APPROFONDIMENTO NIS 2

COS'È LA NIS 2

La NIS 2 è la Direttiva 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.

Essendo una Direttiva è necessario che venga recepita all'interno dell'ordinamento italiano.

Il termine per il recepimento nazionale della Direttiva NIS 2 è stato fissato al **17 ottobre 2024**.

A CHI SI APPLICA

SOGGETTI ELENCATI NEGLI ALLEGATI I (ALTA CRITICITÀ) E II (ALTRI SETTORI CRITICI) CHE SONO CONSIDERATI MEDIE IMPRESE (numero di dipendenti compreso fra 50 e 250 o un fatturato annuo o un totale di bilancio compreso fra 10 e 50 milioni di euro o con un totale di bilancio annuo non superiore a 43 milioni di euro,)

SOGGETTI DELLE TIPOLOGIE DI CUI ALL'ALLEGATO I O II INDIPENDENTEMENTE DALLE LORO DIMENSIONI QUALORA

a) i servizi siano forniti da:
   - i) fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico;
   - ii) prestatori di servizi fiduciari qualificati
   - iii) registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;

b) il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;

c) La Direttiva si applica anche nel caso in cui una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;

d) La Direttiva si applica anche nel caso in cui una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;

e) il soggetto sia critico in ragione della sua particolare importanza a livello nazionale regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;

f) il soggetto è un ente della pubblica amministrazione:

SOGGETTE ESSENZIALI

a) soggetti di cui all'allegato I che superano i massimali per le medie imprese
b) prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché prestatori di servizi DNS, indipendentemente dalle loro dimensioni; Nota: «servizio fiduciario», un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: 1) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure 2) creazione, verifica e convalida di certificati di autenticazione di siti web; o 3) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi;
c) fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese
d) soggetti della pubblica amministrazione
e) qualsiasi altro soggetto di cui all'allegato I o II che uno Stato membro identifica come soggetti essenziali
f) soggetti ti, indipendentemente dalle loro dimensioni, identificati come soggetti critici dalla Direttiva 2022/2557 https://eur-lex.europa.eu/legal content/IT/TXT/PDF/?uri=CELEX:32022L2557&from=EN

ALLEGATO I: SETTORI AD ALTA CRITICITÀ:

Energia

Settore	Sottosettore	Tipo di soggetto
1. Energia	a) Energia elettrica	— Impresa elettrica quale definita all'articolo 2, punto 57), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio (1) che esercita attività di «fornitura» quale definita all'articolo 2, punto 12), di tale direttiva
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 29), della direttiva (UE) 2019/944
		— Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 35), della direttiva (UE) 2019/944
		— Produttori quali definiti all'articolo 2, punto 38), della direttiva (UE) 2019/944
		— Gestori del mercato elettrico designato quali definiti all'articolo 2, punto 8), del regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio (2) — Partecipanti al mercato dell'energia elettrica quali definiti all'articolo 2, punto 25), del regolamento (UE) 2019/943 che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia quali definiti all'articolo 2, punti 18), 20) e 59) della direttiva (UE) 2019/944 — Gestori di un punto di ricarica responsabili della gestione e del funzionamento di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità
	b) Teleriscaldamento e teleraffrescamento	— Gestori di teleriscaldamento o teleraffrescamento quali definiti all'articolo 2, punto 19), della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio (3)
	c) Petrolio	— Gestori di oleodotti
		— Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
		— Organismi centrali di stoccaggio quali definiti all'articolo 2, lettera f), della direttiva 2009/119/CE del Consiglio (4)
	d) Gas	— Imprese fornitrici quali definite all'articolo 2, punto 8), della direttiva 2009/73/CE del Parlamento europeo e del Consiglio (5)
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 6), della direttiva 2009/73/CE
		— Gestori del sistema di trasporto quali definiti all'articolo 2, punto 4), della direttiva 2009/73/CE
		— Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, punto 10), della direttiva 2009/73/CE
		— Gestori del sistema GNL quali definiti all'articolo 2, punto 12), della direttiva 2009/73/CE
		— Imprese di gas naturale quali definite all'articolo 2, punto 1), della direttiva 2009/73/CE;
		— Gestori di impianti di raffinazione e trattamento di gas naturale
	e) Idrogeno	— Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno

