CHIAPPORI – BENZI
DOTTORI COMMERCIALISTI ASSOCIATI

Dott. DOMENICO CHIAPPORI - REVISORE CONTABILE
Dott.sa MAURA BENZI - REVISORE CONTABILE

Dott.sa VALERIA MASSOLLO
Dott. FEDERICO FERRANTE
Dott. ROBERTO MAZZITELLI
Dott. UMBERTO CARRARA

Circolare mensile per l'impresa

Servizio di informazione amministrativa, contabile e tributaria per le imprese

Agosto 2026

Rif.: 09

D.Lgs. 138/2024, in applicazione dell Direttiva (UE) 2022/2555 *pag. 2*
(La Direttiva UE-NIS2 sulla cibersicurezza)

VIA PALESTRO 15/9 - 16122 GENOVA - TEL. 010. 81 09 90 - 010. 839 90 96
CODICE FISCALE E PARTITA IVA : 03339810107
E-mail : amministrazione@chiappori-benzi.it

D.Lgs. 138/2024, in applicazione dell Direttiva (UE) 2022/2555

(La Direttiva UE-NIS2 sulla cibersicurezza)

Gent.mi Clienti,

Con l'entrata in vigore del quadro normativo legato alla Direttiva (UE) 2022/2555 (NIS2), recepita in Italia dal Decreto Legislativo n. 138/2024, l'Unione Europea ha significativamente innalzato il livello richiesto di flessibilità informatica e gestione del rischio cyber, estendendo gli obblighi di conformità a un perimetro molto più ampio di settori critici e strategici. La presente circolare ha l'obiettivo di illustrare il contesto normativo, i soggetti direttamente coinvolti dagli obblighi di legge e le implicazioni pratiche sulla governance della sicurezza e sulla catena di fornitura (supply chain).

Segue un breve indice:

1. L’impatto della NIS2 sulla resilienza digitale delle imprese
2. NIS2: la normativa e gli adempimenti per l’anno 2026
3. Quali aziende sono soggette alla NIS2
3.1. Chi sono i soggetti essenziali della NIS2
3.2. Chi sono i soggetti importanti della NIS2
4. Cosa prevede la NIS2: gli obblighi di ottobre 2026
5. Cos’è la certificazione NIS2

1. L’impatto della NIS2 sulla resilienza digitale delle imprese

L’approssimarsi della scadenza **di ottobre 2026** pone la gran parte delle aziende italiane davanti all’obbligo di completare i processi di adeguamento alla NIS2.
Questa tappa temporale si inserisce in un percorso di messa in sicurezza avviato con l’operatività dei sistemi di notifica degli incidenti. Entro il mese di ottobre, le aziende dovranno aver reso pienamente funzionanti le misure di sicurezza di base.

In un mercato interconnesso, l’allineamento agli standard entro l’autunno è una condizione necessaria per tutelare la continuità del business e la solidità della catena di fornitura. Una gestione rigorosa di questa fase permette alle imprese di consolidare la propria affidabilità e di prevenire interruzioni critiche, che potrebbero compromettere il loro posizionamento competitivo.

2. NIS2: la normativa e gli adempimenti per l’anno 2026

Il 2026 segna il passaggio della NIS2 dalla fase di recepimento formale a quella di attuazione operativa.
Il percorso tracciato dal D.Lgs. 138/2024, in armonia con la Direttiva (UE) 2022/2555 , impone alle imprese un calendario di scadenze serrate, che per il 2026 si articola in tre fasi cruciali:

