



Essere al passo con la Direttiva NIS 2: Cosa devono sapere le imprese

Premessa

Affrontare le sfide derivanti da un panorama normativo e tecnologico sempre più complesso, insieme alle minacce in costante evoluzione, richiederà un impegno sistemico da parte delle organizzazioni per elevare il livello di sicurezza cibernetica a livello nazionale ed europeo nei prossimi anni.

L'entrata in vigore della **Direttiva NIS 2** a gennaio 2023 ha introdotto nuovi obblighi di sicurezza informatica per grandi e medie imprese, sia pubbliche che private. Con il recepimento imminente da parte degli Stati Membri, i soggetti coinvolti dovranno rispettare requisiti stringenti in materia di governance, continuità operativa, controllo della catena di approvvigionamento,

segnalazione degli incidenti e gestione dei rischi.

Il **18 ottobre 2024**, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha messo a disposizione una piattaforma digitale per l'auto-registrazione, dove le organizzazioni che ritengono di essere coinvolte dalle prescrizioni della **Direttiva NIS 2** potranno auto-registrarsi, fornendo un elenco dettagliato delle proprie attività e dei servizi offerti. Successivamente, l'ACN valuterà la posizione di ciascun soggetto e darà riscontro sulla rilevanza e conformità rispetto alle nuove norme di sicurezza cibernetica.

Indice

Introduzione	03
Che impatto avrà la Direttiva NIS 2 sulla tua organizzazione?	04
I soggetti tenuti ad adeguarsi	04
Sei un soggetto obbligato?	07
Obblighi	09
Segnalazione e gestione degli incidenti	11
Sanzioni	11

Introduzione

A gennaio 2023, gli Stati membri dell'Unione Europea hanno ufficialmente approvato una revisione della Direttiva sulla sicurezza delle reti e dei sistemi informatici (Network and Information Systems - NIS) del 2016. Progettata come risposta a cyber attacchi ampiamente diffusi e dannosi, la **Direttiva NIS 2** potenzia i requisiti di sicurezza, semplifica gli obblighi di reportistica e introduce misure di supervisione più severe, insieme a requisiti di applicazione più rigorosi. L'obiettivo della nuova Direttiva è rafforzare le difese delle entità critiche contro le vulnerabilità della supply chain, gli attacchi ransomware e altre minacce informatiche.



La **Direttiva NIS 2** ha l'obiettivo di potenziare i requisiti di sicurezza, semplificare gli obblighi di reportistica e introdurre misure di supervisione più severe, insieme a requisiti di applicazione più rigorosi, con l'obiettivo di aumentare la cybersecurity.

Gli Stati membri, tuttavia, si sono dimostrati riluttanti nell'applicare sanzioni, allocare risorse finanziarie e umane, e condividere informazioni in modo sistematico. Ciò ha contribuito a minare, da un lato, l'efficacia delle misure di cybersicurezza adottate dai soggetti in perimetro e, dall'altro, la capacità dell'UE di conseguire un adeguato livello di consapevolezza situazionale comune. Tutte queste sfide rendono ancora più cruciale l'implementazione efficace della **Direttiva NIS 2**, per migliorare la sicurezza cibernetica complessiva.

Questo documento fornisce una breve panoramica della **Direttiva NIS 2** e spiega come potrebbe influire sul business, fornendo anche indicazioni su come prepararsi.

Che impatto avrà la Direttiva NIS 2 sulla tua organizzazione?

Va sottolineato che la **Direttiva NIS 2** rappresenta un'evoluzione della **Direttiva NIS originale**, la quale aveva l'obiettivo di potenziare i livelli di cybersecurity in tutta l'Unione Europea. Le modifiche e le nuove disposizioni introdotte dalla Direttiva NIS 2 mettono un forte accento sull'aspetto della preparazione, ed avrà un impatto significativo sulle organizzazioni. La **Direttiva NIS 2** copre più settori, introduce controlli di sicurezza più approfonditi e impone requisiti di reportistica sugli incidenti più rigorosi.

- Le organizzazioni precedentemente esentate potrebbero dover implementare nuovi sistemi e pratiche di sicurezza informatica per adeguarsi alla **Direttiva NIS 2**.
- Al contempo, le organizzazioni già vincolate dalla Direttiva originale potrebbero essere obbligate a rivedere i loro sistemi e le pratiche di sicurezza per conformarsi alla **Direttiva NIS 2**.



