DIRETTIVA NIS 2

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

Adeguamento alla Direttiva Europea 2022/2555

(NIS 2: Network and Information Security 2)

1. Cosa è

La Direttiva NIS 2, acronimo di "Network and Information Security 2", è la nuova normativa europea (Direttiva 2022/2555) che sostituisce la precedente Direttiva NIS (2016/1148).
Questa normativa stabilisce un quadro comune per la sicurezza delle reti e dei sistemi informativi degli Stati Membri dell'UE, con l'obiettivo di uniformare le misure di sicurezza e rafforzare la resilienza informatica.
La Direttiva NIS 2 introduce un approccio più coerente e collaborativo alla gestione della sicurezza informatica, affrontando le disparità tra i diversi Paesi dell'UE.
Essa impone il coinvolgimento della direzione, requisiti **più rigorosi in termini di segnalazione degli incidenti, un approccio basato sul rischio e applicazione delle norme, per garantire un livello di sicurezza elevato e uniforme a livello europeo**.

L'adeguamento alla Direttiva NIS 2 comporta numerosi vantaggi, tra cui:

- **Riduzione dei rischi aziendali**:
Minimizza il rischio di incidenti di sicurezza informatica attraverso misure proattive di gestione delle informazioni.

- **Allineamento alle normative e alle best practice internazionali**:
Assicura che l'organizzazione sia in linea con il mercato e con le migliori pratiche globali in materia di sicurezza informatica.

- **Vantaggio competitivo**:
Rafforza la reputazione dell'azienda agli occhi di clienti e fornitori, dimostrando un impegno serio verso la sicurezza delle informazioni.

2. Perchè adeguarsi

Oltre a rispondere a un obbligo di legge per molte aziende, l'adeguamento volontario alla Direttiva NIS 2 offre un'opportunità strategica per migliorare il sistema di gestione della sicurezza delle informazioni.
Implementare i requisiti minimi di sicurezza indicati dalla direttiva consente di identificare e risolvere criticità e di sviluppare un sistema più robusto.

Rendere la tua azienda conforme alla Direttiva NIS 2 dimostra un livello adeguato di attenzione alla sicurezza informatica, cruciale anche per la sicurezza della supply chain.
Inoltre, la conformità alla Direttiva NIS 2 attesta ai clienti, fornitori e partner che l'azienda è affidabile e attenta alla protezione delle informazioni.

3. A chi è rivolta

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

La Direttiva NIS 2 si applica a specifici settori aziendali, che rispondono a determinati parametri quali:

Aziende operanti nei settori essenziali

- Energia
- Trasporti
- P.A.
- Sanità
- Infrastrutture digitali
- Banche
- Mercati Finanziari
- Acqua potabile
- Acque reflue
- Ricerca spaziale
- Informazione e comunicazione

Aziende operanti nei settori importanti

- Servizi postali
- Gestione rifiuti
- Imprese alimentari
- Sostanze chimiche
- Fabbricazione mezzi di trasporto
- Fabbricazione impianti elettrici e n.c.a.
- Fornitori servizi digitali
- Fabbricazione dispositivi medici
- Ricerca
- Fabbricazione prodotti ottici

Aziende aventi i seguenti requisiti dimensionali (D. Lgs. 138/2024)

- 50 dipendenti
- 10 mln di fatturato o bilancio annuo

4. Scadenze Chiave e roadmap NIS 2

31 dicembre 2024:
Assessment Cyber Security per verificare l'applicabilità del decreto.

17 gennaio 2025:
Registrazione per fornitori specifici (es. cloud, data center).

15 aprile 2025:
Comunicazione dell'inclusione nell'elenco e nomina del responsabile per la conformità.

ottobre 2026:
Implementazione degli obblighi di governance e gestione dei rischi.

2025 — 2026

1° gennaio 28 febbraio 2025:
Registrazione sulla piattaforma ACN per i soggetti interessati.

31 marzo 2025:
ACN pubblica l'elenco dei soggetti essenziali e importanti.

