

Homepage > Diritto e fisco > Giustizia

## Cybersicurezza ai nastri di partenza per imprese e p.a.

Dal 1° dicembre 2024 disponibile sul sito della ACN, Agenzia per la cybersicurezza nazionale, la piattaforma per la registrazione dei soggetti tenuti agli obblighi



di [Antonio Ciccina Messina](#) 28/11/2024 | Aggiornato il 28/11/2024



La piattaforma è gestita dall'Agenzia nazionale

**Cybersicurezza** ai nastri di partenza. Dal 1° dicembre 2024 disponibile sul sito della **ACN**, Agenzia per la cybersicurezza nazionale, la piattaforma per la registrazione di **imprese** e pubbliche amministrazioni tenute agli obblighi di cybersicurezza, previsti dalla direttiva nota come NIS2, ovvero la direttiva UE n. 2022/2555 recepita con il d.lgs. d.lgs. 138/2024.

La **piattaforma** sarà anche uno strumento per verificare se si rientra nell'ambito di applicazione della normativa.

---

Al riguardo si stima che ci siano **50 mila enti**, tra soggetti pubblici e soggetti privati, potenzialmente coinvolti nella manovra di **sicurezza cibernetica nazionale**, che devono valutare se iscriversi nella piattaforma. È quanto è emerso nel corso del **convegno** del 27/11/2024 organizzato a Roma dall'Agenzia per la Cybersicurezza Nazionale (ACN), interamente dedicato alla **Direttiva europea Nis2**.

### **Conto alla rovescia**

Parte, dunque, il conto alla rovescia degli **adempimenti** che responsabilizzano una ampia platea di imprese (anche piccole e medie) e di pubbliche **amministrazioni**: sono elencati in quattro allegati al citato d.lgs. 138/2024.

Il primo nodo da sciogliere è proprio comprendere se si rientra nelle **categorie individuate** nei predetti allegati ed è su questo aspetto che le imprese e i soggetti pubblici si stanno interrogando in questi giorni. Un aiuto concreto potrà essere dato dalla **piattaforma dell'ACN**, sulla quale si potranno inserire le informazioni relative al proprio ente e avere un riscontro, sulla base dei **dati caricati**.

Sul sito dell'ACN si trova anche una **tabella** con tutte le **categorie dei soggetti obbligati**, distinti per settore pubblico e privato e in base al campo in cui esercitano l'attività.

Entro il 28 febbraio 2025, dunque, i soggetti pubblici e privati a cui si applica la **NIS** devono manifestarsi all'**Autorità nazionale competente NIS**, registrandosi sulla piattaforma digitale che, come detto, sarà resa disponibile **dal 1° dicembre 2024**.

L'adempimento della registrazione serve ad ACN di **censire i soggetti** coinvolti, non solo per l'attività di vigilanza ma anche per quella di assistenza e **supporto**.

### **Registrazione cruciale**

La fase della registrazione è, quindi, cruciale e, non a caso, la normativa prevede che la **mancata registrazione** è punita con una sanzione amministrativa pecuniaria con un importo fino al **0.1% del fatturato annuo** su scala mondiale del soggetto.

Peraltro, la registrazione di un soggetto sulla **piattaforma** di ACN non significa acquisire immediatamente la qualifica di soggetto obbligato agli adempimenti NIS2, La **registrazione**, infatti, è successivamente sottoposta ad una fase di analisi.

Successivamente, dopo la registrazione, nel **mele di aprile 2025**, i soggetti che si sono registrati riceveranno una **comunicazione** per confermare, o meno, il loro inserimento nell'elenco dei soggetti NIS e a quel punto i **soggetti confermati** da ACN dovranno integrare le informazioni, sempre tramite la piattaforma digitale, indicando spazio IP, nomi di dominio disponibili, ambito territoriale di **fornitura dei servizi**, rappresentanti legali (che sono anche responsabili degli inadempimenti in caso di violazioni), **punti di contatto**.

Anche per gli obblighi è previsto un approccio graduale. In particolare, entro gennaio 2026 (ovvero **entro 9 mesi** dalla ricezione della notifica di inserimento nell'elenco dei soggetti NIS) scatterà l'**obbligo di notificare** gli incidenti informatici, Inoltre, entro ottobre 2026 (ovvero entro 18 mesi dalla ricezione della notifica di inserimento nell'elenco dei soggetti NIS), si dovranno **adempiere gli obblighi** di base in materia di sicurezza informatica. Il catalogo degli adempimenti è molto nutrito e prevede l'approvazione delle misure di **gestione dei rischi** e della sicurezza informatica e dei piani di formazione, l'adozione di **misure tecniche**, operative e organizzative, tra cui analisi multi-rischio, precauzioni per la continuità operativa, sistemi di crittografia e **controllo degli accessi** e adempimenti specifici per i gestori dei registri di nomi di dominio.

*Riproduzione riservata*

**Antonio Ciccia Messina**

Collaboratore



---

 **LinkedIn**

---