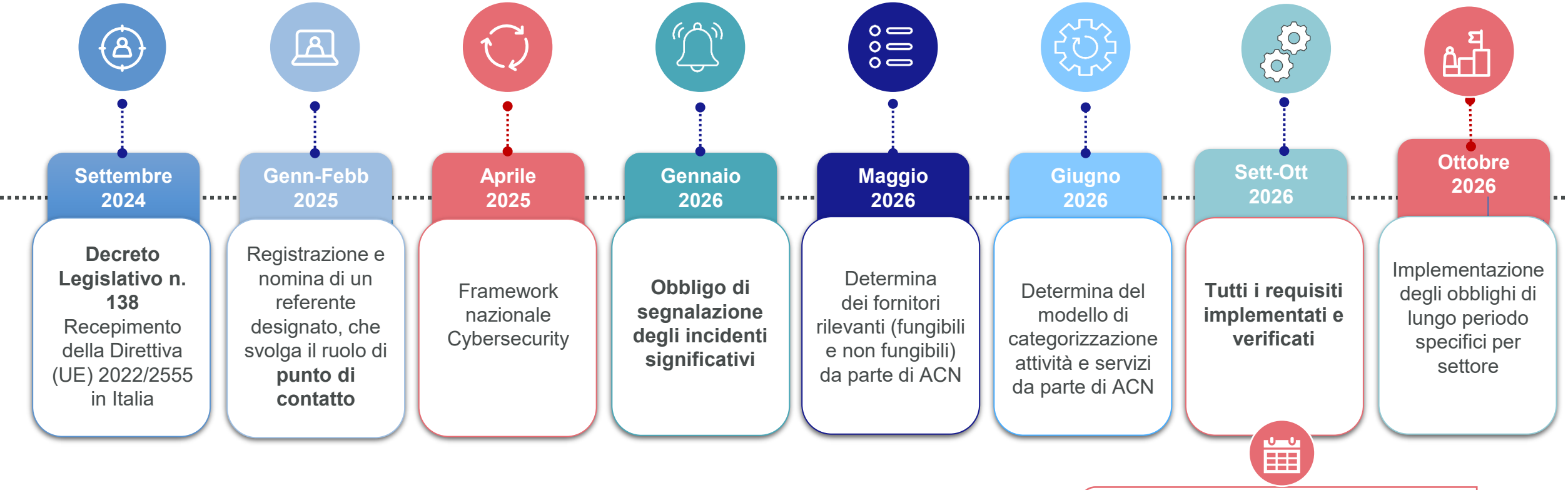
forvis mazars

# Agenda

- Timeline Italiana e Europea
- Principali progetti NIS2
- Modello di Governance: ruoli e responsabilità
- Modello NIS2 a regime
- Le ultime novità:
  - Gestione incidenti
  - Fornitori rilevanti
  - Categorizzazione
- Framework NIS2
- Domande per ACN

# NIS2 in Italia
## La timeline italiana

L'Agenzia per la Cybersicurezza Nazionale (ACN) è l'autorità nazionale competente per la NIS2, responsabile di garantire la tutela degli interessi nazionali nel campo della cybersicurezza. Inoltre, l'ACN svolge il ruolo di CSIRT nazionale italiano (Computer Security Incident Response Team).