I soggetti tenuti ad adeguarsi

La portata di applicazione della NIS 2 è notevolmente più ampia rispetto alla precedente NIS, coinvolgendo un numero più esteso di soggetti e settori. A differenza della NIS, che si rivolgeva esclusivamente agli "Operatori di servizi essenziali" (OSE) e ai "Fornitori di servizi digitali" (FSD), la nuova Direttiva si estende a tutte le organizzazioni identificate come soggetti "Essenziali" o "Importanti".

MEDIE IMPRESE



Per determinare l'inclusione di un'organizzazione in una di queste categorie, viene introdotto un criterio duplice basato sulla dimensione (size-cap rule) e sul settore di appartenenza. Rientrano nel perimetro le **medie imprese**, definite come **quelle con meno di 250 dipendenti** e un **fatturato annuo non superiore a 50 milioni di euro**, o le imprese che superano i massimali delle medie imprese nei settori specificati negli allegati I e II della Direttiva.

PICCOLE IMPRESE



Anche alcune piccole imprese rientrano nel perimetro, come ad esempio quelle con **meno di 50 dipendenti** e un **fatturato annuo inferiore a 10 milioni di euro**, e le **microimprese** con **meno di 10 dipendenti** e un **fatturato annuo non superiore a 2 milioni di euro**, a condizione che svolgano un ruolo chiave per la società, l'economia o siano cruciali per particolari settori o tipi di servizi, rientrando così nell'ambito di applicazione della presente Direttiva.

SETTORI AD ALTA CRITICITA'



Energia



Trasporti



Settore bancario



Infrastrutture dei mercati finanziari



Settore sanitario



Acqua potabile



Acque reflue



Infrastrutture digitali



Gestione dei servizi TIC



Pubblica Amministrazione



Spazio

ALTRI SERVIZI CRITICI



Servizi postali e di corriere



Gestione dei rifiuti



Fabbricazione, produzione e distribuzione di sostanze chimiche



Produzione, trasformazione e distribuzione di alimenti



Fabbricazione (dispositivi medici, computer, autoveicoli, ecc.)



Fornitori di servizi digitali



Ricerca

Il criterio della dimensione non si applica alle Pubbliche Amministrazioni. Infatti, **sono soggette agli obblighi della NIS 2 gli enti della PA centrale**, definiti conformemente al diritto nazionale di uno Stato membro, e **gli enti a livello regionale** che, in seguito a una valutazione basata sul rischio, offrono servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali ed economiche critiche. Tuttavia, **sono esentati dagli obblighi della NIS 2** gli enti della **pubblica amministrazione** che operano **nei settori della sicurezza nazionale, pubblica sicurezza, difesa, contrasto, prevenzione, indagini, accertamento e perseguimento dei reati**.

In particolare, l'**Allegato I** alla Direttiva stabilisce i settori considerati "ad alta criticità", mentre l'**Allegato II** elenca i settori ritenuti "critici".

La Direttiva NIS 2 introduce requisiti più rigorosi per la cybersecurity e la gestione del rischio

L'articolo 21 della **Direttiva NIS 2** impone agli Stati membri di assicurare che le entità essenziali e rilevanti gestiscano il rischio implementando sistemi, politiche e migliori pratiche efficaci che abbraccino una vasta gamma di misure e discipline di sicurezza informatica, tra cui:

Obblighi

- Continuità operativa, come la gestione dei backup e il ripristino di emergenza.
- Pratiche di base per la cyber-igiene.
- Sicurezza della supply chain.
- Sicurezza delle risorse umane, policy di controllo degli accessi e gestione delle risorse.
- Accesso Zero Trust (autenticazione multi fattoriale, autenticazione continua).
- Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi.
- Tecnologie di crittografia e cifratura.

Evidenze documentali

- Organizzazione per la sicurezza informatica.
- Politiche di sicurezza informatica.
- Valutazione del rischio.
- Piano di trattamento del rischio.
- Piano di gestione delle vulnerabilità.
- Piano di adeguamento, ovvero un piano che identifichi gli interventi necessari ad assicurare l'attuazione delle misure di sicurezza.
- Piano di continuità operativa, di ripristino in caso di disastro e di gestione delle crisi.
- Piano di formazione.
- Piano per la gestione degli incidenti informatici.