Trasporti

Settore	Sottosettore	Tipo di soggetto
2. Trasporti	a) Trasporto aereo	— Vettori aerei quali definiti all'articolo 3, punto 4), del regolamento (CE) n. 300/2008 utilizzati a fini commerciali
		— Gestori aeroportuali quali definiti all'articolo 2, punto 2), della direttiva 2009/12/CE del Parlamento europeo e del Consiglio ([6]), aeroporti quali definiti all'articolo 2, punto 1), di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio ([7]), e soggetti che gestiscono impianti annessi situati in aeroporti
		— Operatori attivi nel controllo della gestione del traffico che forniscono un servizio di controllo del traffico aereo quali definiti all'articolo 2, punto 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio ([8])
	b) Trasporto ferroviario	— Gestori dell'infrastruttura quali definiti all'articolo 3, punto 2), della direttiva 2012/34/UE del Parlamento europeo e del Consiglio ([9])
		— Imprese ferroviarie quali definiti all'articolo 3, punto 1), della direttiva 2012/34/UE, compresi gli operatori degli impianti di servizio quali definiti all'articolo 3, punto 12), di tale direttiva
	c) Trasporto per vie d'acqua	— Compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite per il trasporto marittimo all'allegato I del regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio ([10]), escluse le singole navi gestite da tale compagnia
		— Organi di gestione dei porti quali definiti all'articolo 3, punto 1), della direttiva 2005/65/CE del Parlamento europeo e del Consiglio ([11]), compresi i relativi impianti portuali quali definiti all'articolo 2, punto 11), del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti
		— Gestori di servizi di assistenza al traffico marittimo (VTS) quali definiti all'articolo 3, lettera o), della direttiva 2002/59/CE del Parlamento europeo e del Consiglio ([12])
	d) Trasporto su strada	— Autorità stradali quali definite all'articolo 2, punto 12), del regolamento delegato (UE) 2015/962 della Commissione ([13]) responsabili del controllo della gestione del traffico, esclusi i soggetti pubblici per i quali la gestione del traffico o la gestione di sistemi di trasporto intelligenti costituiscono soltanto una parte non essenziale della loro attività generale
		— Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 4, punto 1), della direttiva 2010/40/UE del Parlamento europeo e del Consiglio ([14])

Settore Bancario

3. Settore bancario		Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio ([15])

Infrastrutture dei Mercati Finanziari

4. Infrastrutture dei mercati finanziari		— Gestori delle sedi di negoziazione quali definiti all'articolo 4, punto 24), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio ([16])
		— Controparti centrali (CCP) quali definite all'articolo 2, punto 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio ([17])

Settore Sanitario

Settore	Sottosettore	Tipo di soggetto
5. Settore sanitario		— Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio ([18])
		— Laboratori di riferimento dell'UE quali definiti all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio ([19])
		— Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio ([20]) — Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2 — Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio ([21])

Acqua Potabile

6. Acqua potabile		Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1, lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio ([22]), ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni

Acque Reflue

7. Acque reflue		Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali quali definite all'articolo 2, punti da 1), 2) e 3), della direttiva 91/271/CEE del Consiglio ([23]), escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale

Infrastrutture Digitali

8.	Infrastrutture digitali		— Fornitori di punti di interscambio internet
			— Fornitori di servizi DNS, esclusi gli operatori dei server dei nomi radice
			— Registri dei nomi di dominio di primo livello (TLD)
			— Fornitori di servizi di cloud computing
			— Fornitori di servizi di data center
			— Fornitori di reti di distribuzione dei contenuti (content delivery network)
			— Fornitori di servizi fiduciari
			— Fornitori di reti pubbliche di comunicazione
			— Fornitori di servizi di comunicazione elettronica accessibili al pubblico

Gestione Dei Servizi TIC (tecnologie dell'informazione e della comunicazione) (Business To Business)

9.	Gestione dei servizi TIC (business-to-business)		— Fornitori di servizi gestiti — Fornitori di servizi di sicurezza gestiti

Pubblica Amministrazione

Settore		Sottosettore	Tipo di soggetto
10.	Pubblica amministrazione		— Enti della pubblica amministrazione delle amministrazioni centrali quali definiti da uno Stato membro conformemente al diritto nazionale
			— Enti della pubblica amministrazione a livello regionale quali definiti da uno Stato membro conformemente al diritto nazionale

