NEWSLETTER

NUOVE NORME DI SICUREZZA INFORMATICA: NIS 2 E D.LGS. 138/2024

DATA: 18 OTTOBRE 2024

INTRODUZIONE

La Direttiva NIS 2 (Network and Information Security) è una DIRETTIVA EUROPEA 2022/2555 che rafforza le misure di sicurezza informatica per proteggere le infrastrutture critiche dell'Unione Europea. In Italia, è stata recepita tramite il Decreto Legislativo 138/2024, che stabilisce nuovi obblighi e misure di sicurezza per le aziende e gli enti pubblici, abrogando la precedente Direttiva UE 2016/1148 (c.d. NIS 1).

PUNTI CHIAVE DELLA DIRETTIVA NIS 2

• Allargamento della platea di soggetti obbligati: Inclusione di settori come sanità, energia, trasporti, telecomunicazioni, servizi digitali, banche, infrastrutture finanziarie, acqua potabile, rifiuti, aziende chimiche, etc.
• Standard di sicurezza più elevati: Adozione di misure avanzate di sicurezza per garantire la resilienza dei sistemi informatici.
• Obblighi di segnalazione incidenti: Comunicazione di incidenti informatici entro 24 ore.
• Controlli e sanzioni: Introduzione di multe severe e controlli periodici.

RECEPIMENTO IN ITALIA: DECRETO LEGISLATIVO 138/2024

Il D.Lgs. 138/2024 stabilisce come la NIS 2 sarà applicata in Italia, con disposizioni specifiche come:
• Obblighi per le aziende italiane: Implementazione di piani di gestione del rischio e formazione sulla sicurezza digitale.
• Sorveglianza e audit: Ruolo rafforzato dell'Agenzia per la Cybersicurezza Nazionale (ACN).
• Multe e sanzioni: Sanzioni fino a 10 milioni di euro o il 2% del fatturato globale annuo.

NEWSLETTER OTTOBRE 2024

CHI DEVE ADEGUARSI?

La NIS 2 e il D.Lgs. 138/2024 coinvolgono una vasta gamma di organizzazioni tra cui:

- Aziende e enti del settore pubblico e privato con infrastrutture essenziali per la società e l'economia.
- Imprese che forniscono servizi di **telecomunicazioni, energia, acqua, trasporti, finanza, sanità , gestione rifiuti, aziende chimiche, etc.**
- Fornitori di servizi digitali, come piattaforme di e-commerce, motori di ricerca e servizi cloud.
- **Piccole e medie imprese (PMI)** che operano in settori critici specificati dalla normativa.

Ambito di applicazione (articoli 3 e 6, allegati I-IV)

[1] Possibile identificazione governativa come essenziali
[2] Possibile identificazione governativa come importanti o essenziali

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia (+)	19 tipologie di soggetto	Essenziali	Importanti[1]	Fuori ambito[2]
Trasporti	10 tipologie di soggetto			
Settore bancario Infrastrutture dei mercati finanziari	DORA Lex specialis			
Settore sanitario (+)	5 tipologie di soggetto			
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali (+)	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto			
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto			
Gestione dei rifiuti	1 tipologia di soggetto			
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto			
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto			
Fabbricazione (Sottosettori)+sottosettore sentito MIT	6 tipologie di soggetto			
Fornitori di servizi digitali (+)	4 tipologie di soggetto			
Ricerca	2 tipologie di soggetto			
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale		Identificazione governativa		
Pubblica Amministrazione regionale e locale	11 categorie di PA			
Ulteriori tipologie di soggetti	4 tipologie e 2 criteri aggiuntivi			

Settori, sottosettori e tipologie di soggetti introdotti dalla NIS2

ESEMPIO:

Ministero delle Imprese e del Made in Italy

L'Autorità di Settore del MIMIT
Fabbricazione, produzione e distribuzione di sostanze chimiche

