

Direttiva NIS2: la scadenza si avvicina...

NIS2

Cosa è richiesto

Cesare Gallotti

- NIS 2 (Direttiva UE 2022/2055) è entrata in vigore il 17 gennaio 2023.
- NIS2 dovrà essere recepita dall'Italia entro l'ottobre 2024.
- Rispetto alla NIS:
 - Aumentano i soggetti.
 - E' richiesta un'analisi dei rischi.
 - Le misure di sicurezza dovranno essere adeguate al contesto, considerando quindi anche la capacità di spesa.

- L'applicabilità dipende da settore e dimensione. La NIS2 è applicabile a:
 - soggetti essenziali (essential entities);
 - soggetti importanti (important entities).
- La differenza pratica riguarda i controlli e le sanzioni.
- Ulteriori soggetti potrebbero essere aggiunti dalla normativa nazionale.
- Le entità dovranno riconoscersi come soggetti a cui è applicabile la NIS 2, non è più l'autorità che le designa come tali. Le entità si dovranno registrare secondo regole che saranno fornite.
- Entro il 17 aprile 2025, gli Stati membri definiscono un elenco dei soggetti.

Soggetti a cui si applica la NIS2 – Uno schema

		NIS-2 Scope – Final version				
Article	Subjects	Activities	Entity criteria (ENI)	Large of least 250 employees OR with an annual turnover of at least 50 million euros (or an annual balance sheet total of at least 43 million euros)	Medium entities of least 50 employees OR with an annual turnover (or balance sheet total) of at least 10 million euros	Small & Micro
Article 2: Entities of their activity						
1. Energy	Electricity, district heating, bioenergy, gas, hydrogens, oil	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important by national authorities (or its role, service, significant impact, essential to society)
2. Transport	Sea (passenger), aviation, railway, rail (freight and passenger), Water (passenger, cargo), ports, traffic control, Road (ITS & charging stations)					
3. Banking	Credit institutions (attention: DOXA licenciate)					
4. Financial Market Infrastructure	Trading venues, central counterparties (attention: DOXA licenciate)					
5. Health	Essential providers: EU reference laboratories, RAI of medicinal products, manufacturers of active substances and generic medicines, manufacturers of medical devices, critical drug suppliers, health care givers Special case: entities holding a distribution authorisation for medicinal products, only if identified as CRI					
6. Drinking Water						
7. Waste Water	(only if it is an essential part of their essential activities)					
Article 3: Digital infrastructure						
8. Digital infrastructure	Essential service providers	The Member State(s) where it is established	Essential	Essential	Essential	
	EU service providers (including root name central)					
	EU service providers					
	Providers of public electronic communication networks					
	Non-qualified cloud service providers					
9. Digital infrastructure	Internet Exchange Point providers Cloud computing service providers Data centre service providers Content delivery network providers	The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important	
10. Digital infrastructure	Managed Service Providers, Managed Security Service Providers					
11. ITI-service management (IS2)						
12. Public Administration entities	EU central governments (including judicial, parliamentary, central banks, offices, national or public security), EU national governments (not listed), (Special for Member States of local governments)	EU that established them	Essential	Essential	Essential	
13. Space	Operators of ground based infrastructure (GRI)	The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important	
Article 4: Entities of their services						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State	Important, except if identified as essential or important by national authorities (or its role, service, significant impact, essential to society)	
2. Waste Management	Waste (if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Retail	Production, provision and distribution					
5. Manufacturing	(in which integrated) medical devices, computers, electrical or optical products, critical equipment, machinery, motor vehicles, tractors, tractors, other transport equipment (except E-VE, SE)					
6. Digital providers	Online marketplaces, search engines, social networks					
7. Research	Research organisations (including education institutions) (Special for Member States: research institutions)					
Entities providing domain name registration services						
All items, but only related to Article 1(2) and Article 2(8)						

Da <https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization>

- NIS2 è multirischio: logico, fisico (in precedenza non richiesto), governo, lock in tecnologico, utilities. E considera l’impatto “sociale ed economico” e richiede un “livello appropriato”.
- Gli Orientamenti della Commissione del 13.9.2023 indicano di considerare le seguenti minacce, sempre in una logica di multirischio:
 - sabotaggi,
 - furti,
 - incendi,
 - inondazioni,
 - problemi di telecomunicazione,
 - problemi di interruzioni di corrente,
 - qualsiasi accesso fisico non autorizzato,
 - guasti del sistema,
 - errori umani,
 - azioni malevole, fenomeni naturali.