“CYBER IGIENE” AI SENSI DELL’ARTICOLO 21 DELLA DIRETTIVA NIS 2

Le strategie di cyber-igiene costituiscono il fondamento per proteggere le infrastrutture dei sistemi informatici e di rete, comprendendo aspetti come hardware, software, sicurezza delle applicazioni online e dati aziendali o utenti finali. Queste strategie includono un insieme comune di pratiche di base, quali l'aggiornamento di software e hardware, la gestione delle password, la supervisione delle nuove installazioni, la limitazione degli account di accesso a livello amministrativo e la realizzazione di backup dei dati. Tale approccio proattivo crea un quadro solido per la preparazione e la sicurezza generale in caso di incidenti o minacce informatiche.

Sei un soggetto obbligato?

Se ritieni che la tua organizzazione possa essere coinvolta dalla Direttiva NIS 2, è essenziale agire subito. La normativa, recepita in Italia, coinvolgerà circa 50.000 nuovi soggetti. Tuttavia, non tutte le società di questi settori saranno automaticamente soggette agli obblighi: la Direttiva stabilisce criteri specifici, basati su dimensione e fatturato.

È importante sapere che, se sei un subappaltatore o fornitore, i tuoi clienti potrebbero chiederti di adeguarti alla **Direttiva NIS 2**, anche se al momento non rientri tra i soggetti obbligati. Preparati a conformarti a questa normativa, poiché i requisiti di sicurezza cibernetica si estendono anche a chi collabora con le organizzazioni critiche. Essere proattivi ora ti aiuterà a evitare sorprese in futuro.

Dal **18 ottobre 2024**, l'ACN ha messo a disposizione una piattaforma digitale per consentire la registrazione dei soggetti coinvolti. Le organizzazioni dovranno **“auto-registrarsi”** fornendo un elenco dettagliato delle proprie attività e dei servizi offerti. I dati richiesti includeranno informazioni sulla natura delle attività, il numero di dipendenti, il fatturato annuo, i contatti principali e le misure di sicurezza già in atto. Queste informazioni sono fondamentali per garantire una corretta attribuzione della categoria di rilevanza e per assicurare la conformità alle prescrizioni della **Direttiva NIS 2**.

La registrazione potrà essere effettuata nella finestra compresa tra il **1° gennaio e il 28 febbraio** di ogni anno quando si ritiene di rientrare tra i soggetti obbligati. L'Agenzia per la Cybersicurezza Nazionale valuterà la richiesta e comunicherà l'eventuale inserimento, mantenimento o rimozione dall'elenco dei soggetti essenziali o importanti.

Entro il 31 maggio di ogni anno è necessario procedere all'aggiornamento della propria posizione sulla piattaforma.

Resta comunque fondamentale mantenere i dati aggiornati e rispettare gli obblighi previsti, tra cui la valutazione periodica del rischio, l'adozione di misure di sicurezza adeguate e la notifica tempestiva di eventuali incidenti significativi.





Scadenze e Attività per l'Adeguamento alla Direttiva NIS 2



- **1 Gennaio - 28 Febbraio:**

- registrazione per i soggetti essenziali e Importanti**

I soggetti essenziali e importanti dovranno registrarsi sulla piattaforma NIS 2.

- Tutti i soggetti NIS già registrati nel 2025**

dovranno presentare una **nuova dichiarazione per l'anno 2026** tramite il **Portale dei Servizi ACN, confermando o aggiornando i dati** della precedente dichiarazione.

