

GUARDUCCI LORENZINI & ASSOCIATI

Dottori Commercialisti

Dott. Enrico Guarducci
Dott. Domenico Ciafardoni
Dott. Salvatore Marchese
Dott. Gianluca Bogini
Dott. Giulio Nicolò Campagni
Dott. Nicola Sportolari
Dott. Marco Battistini
Dott.ssa Veronica Bonciarelli

Ai Preg.mi
Signori Clienti
Loro Sedi

Circolare n. 18/2025

Perugia, 30 giugno 2025

Oggetto: Normativa NIS 2

La direttiva NIS2 (Network and Information Security 2) è una normativa europea sulla cybersicurezza, mirata a rafforzare le infrastrutture digitali critiche.

Essa stabilisce un quadro giuridico uniforme per la sicurezza informatica in 18 settori critici all'interno dell'UE, imponendo misure per proteggere, come detto, le infrastrutture digitali.

In merito a tale nuovo adempimento lo Studio provvede a fornire le linee guida, fermo restando che è indispensabile per coloro potenzialmente soggetti all'obbligo di contattare esperti informatici.

Soggetti interessati

La NIS2 si applica a un'ampia gamma di organizzazioni, in particolare quelle che operano in settori considerati critici per il funzionamento della società europea, quali, tra gli altri:

- Settore sanitario: Strutture sanitarie e aziende farmaceutiche.
- Settore energetico: Aziende che operano nella produzione, trasporto e distribuzione di energia.
- Settore dei trasporti: Aziende che operano nei settori del trasporto aereo, ferroviario, marittimo e su strada.
- Fornitori di servizi digitali: Data center, piattaforme di social network, fornitori di servizi cloud e altri.
- Altri settori: Inclusi i servizi postali, la gestione dei rifiuti, l'industria aerospaziale e la filiera agro-alimentare.

Soggetti obbligati

Sono tenute a rispettare gli obblighi della normativa tutte le aziende con almeno 50 dipendenti o un fatturato annuo superiore ai 10 milioni di euro. Tuttavia, anche aziende più piccole potrebbero essere coinvolte se operano in un settore critico o forniscono servizi essenziali a soggetti obbligati

Cosa prevede la direttiva NIS2

La direttiva NIS2 impone alle organizzazioni di:

- Gestire i rischi informatici: adottare misure tecniche e organizzative per mitigare i rischi cybernetic. Questo include la gestione delle vulnerabilità, la protezione della catena di approvvigionamento e la formazione del personale.
- Rendere conto della sicurezza: implementare misure per garantire la sicurezza dei sistemi informativi e delle reti, prevenire incidenti e minimizzare l'impatto degli stessi.
- Notificare gli incidenti: le aziende devono notificare alle autorità competenti eventuali incidenti di sicurezza entro 24 ore.
- Garantire la continuità operativa: implementare piani di risposta agli incidenti e misure per garantire la continuità dei servizi essenziali anche in caso di attacco informatico.
- Assicurare la trasparenza: aggiornare regolarmente le informazioni richieste dalla piattaforma ACN (Agenzia per la Cybersicurezza Nazionale).

Come adeguarsi alla Direttiva NIS 2

Per essere conformi alla Direttiva NIS 2, le aziende devono adottare un approccio strutturato alla cybersecurity, implementando misure tecniche e organizzative efficaci per prevenire, rilevare e rispondere agli attacchi informatici.

La normativa stabilisce obblighi precisi che vanno dalla gestione del rischio alla notifica degli incidenti, fino alla protezione della [supply chain](#) e alla formazione del personale.

1. Analisi del rischio e misure di sicurezza

Ogni azienda deve condurre una valutazione dettagliata delle vulnerabilità informatiche, identificando le possibili minacce ai propri sistemi IT e adottando misure di mitigazione adeguate. Tra le azioni richieste:

- implementare strumenti avanzati di difesa, come firewall, antivirus e sistemi di rilevamento delle intrusioni (IDS/IPS).
- proteggere i dati sensibili con crittografia e backup regolari.
- garantire il monitoraggio continuo delle infrastrutture IT tramite un Security Operations Center (SOC).

2. Sicurezza della supply chain

La protezione non riguarda solo l'azienda, ma anche i fornitori e i partner con cui collabora. La Direttiva NIS 2 impone di:

- verificare il livello di sicurezza dei fornitori e richiedere loro certificazioni o audit di conformità.
- adottare clausole contrattuali specifiche per garantire che anche terze parti rispettino gli standard di cybersecurity.
- monitorare costantemente la supply chain per individuare possibili falle nei sistemi.

3. Formazione e sensibilizzazione del personale

La NIS 2 obbliga le aziende a:

- organizzare corsi di formazione periodici per dipendenti e dirigenti.
- simulare attacchi informatici per testare la capacità di risposta.
- definire procedure interne chiare per riconoscere e segnalare minacce sospette.

4. Controlli e audit periodici

Le autorità di vigilanza eseguiranno verifiche ispettive per accertare la conformità alla normativa. Le aziende devono quindi:

- effettuare controlli interni regolari per valutare l'efficacia delle misure adottate.
- prepararsi ad audit ufficiali, documentando tutte le attività svolte per garantire la sicurezza informatica.
- adeguarsi rapidamente a nuove direttive e aggiornamenti normativi.

Scadenze importanti

- 1^a gennaio 2026: termine per l'adeguamento completo alle nuove normative da parte dei soggetti interessati.

Sanzioni

In caso di mancato rispetto della direttiva NIS2, sono previste sanzioni amministrative pecuniarie che possono arrivare fino a 10 milioni di euro o il 2% del fatturato globale annuo per i servizi essenziali, e fino a 7 milioni di euro o l'1,4% del fatturato globale annuo per gli altri soggetti.

Cordiali saluti