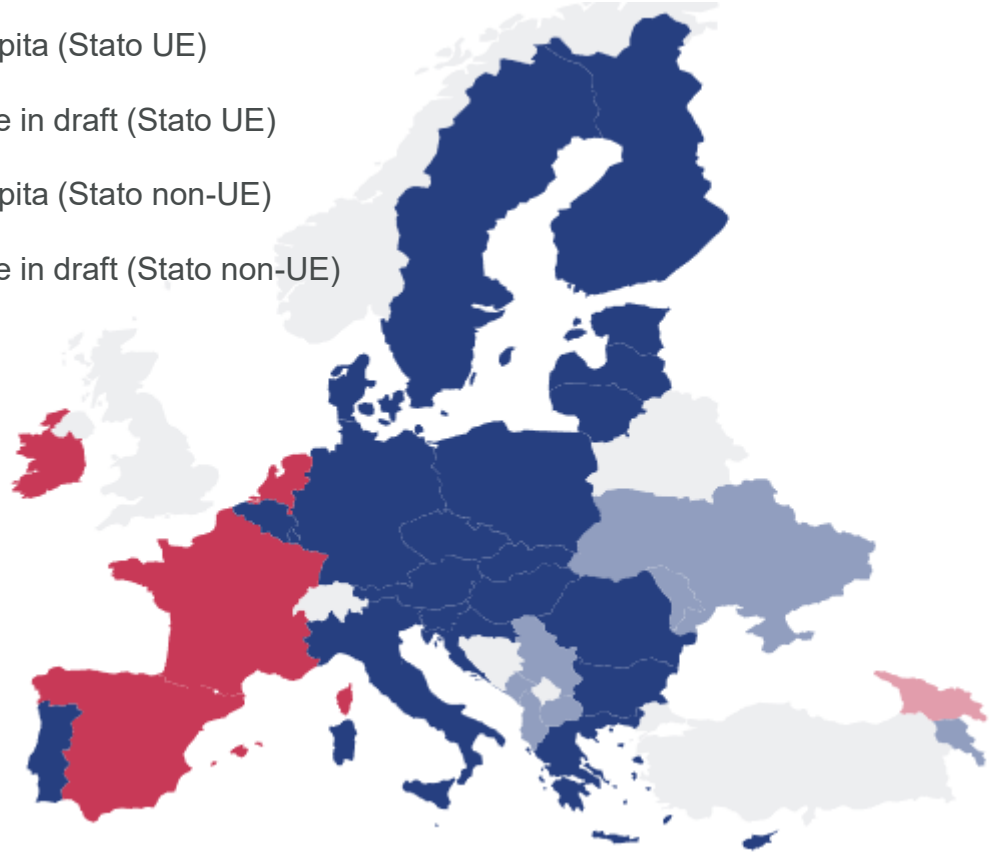



*Scadenza per la conformità alla normativa NIS2 italiana e ai relativi requisiti*

**Annualmente: aggiornamento portale, fornitori critici e categorizzazione, ecc.**

# NIS2 in Europa
# **Recepimento**

- Recepita (Stato UE)
- Legge in draft (Stato UE)
- Recepita (Stato non-UE)
- Legge in draft (Stato non-UE)



https://ecs-org.eu/policy/nis2-directive-transposition-tracker/

## 1 Recepimento già avvenuto

| | | | |
|---|---|---|---|
| 1 | Lettonia | Entrata in vigore: 1 set. 2025 | Compliance: 16 ott. 2025 |
| 2 | Italia | 16 ott. 2024 | Compliance: 16 ott. 2026 |
| 3 | Belgio | 18 ott. 2024 | Compliance: 18 apr. 2027 |
| 4 | Lituania | 18 ott. 2024 | Compliance: apr. 2027 |
| 5 | Grecia | 27 nov. 2024 | Compliance: set. 2026 |
| 6 | Croazia | 30 nov. 2024 | Compliance: nov. 2026 |
| 7 | Romania | 31 dic. 2024 | Compliance: non definita |
| 8 | Slovacchia | 1 gen. 2025 | Compliance: nov. 2027 / a ult. dal 31 dic. 2026 |
| 9 | Ungheria | 1 gen. 2025 | Compliance: a ult del 30 giu. 2026 |
| 10 | Malta | 8 mar. 2025 | Compliance: 23 gen. 2026 |
| 11 | Finlandia | 8 apr. 2025 | Compliance: non definita |
| 12 | Cipro | apr. 2025 | Compliance: non definita |
| 13 | Lussemburgo | 10 mag. 2026 | Compliance: non definita |
| 14 | Slovenia | 10 giu. 2025 | Compliance: seconda metà 2026 |
| 15 | Danimarca | 1 lug. 2025 | Compliance: non definita |
| 16 | Rep. Ceca | 1 nov. 2025 | Compliance: nov. 2026 |
| 17 | Germania | 5 dic. 2025 | Compliance: 2028 |
| 18 | Estonia | 1 gen. 2026 | Compliance: 2029 |
| 19 | Svezia | 15 gen. 2026 | Compliance: non definita |
| 20 | Bulgaria | 17 feb. 2026 | Compliance: nessun grace period definito |
| 21 | Polonia | 3 apr. 2026 | Compliance: apr. 2027 / a ult. apr. 2028 |
| 22 | Portogallo | 3 apr. 2026 | Compliance: non definita |
| 23 | Austria | 10 ott. 2026 | Compliance: 3 set. 2027 |

