**Direttiva UE NIS 2**

**Direttiva UE NIS 2**

Norma comunitaria che mira a creare uno standard **cyber security** condiviso in **UE** per mettere in sicurezza e in modo uniforme, soprattutto, da un punto di vista organizzativo, le infrastrutture e i servizi delle aziende/enti riconducibili ai settori previsti nei **2 cluster** di riferimento, **settori essenziali** (allegato A direttiva NIS2) e **settori importanti** (allegato B direttiva NIS2).

Il testo della normativa NIS 2, che sostituisce la precedente versione NIS, operativa il 26/06/18, è stato approvato il 17 Gennaio 2023, fissando la **scadenza** **per il recepimento** e l’entrata in vigore negli stati membri per il **17 ottobre 2024**, **in Italia è stato recepito con atto del Governo (AG) nel CdM n° 91 dello 07/08/24** e posta sotto il controllo delle autorità competenti o ai **Computer Security Incident Response Teams (CSIRT) che fanno capo all’ACN (*Agenzia per la cyber sicurezza nazionale).***



**A chi è rivolta**

La nuova direttiva UE **per l’obbligatorietà** introduce anche il **criterio del dimensionamento** che interesserà non solo gli enti PA, le grandi imprese, ma anche le **imprese medio-grandi (con un minimo di 50 dipendenti e un fatturato annuo superiore a 10 milioni) che operano all’interno dei settori rilevanti** (A –B)**, le imprese più piccole in generale sono escluse, con l’eccezione di quelle la cui attività è ritenuta di importanza essenziale/critica per la società**.

La NIS 2 non considera essenziale o importante solo la singola organizzazione o il fornitore di servizio, ma anche **la sua supply chain, inoltre, da un punto di vista operativo** la norma, per le procedure e misure da adottare, si rifà principalmente allo **schema** della certificazione **ISO 27001**.

La NIS 2, tra le varie novità, precisa anche che, qualora un soggetto constati una non conformità o un attacco, incidente, ecc., deve comunicarlo e **adottare senza indebito ritardo, tutte le misure correttive** necessarie, appropriate e proporzionate.

**Misure & Requisiti - Obiettivi**

Le misure che i soggetti essenziali e importanti devono mettere in atto devono essere basate su un approccio multirischio, con **l’obiettivo di proteggere** i sistemi informatici e di rete e il loro ambiente fisico da incidenti, in tal senso, dette misure devono comprendere alcuni elementi tra cui, a titolo esemplificativo:

* **Valutazione del rischio**
* **Implementazione di misure di sicurezza**
* **Gestione degli incidenti**
* **Piani di risposta agli incidenti**
* **Notifica degli incidenti**
* **Audit e monitoraggio**
* **Formazione e sensibilizzazione**
* **Cooperazione e condivisione**
* **Misure di sicurezza tecniche**
* **Misure di sicurezza organizzative**