1° gennaio 2026:
Adeguamento agli obblighi di notifica degli incidenti e aggiornamento annuale delle informazioni sulla piattaforma ACN.

5. Obblighi e sanzioni

DATACONSEC
DATA PROTECTION - CONSULTING - SECURITY

La Direttiva NIS 2 definisce un **sistema di vigilanza** più rigoroso per la sicurezza informatica e **sanzioni più severe** per i soggetti inadempienti.

Le organizzazioni in ambito saranno sottoposte a **controlli** più frequenti e approfonditi e dovranno **notificare** tempestivamente qualsiasi **incidente informatico** che abbia un impatto significativo sulla fornitura dei propri servizi e, in particolare, presentare al relativo CSIRT o se del caso l'autorità competente:

- un **preallarme** entro 24 ore dal momento in cui sono stati informati dell'incidente significativo;
- una **notifica** entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo;
- una **relazione finale** dettagliata entro un mese dalla trasmissione della notifica dell'incidente di cui al punto precedente.

Il **mancato rispetto degli obblighi previsti** comporterà **sanzioni pecuniarie amministrative** che potranno arrivare fino al maggiore tra **€ 10.000.000** o **2%** del fatturato mondiale annuo dell'azienda per i **Soggetti Essenziali** e **€ 7.000.000** o **1,4%** del fatturato mondiale annuo per i **Soggetti Importanti**. Nei casi più gravi, la mancata conformità di un soggetto essenziale può portare alla **sospensione o al divieto temporaneo per i dirigenti** (es. amministratore delegato/rappresentante legale) **di esercitare le loro funzioni** all'interno dell'entità stessa.

6. I nostri servizi per l'adeguamento alla direttiva

- **GAP Analysis**:
  Analisi delle lacune rispetto ai requisiti NIS2 per identificare aree di miglioramento.
- **Compliance NIS 2**:
  Supporto completo per l'allineamento dell'azienda alla direttiva.
- **Individuazione di standard/framework di sicurezza**:
  Selezione degli standard e dei framework di sicurezza più adeguati per rispettare i requisiti normative (es. ISO 27001).
- **Internal Audit**:
  Servizio di audit interno per verificare la conformità e migliorare i processi di sicurezza.
- **Audit ai fornitori (qualifica supply chain)**:
  Verifica della conformità dei fornitori alla direttiva per garantire la sicurezza della supply chain.

Questi servizi sono progettati per supportare le aziende in tutte le fasi di adeguamento alla Direttiva NIS 2, garantendo la massima sicurezza e competitività sul mercato da parte di professionisti con competenze tecnico-giuridico-organizzative.

7. Figure professionali presenti nel nostro team

Le attività saranno erogate da un team di consulenti specializzati che vantano una riconosciuta professionalità, anche in ambito accademico, all'occorrenza integrato da professionisti esterni.
DCS costituirà un Team di consulenti così composto:

- **Responsabili di progetto** in possesso di certificazione CISA, Lead Auditor Information Security Management System ISO27001, Lead Auditor Business Continuity Management System ISO 22301;

- **Auditor Privacy GDPR** specializzati in ICT con ventennale esperienza in possesso di certificazione Lead Auditor Sistemi di Gestione Qualità ISO 9001, Lead Auditor Information Security Management System ISO 27001, Lead Auditor Business Continuity Management System BS25999/ISO 22301;

- **Security Tester** (VA e PT);

- **Security Manager Senior** con ventennale esperienza;

- **Consulente Privacy Junior** (Front & Back Office);

- **Project Manager** specializzato in Sistemi di Gestione a 360°;

- Docenti universitari specializzati in materie Tecnico-giuridiche.

DataConSec S.r.l.
Business Security & IT Governance

V.le Fratti, 56 Parma (Italy)
Tel. e Fax: +39 0521.771298
e-mail: info@dataconsec.com
amministrazione@pec.dataconsec.com
www.dataconsec.com

P.IVA e C.F. 02470920345