## 2 Paesi ancora in iter legislativo

| | | |
|---|---|---|
| 1 | Francia | non ancora recepita; disegno di legge in corso; adozione attesa nel 2026 |
| 2 | Olanda | non ancora recepita; Cybersecurity Act in iter parlamentare; entrata in vigore attesa nel 2026 |
| 3 | Spagna | non ancora recepita; draft law approvata dal Consiglio dei Ministri il 14 gen. 2025; iter in corso |
| 4 | Irlanda | non ancora recepita; National Cyber Security Bill 2024 in iter; formulazione ancora pendente |

## Applicazioni extra UE

| | | |
|---|---|---|
| 1 | Svizzera | Swiss Information Security Act |
| 2 | Norvegia | Digitalsikkerhetsloven |
| 3 | Regno Unito | Network and Information Systems Regulations 2018 |

Le scadenze di compliance possono variare in base al tipo di entità, ai settori regolati

(*) Le informazioni sugli obblighi di compliance sono state raccolte da siti governativi; tuttavia, possono esserci differenze in base al tipo di entità o a eventuali fasi intermedie.



forvis mazars

Governance

# Progetti principali in ambito NIS2

## 01

### Governance e Analisi rischi

Strutture, policy e responsabilità.

Analisi dei rischi

## 02

### Gestione dei rischi di terze parti

Valutazione del rischio

Gestione e Monitoraggio delle terze parti


## 03

### Resilienza Operativa e Cybersecurity

BC-DR & Crisis Management


## 04

### Audit e Testing

Verifiche indipendenti e attività di assurance

Governance

# Modello di governance dei gruppi

## *Gruppo / HQ*

**Definizione del Modello**
Definizione del modello NIS2 e policy di gruppo

**Linee Guida e Governance Cyber**
Definizione indirizzi, regolamenti e governance cyber

**Monitoraggio e supporto**
Supervisione dell'implementazione e supporto alle entità locali

**Modello centralizzato**

**Esecuzione locale**

## *Entità Locali*

**Referente NIS2 Locale**
Designato in base alla normativa locale

**Esecuzione**
Implementazione requisiti locali, coordinamento e reporting

**Adattamento**
Allineamento del modello HQ alle normative locali

Governance

# Modello per gestire NIS2 a regime

### Struttura e governance

Strutture di governance e insieme di controlli e processi a supporto della supervisione, della conformità NIS2 e della gestione dei rischi.

### Ruoli e responsabilità

Ruoli e responsabilità chiari e formalizzati, al fine di garantire accountability e adeguata segregazione delle funzioni.

### Framework NIS2

Riferimento metodologico (policy, risk analysis, processi, strumenti di gestione) e implementazioni tecnologiche adottate per l'identificazione, la valutazione e la gestione dei requisiti normativi applicabili.

### Reporting e Flussi Informativi

Meccanismi di reporting e flussi informativi per assicurare una comunicazione tempestiva e completa verso il management e le autorità competenti.

