

NIS2 Directive



**Dalla NIS alla NIS 2:
Motivazioni e contesto legislativo**

Giacomo Bianchi



«**NETWORK AND INFORMATION SYSTEM**»



Segna un passo significativo verso la piena definizione e attuazione della strategia cyber dell'UE



Contribuisce a rafforzare il livello collettivo di sicurezza informatica degli Stati membri dell'UE aumentando i requisiti di applicazione della cybersecurity

Le motivazioni

Primo strumento orizzontale del mercato interno volto a migliorare la resilienza dei sistemi di rete e informazione nell'Unione contro i rischi di cybersicurezza.



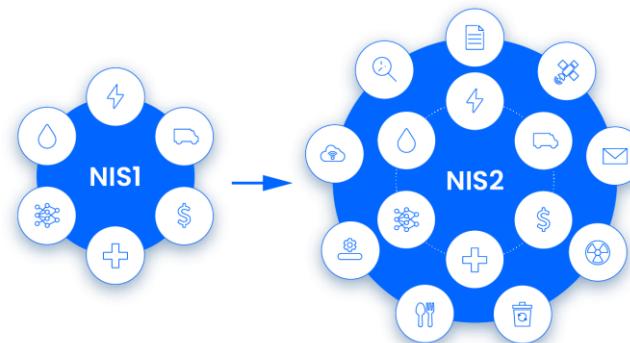
LIMITAZIONI

- a) Livello **insufficiente** di resilienza cibernetica delle imprese che operano nell'UE
- b) Resilienza **incoerente** tra gli Stati membri e i settori
- c) Insufficiente **comprendere** comune delle principali minacce e sfide tra gli Stati membri
- d) Mancanza di una **risposta comune** alle crisi



Insieme rivisto di norme mirate a **rafforzare** il livello di resilienza cibernetica nell'UE

Contesto Legislativo



Presentazione proposta
sulle misure per un
livello comune elevato di
cybersicurezza in tutta
l'UE

16 Dicembre 2020

17 Gennaio 2023

La Direttiva entra in
vigore e viene
pubblicata in Gazzetta
Ufficiale UE

La Direttiva abroga la
Direttiva (UE) 2016/1148
con effetto immediato

18 Ottobre 2024

Gli obiettivi

Articolo 1:
***Raggiungere un
elevato livello
comune di
cybersicurezza in
tutta l'UE***



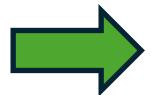
Ampliare il campo di applicazione della direttiva vigente

Obblighi di adozione / rafforzamento di una strategia nazionale per la cybersicurezza

Affrontare la sicurezza delle supply chain

Semplificare gli obblighi di incident reporting (incidenti informatici)

Obblighi di designazione autorità nazionali competenti



AUMENTARE IL LIVELLO DI RESILIENZA INFORMATICA DELLE AZIENDE

RIDURRE LE DISCREPANZE NEL MERCATO INTERNO NEI SETTORI OGGETTO DELLA DIRETTIVA

ACCRESCERE LA CONSAPEVOLEZZA E LA CAPACITÀ DI PREPARARSI E RISONDERE A INCIDENTI O CRISI SU LARGA SCALA

I settori interessati

La NIS2 si applica a qualsiasi azienda che opera nell'UE, compresi *"tutti gli enti pubblici e privati nel mercato interno, che svolgono funzioni importanti per l'economia e la società nel suo insieme"*, che *"sono tenuti ad adottare adeguate misure di sicurezza informatica"*.

La direttiva divide le **"entità interessate"** in due tipologie:

**ENTITÀ ESSENZIALI
(ALTAMENTE CRITICI)**

- Sono soggette a requisiti normativi **più rigorosi** per il monitoraggio della conformità, obblighi di segnalazione degli incidenti e misure di applicazione dei sistemi informativi

**ENTITÀ IMPORTANTI
(CRITICI)**

- Non sono soggette a requisiti normativi **così rigorosi** come quelli previsti per le EE

Entità essenziali (altamente critici)

ENERGIA	INFRASTRUTTURE DIGITALI
TRASPORTI	GESTIONE DEI SERVIZI T/C (BUSINESS-TO-BUSINESS)
SETTORE BANCARIO	PUBBLICA AMMINISTRAZIONE
INFRASTRUTTURE DEI MERCATI FINANZIARI	SPAZIO
SETTORE SANITARIO	ACQUA POTABILE E ACQUE REFLUE

Entità importanti (critici)

SERVIZI POSTALI E DI CORRIERE

**PRODUZIONE, TRASFORMAZIONE E
DISTRIBUZIONE DI ALIMENTI**

GESTIONE DEI RIFIUTI

FABBRICAZIONE

**FABBRICAZIONE, PRODUZIONE E
DISTRIBUZIONE DI SOSTANZE CHIMICHE**

FORNITORI DI SERVIZI DIGITALI

RICERCA

Esclusioni

La Direttiva **NON** si applica ai soggetti che operano nei:

SETTORI DELLA DIFESA

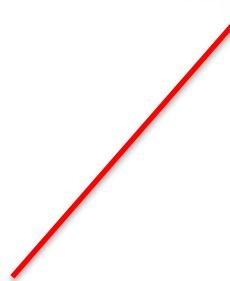
SETTORI DELLA SICUREZZA NAZIONALE

**SETTORI DELLA PUBBLICA SICUREZZA E
ATTIVITÀ DI CONTRASTO**

A chi si applica



ESCLUSIONE



ORGANIZZAZIONI DI MEDIE E GRANDI
DIMENSIONI
(+ 50 dipendenti / 10 mln di fatturato)

ORGANIZZAZIONI RITENUTE DI IMPORTANZA
CRITICA

INTERA CATENA DI APPROVVIGIONAMENTO
DELLA SINGOLA ORGANIZZAZIONE

ORGANIZZAZIONI CON MENO DI 50 DIPENDENTI O CON UN
FATTURATO ANNUO INFERIORE A 10 MILIONI



**MICRO e
PICCOLE
IMPRESE**

**PRESTANO UN SERVIZIO AD UNA MEDIA O
GRANDE ORGANIZZAZIONE**

**SOGGETTO NELLA CATENA DI
APPROVVIGIONAMENTO**

SETTORE ESSENZIALE / CRITICO

ESPLICITAMENTE RICHIESTO

NIS2 Directive



GRAZIE PER L'ATTENZIONE