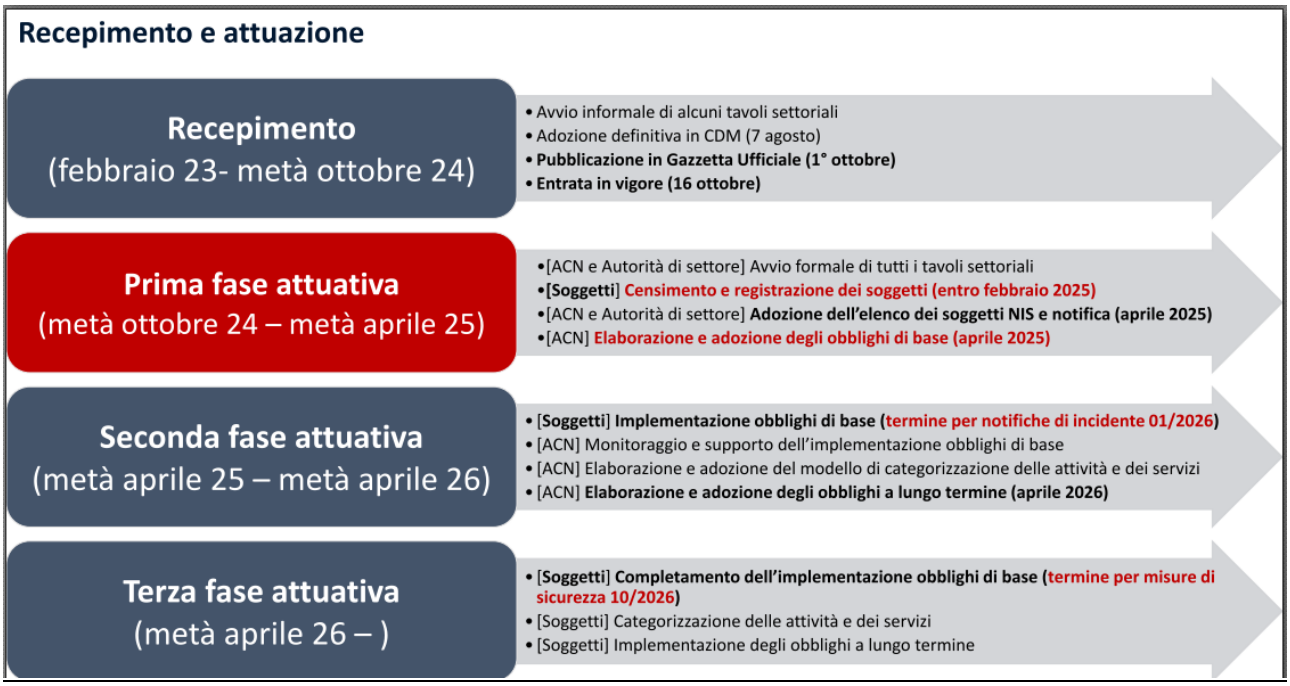
«Imprese che si occupano della **fabbricazione** di sostanze e della **distribuzione** di sostanze o miscele di cui all'articolo 3, punti 9) e 14), del regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio e imprese che si occupano della **produzione** di articoli quali definite all'articolo 3, punto 3), del medesimo regolamento, da sostanze o miscele»