# Governance
## Principali ruoli e responsabilità

**CdA**

### Consiglio di Amministrazione

- Responsabile del modello NIS2
- Approva le politiche strategiche
- Supervisiona l'attuazione e monitora la compliance
- Riceve aggiornamenti dal PdC
- Ricevere training e approvare piano training

**Team NI2**

**PdC**

### Punto di Contatto

- Si occupa della governance dell'interno progetto
- Supporta il CdA nel controllo dei rischi operativi
- Si occupa degli aggiornamenti NIS2
- Gestisce gli incidenti assieme al referente CSIRT

### Compliance

- Monitoraggio conformità e requisiti NIS2

### Risk Management

- Valutazione rischi ICT/OT, metodologie e monitoraggio

### Legal / Procurement

- Conformità normativa e contrattuale

### Internal Audit / Auditor Esterni

- Verifica indipendente sull'efficacia del modello NIS2

# Gestione degli incidenti significativi

## Definizione, timeline e notifica degli incidenti

**Cos'è un 'incidente significativo':**

- Gravi attacchi informatici che colpiscono i servizi essenziali
- Compromessa di dati sensibili o infrastrutture critiche

**Categorie di Incidenti Significativi secondo ACN**

**IS-1 PERDITA DI CONFIDENZIALITA'**
Divulgazione non autorizzata di dati al di fuori dell'organizzazione

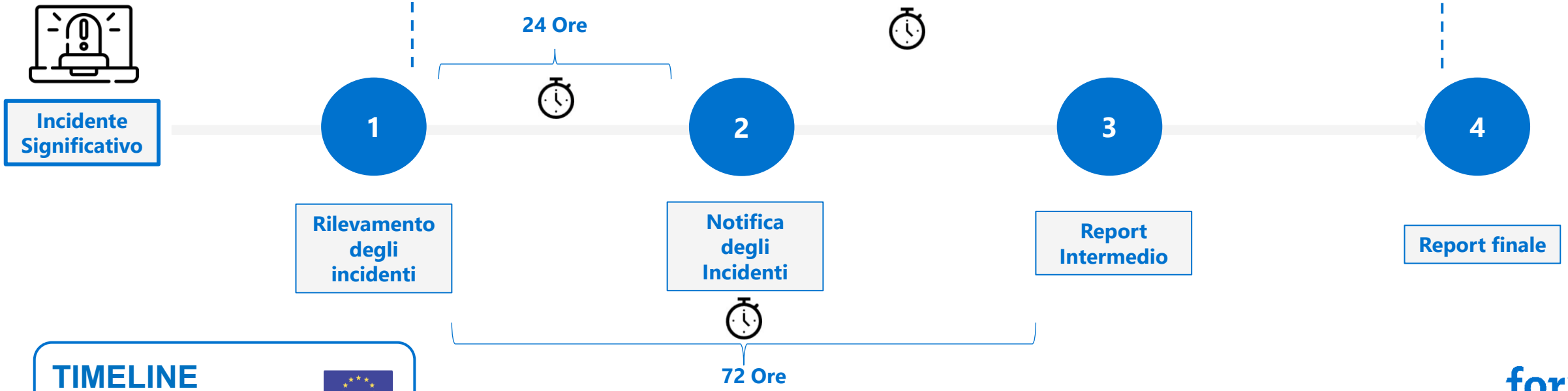
**IS-2 PERDITA DI INTEGRITA'**
Alterazione non autorizzata dei dati con impatto esterno

**IS-3 VIOLAZIONE DEI LIVELLO DI SERVIZIO**
Mancato rispetto dei livelli di servizio definiti, a causa di un incidente informatico

**IS-4 ACCESSO NON AUTORIZZATO/ ABUSO DEI PRIVILEGI**
Accesso non autorizzato
Abuso dei diritti di accesso legittimi

Solo per entità essenziali

**Solo incidenti di cybersecurity significativi richiedono la notifica obbligatoria all'ACN in conformità con i requisiti NIS2**




**TIMELINE DIRETTIVA NIS2**

# Determine ACN

# Fornitori rilevanti - Determina ACN N. 127437/2026

## Fornitori rilevanti

I soggetti NIS sono tenuti a censire, tramite il servizio "Aggiornamento annuale informazioni" sulla Piattaforma ACN, tutti i fornitori qualificabili come rilevanti secondo i criteri definiti dalla normativa.