Spazio

11.	Spazio		Operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica

ALLEGATO II: ALTRI SETTORI CRITICI

Settore	Sottosettore	Tipo di soggetto
1. Servizi postali e di corriere		Fornitori di servizi postali quali definiti all'articolo 2, punto 1 *bis*), della direttiva 97/67/CE, tra cui i fornitori di servizi di corriere
2. Gestione dei rifiuti		Imprese che si occupano della gestione dei rifiuti quali definite all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio (1), escluse quelle per cui la gestione dei rifiuti non è la principale attività economica
3. Fabbricazione, produzione e distribuzione di sostanze chimiche		Imprese che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele di cui all'articolo 3, punti 9) e 14), del regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio (2) e imprese che si occupano della produzione di articoli quali definite all'articolo 3, punto 3), del medesimo regolamento, da sostanze o miscele
4. Produzione, trasformazione e distribuzione di alimenti		Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio (3) che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione
5. Fabbricazione	a) Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro	Soggetti che fabbricano dispositivi medici quali definiti all'articolo 2, punto 1), del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio (4) e soggetti che fabbricano dispositivi medico-diagnostici in vitro quali definiti all'articolo 2, punto 2), del regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio (5) ad eccezione dei soggetti che fabbricano dispositivi medici di cui all'allegato I, punto 5), quinto trattino, della presente direttiva
	b) Fabbricazione di computer e prodotti di elettronica e ottica	Imprese che svolgono attività economiche di cui alla sezione C, divisione 26, della NACE Rev. 2
	c) Fabbricazione di apparecchiature elettriche	Imprese che svolgono attività economiche di cui alla sezione C, divisione 27, della NACE Rev. 2
	d) Fabbricazione di macchinari e apparecchiature n.c.a.	Imprese che svolgono attività economiche di cui alla sezione C, divisione 28, della NACE Rev. 2
	e) Fabbricazione di autoveicoli, rimorchi e semirimorchi	Imprese che svolgono attività economiche di cui alla sezione C, divisione 29, della NACE Rev. 2
	f) Fabbricazione di altri mezzi di trasporto	Imprese che svolgono attività economiche di cui alla sezione C, divisione 30, della NACE Rev. 2

Settore	Sottosettore	Tipo di soggetto
6. Fornitori di servizi digitali		— Fornitori di mercati online
		— Fornitori di motori di ricerca online
		— Fornitori di piattaforme di servizi di social network
7. Ricerca		Organizzazioni di ricerca

«mercato online»: un servizio che utilizza un software, compresi siti web, parte di siti web o un'applicazione, gestito da o per conto del professionista, che permette ai consumatori di concludere contratti a distanza con altri professionisti o consumatori.

SOGGETTI IMPORTANTI

Entro il 17 aprile 2025, gli Stati membri definiscono un elenco dei soggetti essenziali ed importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio.

I soggetti importanti sono:

- il soggetto è l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
- una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;
- una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;
- il soggetto sia critico in ragione della sua particolare importanza a livello nazionale regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro.

OBBLIGHI PREVISTI DALLA NIS2

GOVERNANCE

Gli organi di gestione dei soggetti essenziali e importanti devono:

- **approvare le misure di gestione dei rischi di cibersicurezza** (vedi anche punto successivo).

Si riporta anche quanto indicato nel Considerando 89:

(89) I soggetti essenziali e importanti dovrebbero adottare un'ampia gamma di pratiche di igiene informatica di base quali

- principi zero trust,
- aggiornamenti del software,
- configurazione dei dispositivi,
- segmentazione della rete,
- gestione dell'identità e dell'accesso o sensibilizzazione degli utenti,
- organizzare per il loro personale una formazione e sensibilizzarlo alle minacce informatiche, al phishing o alle tecniche di ingegneria sociale.

Inoltre, tali soggetti dovrebbero valutare le loro capacità di cibersicurezza e, se del caso, perseguire l'integrazione di tecnologie per il rafforzamento della cibersicurezza quali l'intelligenza artificiale o i sistemi di apprendimento automatico, per migliorare le loro capacità e la sicurezza dei sistemi informatici e di rete.

- **Partecipare alla formazione**
- **Offrire periodicamente analoga formazione ai loro dipendenti** per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto.

OBBLIGO DI SEGNALAZIONE DEGLI INCIDENTI

Ciascuno Stato membro provvede affinché i soggetti essenziali e importanti notifichino senza indebito ritardo al proprio CSIRT (**COMPUTER SECURITY INCIDENT RESPONSE TEAM_Per l'Italia è l'Agenzia per la cybersicurezza nazionale (ACN))** o, se opportuno, alla propria autorità competente, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi (incidente significativo).

Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Tempistiche della notifica

Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente:

a) **senza indebito ritardo, e comunque entro 24 ore** da quando sono venuti a conoscenza dell'incidente significativo, un preallarme che, se opportuno, indichi se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

b) **senza indebito ritardo, e comunque entro 72 ore** da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, se opportuno, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

c) **su richiesta di un CSIRT** o, se opportuno, di un'autorità competente, **una relazione intermedia** sui pertinenti aggiornamenti della situazione;

d) **una relazione finale entro un mese dalla trasmissione della notifica** dell'incidente di cui alla lettera b), che comprenda:

i) una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;

ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;

iii) le misure di attenuazione adottate e in corso;

iv) se opportuno, l'impatto transfrontaliero dell'incidente

SANZIONI

- **Soggetti Essenziali**: sanzioni pecuniarie amministrative pari a un massimo di 10 Milioni di euro o il 2% del totale del fatturato mondiale globale.
- **Soggetti Importanti**: sanzioni pecuniarie amministrative massimo di 7 Milioni di euro o a fino ad un massimo del 1,4 % del totale del fatturato mondiale globale.