- **gennaio 2026, operatività della risposta**: a inizio anno è scattato l’obbligo di notifica degli incidenti significativi. Le aziende devono essere pronte a identificare tali eventi e attivare i canali di notifica verso l’ACN secondo le tempistiche di legge, definendo ruoli e responsabilità certi. Inoltre, è stata riaperta la piattaforma ACN per il rinnovo delle iscrizioni esistenti e l’inserimento delle nuove;
- **febbraio – settembre 2026, adeguamento settoriale**: le organizzazioni sono chiamate a recepire le linee guida specifiche che l’ACN pubblica per i singoli comparti. L’adeguamento delle misure di sicurezza deve essere calibrato sulle peculiarità del proprio contesto operativo;
- **ottobre 2026, consolidamento e integrazione**: entro questo termine, le misure di sicurezza di base devono uscire dalla dimensione documentale per diventare prassi consolidate. La scadenza di ottobre esige che l’assetto organizzativo e tecnico sia pienamente funzionante e

integrato nei processi aziendali quotidiani, garantendo la resilienza richiesta dalla norma. E precisamente:

- **gli organi di amministrazione e gestione devono approvare formalmente e supervisionare l'adozione delle misure di sicurezza (art. 23 del Decreto);**
- **deve essere completata la formazione specifica per gli organi di amministrazione e l' attivazione dei programmi periodici per i dipendenti;**
- **operatività delle misure per tutti i cluster definiti dagli Allegati 1 e 2 della Determinazione 379907/2025 -Governance (GV), Identificazione (ID), Protezione (PR), Rilevamento (DE), Risposta (RS), Ripristino (RC) -coerenti con il Framework Nazionale per la Cybersecurity e Data Protection da cui sono derivati;**
- **completamento della formazione specifica per gli organi di amministrazione e attivazione dei programmi periodici per i dipendenti;**
- **test e simulazione delle procedure di incident response;**
- **audit interni e chiusura delle non conformità rilevate in fase di gap analysis;**
- **verifica della supply chain: mappatura dei fornitori ICT rilevanti, audit mirati, clausole contrattuali aggiornate.**

3. Quali aziende sono soggette alla NIS2

Il perimetro di applicazione della NIS2 distingue le organizzazioni in due categorie: soggetti essenziali e soggetti importanti.

Entrambe le categorie comprendono comparti industriali e di servizio imprescindibili per l'equilibrio economico e sociale dell'UE. Tuttavia, la loro differenziazione deriva da un'analisi combinata, che incrocia le dimensioni dell'azienda con la rilevanza strategica che essa riveste per la tenuta del mercato unico.

3.1.1. Chi sono i soggetti essenziali nella NIS2

Vengono definiti soggetti essenziali quegli operatori la cui paralisi informatica determinerebbe ripercussioni sistemiche sulla tenuta del Paese.

La qualifica di “essenziale” scatta automaticamente per i soggetti con un numero di dipendenti pari o superiore a 250 o che registrano un volume d’affari superiore a 50 milioni di euro (o un bilancio di almeno 43 milioni), a condizione che operino nei pilastri strategici della società.
Il perimetro di questa categoria abbraccia i seguenti settori: energia, trasporti, finanza, sanità, acqua potabile, acque reflue, infrastrutture digitali, operatori di servizi spaziali terrestri e fornitori di servizi correlati, Pubblica Amministrazione.

3.2.2. Chi sono i soggetti importanti nella NIS2

Sono considerati soggetti importanti le organizzazioni che, pur non essendo classificate come “essenziali”, rivestono un ruolo significativo per l’equilibrio del mercato e della società.
In questa categoria rientrano le realtà che occupano almeno 50 dipendenti oppure quelle che, indipendentemente dal numero di collaboratori, registrano un volume d’affari superiore a 10 milioni di euro.
Il perimetro operativo dei soggetti importanti tocca ambiti diversificati, ma fondamentali: servizi postali, gestione dei rifiuti, prodotti chimici, alimentare, manifatturiero, ricerca e servizi digitali.
In concreto, l’effetto della NIS2 si estende ben oltre i confini dei soggetti censiti, poiché la normativa impone alle organizzazioni obbligate una verifica rigorosa sulla resilienza dei propri partner commerciali.
Questo meccanismo di responsabilità a cascata trasforma la sicurezza informatica in un requisito contrattuale imprescindibile: le realtà più strutturate integreranno standard di protezione specifici come precondizione per la qualifica dei fornitori, rendendo la conformità un fattore determinante per rimanere competitivi sul mercato.