**Scadenza obbligatoria**

***Entro il 31 maggio 2026, i soggetti NIS dovevano aggiornare sulla Piattaforma ACN l'elenco completo dei fornitori rilevanti.***

**Cosa cambia**

La determina aggiorna le modalità di utilizzo e accesso alla piattaforma ACN.

**Nuovo obbligo**

Viene introdotta l'elencazione dei fornitori rilevanti da comunicare tramite piattaforma.

**Chi è coinvolto**

Tutti i soggetti NIS che effettuano l'aggiornamento annuale delle informazioni.

| Paese | Codice fiscale/Codice IPA | Ragione sociale | CPV | Note | Criterio di rilevanza |
|---|---|---|---|---|---|
| IT | | | 09310000-5 | Utenze energia | Fornitura non fungibile |
| IT | | | 72212730-5 | Provider IT: servizi di data center, cloud hosting,..... | Fornitura ICT non fungibile |
| IT | | | 32500000-8 | Fornitura di hardware di rete ad alte prestazioni..... | Fornitura ICT |

# Determine ACN
# Categorizzazione - Determina ACN N. 127437/2026

## Categorizzazione delle attività e dei servizi

Tale determina contiene:

1. Modello di categorizzazione (10 macro-aree);
2. Descrizione del servizio/attività;
3. Categorie di rilevanza (4 livelli: alto, medio, basso, minimo);
4. Analisi di rilevanza (BIA o simile analisi);
5. Giustificare in caso di riduzione della rilevanza.

| Macro-area | Denominazione Attività/Servizio | Descrizione | Categoria di rilevanza pre-assegnata | Categoria di rilevanza attribuita |
|---|---|---|---|---|
| Monitoraggio e controllo | **Sicurezza, monitoraggio e controllo IT: SOC/SIEM, alert, incident resp** | Il macro-processo "Sicurezza, monitoraggio e controllo IT" accorpa l'attività "Monitoraggio cybersecurity e gestione incidenti" e comprende le attività operative, organizzative e di controllo relative a: SOC/SIEM, alert, incident response, | *Impatto alto* | Impatto alto |
| Produzione di beni e servizi - Produzione, trasformazione e distribuzione di alimenti | | | *Impatto medio* | Impatto medio |
| Ricerca, sviluppo e progettazione | | | *Impatto medio* | Impatto alto |
| Gestione finanziaria | | | *Impatto basso* | Impatto alto |
| Gestione amministrativa | | | *Impatto minimo* | Impatto alto |

**Obbligo dal:**
**1° maggio 2026**

**Scadenza annuale:**
**1 Maggio – 30 Giugno**

**Prima applicazione:**
**Anno 2026**

**1 maggio 2026** — **Apertura finestra**

**31 maggio 2026** — **Scadenza fornitori**

**30 giugno 2026** — **Scadenza categorizzazione**

**Annuale** — **Rinnovo ogni anno**

# Governance
## Framework NIS2

# Governance
# **Framework NIS2**

| Framework NIS2 | Principali contenuti |
|---|---|
| Organizzazione per Information Security | • Definizione di ruoli e responsabilità<br>• Struttura organizzativa e governance della sicurezza<br>• Meccanismi di reporting verso il top management |
| IT Security Policy | • Definizione della normativa di sicurezza (*)<br>• Processi di gestione della sicurezza |
| Risk Assessment & Risk treatment Plan | • Metodologia di valutazione del rischio (asset, impatti, …)<br>• Identificazione e prioritizzazione dei rischi ICT<br>• Piano di trattamento con azioni, responsabilità e tempistiche |
| Vulnerability Plan | • Programma di VA (scansioni periodiche)<br>• Prioritizzazione in base al rischio<br>• Integrazione con patch management<br>• Attività avanzate (penetration test, red teaming) |