Medie e Grandi (>10M€ / 50 dipendenti): Importanti

Numerosità prevista: >500

TEMPISTICHE DI ENTRATA IN VIGORE

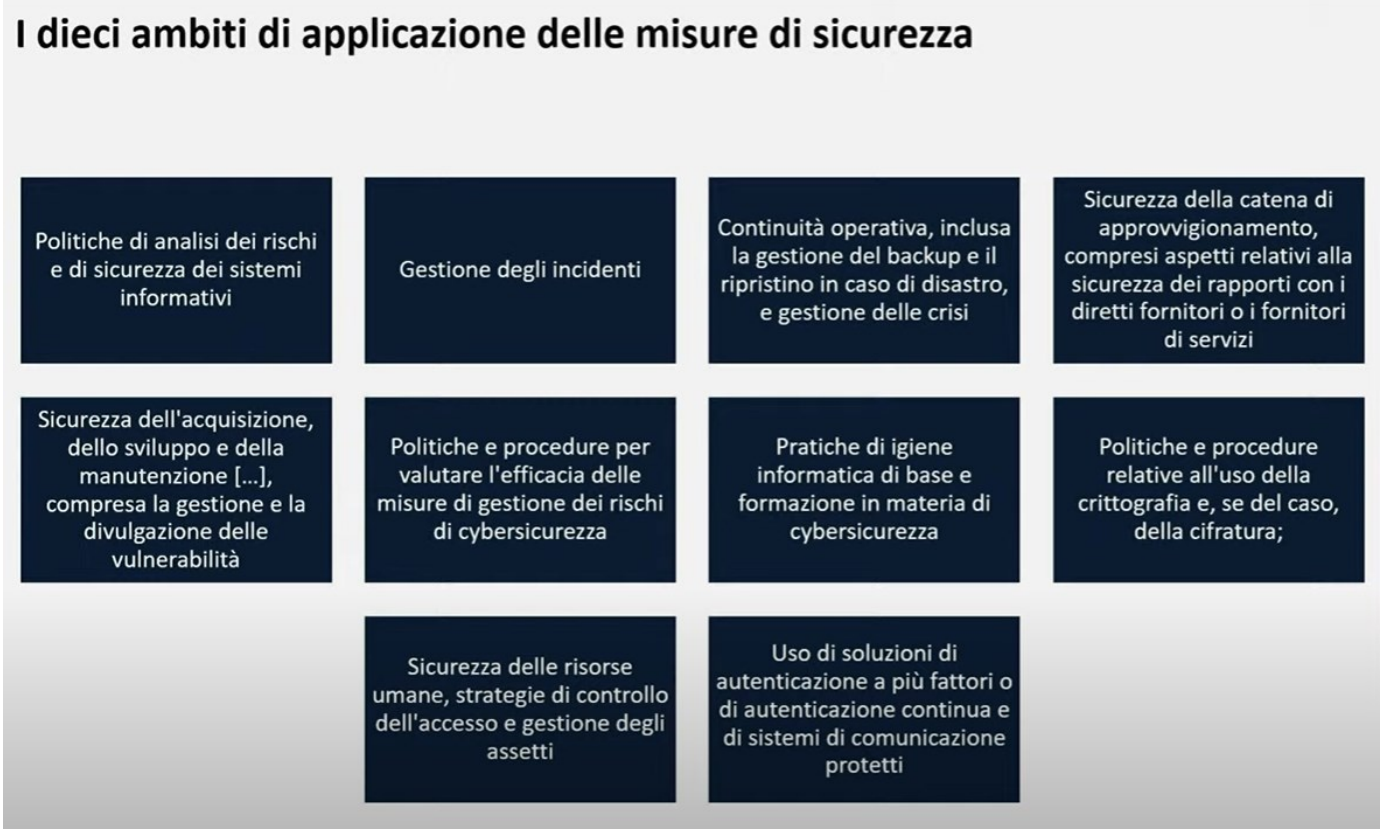
Le aziende devono adeguarsi entro **18 mesi dall'entrata in vigore** della direttiva europea, prevista per ottobre 2024. Le nuove misure saranno obbligatorie da aprile 2026. Si raccomanda di iniziare l'adeguamento quanto prima per evitare ritardi e sanzioni.



IMPLICAZIONI PER LE AZIENDE

Le imprese italiane devono agire rapidamente per allinearsi alle nuove normative, investendo in tecnologie di sicurezza, aggiornando le politiche aziendali e coinvolgendo tutto il personale. Le aziende dovrebbero anche considerare l'assistenza di consulenti esperti per garantire il rispetto delle nuove norme.

La NIS 2 e il D.Lgs. 138/2024 rappresentano una svolta nella sicurezza informatica italiana, con l'obiettivo di rendere il Paese più resiliente di fronte alle minacce digitali. È essenziale che le organizzazioni si preparino adeguatamente per affrontare queste sfide e proteggere i loro sistemi e dati sensibili.



SUPPORTO DI JKO CONSULTING

JKO Consulting offre supporto completo alle aziende per l'adeguamento alla Direttiva NIS 2, fornendo consulenza specializzata per garantire la conformità alle nuove normative di sicurezza informatica. Grazie a un team di esperti, JKO Consulting aiuta le imprese a implementare piani di gestione del rischio informatico, sviluppare politiche di sicurezza avanzate e formare il personale, assicurando il rispetto degli standard previsti.

Inviare una e-mail di contatto a : letizia@jkoconsulting.it