4. Cosa prevede la NIS2: gli obblighi di ottobre 2026

Il traguardo di ottobre 2026 non è un termine generico, ma l’atto conclusivo di un cronoprogramma partito con la notifica di inclusione negli elenchi dell’ACN.
Questa comunicazione ufficiale apre una ‘finestra’ di 18 mesi entro cui le organizzazioni devono allinearsi ai nuovi standard. Poiché le prime fasi di censimento si sono concentrate tra la fine del 2024 e l’inizio del 2025, l’autunno del 2026 segna il momento in cui il periodo di tolleranza si esaurisce: entro questa data, le intenzioni devono essersi già trasformate in

capacità difensiva reale attraverso l'adozione di un modello di sicurezza basato su cinque direttrici operative concretamente funzionanti.

Il primo pilastro riguarda l'identificazione, ovvero la capacità di mappare con precisione tutti gli asset aziendali e condurre un'analisi del rischio accurata: non si può difendere ciò di cui non si conosce l'esistenza o il valore.

Una volta definito il perimetro, scattano le misure di protezione, che prevedono l'uso concreto di strumenti come firewall, sistemi di protezione degli endpoint e l'autenticazione a più fattori (MFA), con l'obiettivo prioritario di ridurre al minimo la superficie esposta a eventuali attacchi.

Tuttavia, la prevenzione da sola non basta. La normativa richiede sistemi capaci di rilevare tempestivamente le minacce attraverso il monitoraggio costante e l'analisi dei log, intercettando ogni anomalia prima che diventi critica.

Nel momento in cui si verifica un evento avverso, l'azienda deve essere pronta a rispondere, seguendo processi prestabiliti di gestione degli incidenti, garantendo reazioni rapide ed efficaci in tempi stretti.

Infine, il ciclo si chiude con il ripristino: attraverso strategie di backup e piani di disaster recovery testati, l'organizzazione deve essere in grado di recuperare i dati e tornare operativa nel minor tempo possibile, assicurando la continuità del business.

Sebbene tali adempimenti accomunino sia i soggetti essenziali che quelli importanti, la reale linea di demarcazione risiede nel regime di vigilanza. I primi soggetti sono sottoposti a controlli ex-ante: l'autorità può dunque disporre verifiche e ispezioni in qualsiasi momento per accertare la conformità, a prescindere dal verificarsi di incidenti. Al contrario, i soggetti importanti sono chiamati a una vigilanza ex-post: in questo caso, i controlli scattano solitamente a seguito di una sospetta violazione o dopo un incidente significativo che abbia portato alla luce falle nei sistemi difensivi.

5. Cos'è la certificazione NIS2

Sebbene la normativa NIS2 non introduca una certificazione obbligatoria o un sistema di certificazione unico in senso stretto, il termine "certificazione NIS2" viene comunemente impiegato per indicare l'adozione di standard e framework riconosciuti utili a dimostrare la conformità ai requisiti della direttiva.

In questo contesto, le certificazioni ISO sono degli strumenti operativi capaci di supportare l'efficacia delle misure adottate.

La ISO 27001 rappresenta il punto di riferimento per la gestione della sicurezza delle informazioni. Adottare questo standard significa implementare un metodo sistematico per proteggere i dati e gestire i rischi informatici, coprendo gran parte dei requisiti richiesti in termini di gestione della sicurezza delle informazioni.

Parallelamente, la ISO 22301 si focalizza sulla resilienza: aiuta le organizzazioni a strutturare piani di continuità operativa realmente testati. Questo garantisce che, di fronte a un incidente, l'azienda disponga delle procedure necessarie per mantenere attivi i servizi essenziali, rispondendo direttamente agli obblighi di ripristino previsti dalla direttiva NIS2.

Lo Studio rimane a disposizione per ogni ulteriore chiarimento.

Con i migliori saluti.

STUDIO CHIAPPORI-BENZI