La Direttiva identifica misure di gestione del rischio:

1. Politiche di analisi dei rischi e della sicurezza
2. Sistemi di gestione degli incidenti
3. Soluzioni di business continuity
4. Misure di sicurezza dell'intera supply chain
5. Sicurezza dell'acquisizione, sviluppo e manutenzione dei sistemi e delle reti informatiche, compresa la gestione e la divulgazione delle vulnerabilità
6. Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersecurity
7. Pratiche di igiene informatica basilari e formazione in materia di sicurezza informatica
8. Uso della crittografia
9. Sicurezza delle risorse umane e politiche di controllo degli accessi (log management) e gestione degli asset
10. Uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti all'interno dell'entità, ove opportuno.

Entro il 17 ottobre 2024, la Commissione adotta atti di esecuzione che stabiliscono i requisiti tecnici e metodologici delle misure per quanto riguarda i fornitori di:

- servizi DNS,
- registri dei nomi di dominio di primo livello (TLD),
- servizi di cloud computing,
- servizi di data center,
- reti di distribuzione dei contenuti,
- servizi gestiti,
- servizi di sicurezza gestiti,
- mercati online,
- motori di ricerca online,
- piattaforme di servizi di social network,
- prestatori di servizi fiduciari.

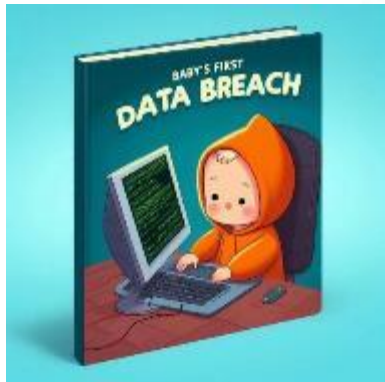


- Si raccomanda di seguire un riferimento «noto» per cominciare ad applicare le misure di sicurezza.
- Riferimento noto a livello internazionale è la ISO/IEC 27001, che fornisce indicazioni per:
 - valutazione del rischio;
 - trattamento del rischio e scelta delle misure di sicurezza;
 - gestione degli incidenti;
 - miglioramento continuo.



- NIS 2 (come NIS 1) prevede l'obbligo di notifica al CSIRT e alle autorità competenti (oltre che ai destinatari stessi del servizio) degli incidenti significativi (se hanno causato o sono in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato o se si sono ripercossi o sono in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli).
- Le comunicazioni al CSIRT dovranno avvenire:
 - Entro 24 ore dalla conoscenza dell'incidente con una notifica di preallarme (per attenuare la potenziale diffusione di incidenti e per consentire di chiedere assistenza).
 - Entro 72 ore dalla conoscenza dell'incidente con aggiornamenti rispetto alle informazioni fornite con il preallarme
 - Entro 1 mese dalla conoscenza dell'incidente con una relazione finale a completamento del processo di segnalazione (questo per poter trarre insegnamenti preziosi dai singoli incidenti).
- Il CSIRT, con il NIS 2, ha maggiori responsabilità di coordinamento.

- Alcuni soggetti sono soggetti a più normative e quindi a diverse modalità di notificazione degli incidenti.
- Obbligatorietà:
 - Articolo 23, stabilisce quando è obbligatorio notificare;
 - Articolo 30, indica quando la notifica è volontaria (altri incidenti, minacce, quasi incidenti, anche da parte degli altri soggetti).
- Definiti anche i «quasi incidenti». Un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato.
- La NIS2 istituisce la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe).



- La NIS2 prevede ulteriori argomenti:
 - Cooperazione tra Stati membri
 - Sanzioni
 - Punti di contatto nazionali
 - Ruolo dell'ENISA



Grazie dell'attenzione



Salute vita allegria pace buonumore speranza