08 • 2024

sata

# CYBERSICUREZZA e IMPRESE ALIMENTARI

## Cosa è cambiato dal 18 ottobre

CONSULENZA IN PILLOLE

A CURA DI: DOTT. ROBERTO CAPURRO, DOTT. DAVIDE BENZI

## Gli aggiornamenti per punti

In sintesi, la Direttiva NIS2 richiede alle imprese alimentari di adottare misure robuste per la cybersicurezza, promuovendo una cultura della sicurezza e un adeguamento continuo alle nuove normative.

- La sicurezza delle reti e dei dati informatici (cibersicurezza) diventa obbligo di legge con il decreto 138 (recepimento della Direttiva UE NIS2) **in vigore dal 18 ottobre**
- L'obbligo investe anche il settore alimentare delle medie imprese ritenute dal legislatore "soggetto importante"
- La responsabilità delle violazioni al decreto è in capo "agli organi amministrativi e agli organi direttivi"
- La cibersicurezza presuppone un approccio di valutazione multi-rischio e una serie di azioni stabilite per legge (art. 24)
- L'attenzione ed il controllo sulle misure per la cibersicurezza va rivolto a tutta la catena di approvvigionamento (fornitori di merci e servizi)
- Necessario individuare risorse, formare i vertici con compiti di responsabilità e formare tutto il personale sui principi basilari di "igiene informatica" e rischi collegati a comportamenti scorretti
- Registrarsi al portale dell'agenzia nazionale per la cibersicurezza fra **il 1 gennaio ed il 28 febbraio 2025**
- Obbligo di notificare tempestivamente gli incidenti e dare prova della gestione dell'incidente con adeguate azioni di rimedio

## Premessa

Negli ultimi anni, la sicurezza informatica è diventata una priorità per governi, aziende e cittadini a causa dell'aumento delle minacce informatiche. L'Unione Europea ha introdotto la Direttiva UE 2022/2555, nota come NIS2, per rafforzare la resilienza delle infrastrutture critiche e migliorare la gestione dei rischi. Questa direttiva sostituisce la precedente Direttiva 2016/1148 (NIS) e apporta modifiche significative, come l'ampliamento del perimetro di applicazione a nuovi settori economici, il rafforzamento delle misure di prevenzione e la promozione della cooperazione tra paesi membri.

## Cos'è la Cybersicurezza

La sicurezza della rete e dei sistemi informativi è definita come la capacità di resistere a qualsiasi azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati. Il PNRR italiano affronta la cybersicurezza come un insieme di tecnologie, attività e procedure volte a garantire la sicurezza informatica di reti e dispositivi. La direttiva NIS2 è già in vigore e gli stati membri devono implementare le misure nazionali entro il 18 ottobre.

## Rischi per individui e imprese

Dal 1 gennaio 2023 al 31 luglio 2024, in Italia si sono verificati 19.364 episodi di cyber attacchi. L'Italia è uno dei paesi più esposti a questi rischi in Europa. Questi dati evidenziano la vulnerabilità delle infrastrutture e la necessità di rafforzare gli strumenti di cyber difesa. Il Ministero dell'Interno sottolinea l'importanza di una cultura della cybersicurezza per cittadini e imprese.

## Dir NIS2 e Imprese Alimentari

La direttiva NIS2 amplia il perimetro di applicazione includendo la produzione, trasformazione e distribuzione di alimenti. Imprese del settore aventi caratteristiche di media o grande impresa sono classificate come "soggetti importanti" e sono tenute ad adeguarsi alla nuova normativa adottando misure tecniche, operative e organizzative adeguate per gestire i rischi informatici.

## Recepimento in Italia

Il recepimento della NIS2 in Italia è stato formalizzato con due provvedimenti legislativi: la Legge n. 90/2024 sulla Cybersecurity e il Decreto 138/2024. Questi provvedimenti definiscono gli obblighi per i soggetti interessati, tra cui la registrazione presso l'Autorità per la Cybersicurezza Nazionale (ACN) e l'adozione di misure specifiche per la gestione dei rischi.

## Preparazione delle Imprese

Le imprese devono sviluppare una cultura della cybersicurezza a tutti i livelli e prevedere un piano di formazione articolato. È necessario un percorso di adeguamento basato su analisi dei rischi per assicurare la conformità alla nuova normativa.

Inoltre, le imprese alimentari devono valutare i potenziali rischi derivanti dai fornitori e prepararsi a rispondere alle richieste di cybersicurezza dai loro clienti.

## Integrazione con altre normative

La direttiva NIS2 ha punti in comune con il GDPR, con l'obiettivo di garantire un elevato livello di sicurezza dei dati. L'approccio basato sull'analisi del rischio è comune a diverse normative, come la sicurezza alimentare e dei lavoratori.

## Certificazioni

L'articolo 27 del Decreto 138 prevede l'utilizzo di servizi o tecnologie certificate a livello EU. Le aziende possono adottare sistemi di certificazione volontaria, come la norma ISO/IEC 27001:2022, per la sicurezza delle informazioni.