(*) GV.PO-01
a) gestione del rischio;
b) ruoli e responsabilità;
c) affidabilità delle risorse umane;
d) conformità e audit di sicurezza;
e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;
f) gestione degli asset;
g) gestione delle vulnerabilità;
h) continuità operativa, ripristino in caso di disastro e gestione delle crisi informatiche;
i) gestione dell'autenticazione, delle identità digitali e del controllo accessi;
j) sicurezza fisica;
k) formazione del personale e consapevolezza;
l) sicurezza dei dati;
m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
n) protezione delle reti e delle comunicazioni;
o) monitoraggio degli eventi di sicurezza;
p) risposta agli incidenti e ripristino.

# Governance
# **Framework NIS2**

| Framework NIS2 | Principali contenuti |
|---|---|
| Training | • Programma di formazione continua sulla sicurezza<br>• Awareness su phishing, social engineering e cyber threats<br>• Formazione specifica per ruoli critici |
| Business Continuity<br>Disaster Recovery Plan<br>Crisis Management | • Piani di business continuity e disaster recovery<br>• Definizione di scenari e impatti su servizi critici<br>• Test periodici (es. tabletop, simulation exercises)<br>• Piano di gestione delle crisi cyber |
| IT Security Incident | • Processo di gestione degli incidenti di sicurezza<br>• Capacità di detection, response e recovery<br>• Procedure di escalation e comunicazione (ACN)<br>• Monitoraggio e reporting degli incidenti |
| Adjustment Plan | • Piano di miglioramento continuo<br>• Azioni derivanti da audit, assessment e incidenti<br>• Monitoraggio dello stato di avanzamento delle remediation |

# Domande per ACN

**Budget e spesa**

- Secondo le indicazioni della Guida per i Dirigenti PMI della ACN il dirigente deve impegnarsi affinché si "pianifichino, attraverso l'allocazione di budget e risorse, l'acquisto di servizi e infrastrutture, e promuovano corsi di formazione o altre iniziative di sensibilizzazione volte al potenziamento di una cultura della cybersicurezza. " Si può considerare questa attività essenziale affinché venga quindi introdotta nel contratto Dirigenti Industriali per renderla pienamente operativa nella governance anche dei rapporti lavorativi?

**Ruoli e responsabilità**

- Quali sono le evidenze concrete che dimostrano che un CDA sta realmente governando il rischio cyber e non lo sta solo delegando all'IT o al CISO?
- Che tipo di reporting dovrebbe ricevere periodicamente il CDA per poter esercitare davvero il proprio ruolo di supervisione sul rischio cyber?
- La formazione degli organi di amministrazione dovrebbe essere prevalentemente normativa, tecnica, di scenario oppure basata su simulazioni di crisi cyber?
- Il CDA deve approvare formalmente le misure di cybersecurity?
- Quali responsabilità personali hanno amministratori e dirigenti?
- Con quale frequenza il CDA deve ricevere aggiornamenti sul rischio cyber?
- Dobbiamo istituire un comitato cyber o un processo di reporting periodico?

**Perimetro**

- Se siamo fornitori di un soggetto NIS2, diventiamo automaticamente soggetti NIS2 anche noi?
- Le holding rientrano nella NIS2?
- Una SPV può rientrare nella NIS2 anche se ha pochi dipendenti?

**Temi generali**

- Qual è l'errore più frequente che ACN vede, o teme di vedere, nell'implementazione della NIS2 da parte delle aziende italiane?



forvis mazars

# Contact


## Forvis Mazars

**Luca Savoia**
**Partner**
Forvis Mazars in Italy
Tel: +39 02 32169300
Mobile: +39 348 82 17 339
Email: luca.savoia@forvismazars.com


# Follow us

**LinkedIn**: Forvis Mazars Group

**X**: ForvisMazarsInItalia

**Facebook**: @ForvisMazarsInItalia

**Instagram**: @ForvisMazarsInItalia

**Find out more**: www.forvismazars.com/it