- **15 aprile - 31 maggio:**

- aggiornamento sul portale NIS 2**

I soggetti essenziali e importanti devono effettuare l'aggiornamento sulla piattaforma NIS. Tra il **15 aprile** e il **31 maggio 2026** è obbligatorio censire i fornitori rilevanti, sia:

Iato ICT coloro che forniscono servizi in ambito hardware e software (es. cloud, data center, reti, posta elettronica)

Iato non ICT coloro che forniscono beni o servizi ritenuti critici per la continuità operativa dell'organizzazione (es. materie prime, semilavorati, manutenzione macchinari)

Per ciascun fornitore devono essere indicati:

- denominazione
- codice fiscale
- paese della sede legale
- codici CPV
- criterio di rilevanza adottato

- **Categorizzazione delle attività e dei servizi**

- Dal 1° maggio al 30 giugno di ogni anno,**

i soggetti NIS devono comunicare e aggiornare, l'elenco delle attività e dei servizi, classificandoli secondo i criteri previsti.

In questa fase è necessario:

- elencare attività e servizi per macro-aree
- assegnare la classe di rilevanza (alto, medio, basso, minimo)
- svolgere una Business Impact Analysis (BIA) semplificata

- **Scadenze e obblighi di adeguamento**

Gli obblighi decorrono dalla data di comunicazione dell'ACN ai soggetti e sono:

Entro **gennaio 2026 - (9 mesi)** per gli obblighi di base in materia di **notifica di incidente**.

Entro **ottobre 2026 - (18 mesi)** per gli obblighi di base in materia di **sicurezza informatica**.

- **Scadenze e obblighi di adeguamento per i soggetti inseriti per la prima volta nel 2026**

Entro il **31 luglio 2027**: adozione delle misure di sicurezza.

Dal **1° gennaio 2027**: obbligo di notifica degli incidenti significativi.

Obblighi

A differenza della Direttiva originaria, i requisiti di cybersecurity della **Direttiva NIS 2** si applicano non solo alle organizzazioni che operano all'interno della sua definizione estesa di "critica" e ai loro dipendenti diretti, ma **anche ai subappaltatori e ai fornitori di servizi che collaborano con loro**.

Con l'adozione della Direttiva da parte degli Stati Membri, **le organizzazioni saranno tenute a conformarsi a rigorosi requisiti**, che possono essere categorizzati in cinque macro-aree:



governance



continuità operativa



presidio della catena di fornitura



segnalazione e gestione degli incidenti



misure per la gestione dei rischi per la cybersicurezza





GOVERNANCE

I vertici delle entità essenziali e rilevanti, come il Consiglio di Amministrazione, sono incaricati di approvare le misure di gestione dei rischi e possono essere considerati responsabili in caso di violazione. Parallelamente, gli organi di gestione sono tenuti a fornire formazione periodica ai propri dipendenti per trasmettere conoscenze e competenze adeguate.



CONTINUITÀ OPERATIVA

Nella gestione dei rischi secondo la Direttiva, si pone un'attenzione speciale sulla continuità dei servizi e la riduzione dell'impatto delle interruzioni, mediante misure come il backup, il ripristino in caso di disastro e la gestione delle crisi.



PRESIDIO DELLA CATENA DI FORNITURA

Un ulteriore aspetto cruciale riguarda la capacità delle organizzazioni di assicurare la sicurezza della propria catena di approvvigionamento, considerando le vulnerabilità specifiche dei fornitori diretti e dei fornitori di servizi, nonché le loro pratiche di sicurezza informatica.



SEGNALAZIONE E GESTIONE DEGLI INCIDENTI

Le entità essenziali o rilevanti sono tenute a segnalare agli specifici CSIRT o alle autorità nazionali competenti qualsiasi incidente che influisca in modo rilevante sulla fornitura dei loro servizi. Ai sensi dell'articolo 23, un incidente è considerato significativo se:

a. Soggetti importanti

- Perdita di riservatezza di dati digitali (totale o parziale).
- Perdita di integrità dei dati con impatto verso l'esterno.
- Violazione dei livelli di servizio attesi (SL – misura DE.CM-01).

b. Soggetti importanti

- **Perdita di riservatezza dei dati digitali (anche parziale, con impatto esterno).**
- **Perdita di integrità dei dati digitali (anche parziale, con impatto esterno).**
- **Violazione dei livelli di servizio attesi (SL – misura DE.CM-01).**
- **Accesso non autorizzato o abuso di privilegi su dati digitali sotto controllo (anche parziale).**



MISURE PER LA GESTIONE DEI RISCHI

La Direttiva NIS 2 impone l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate ai rischi di cybersecurity, seguendo un approccio multirischio. Queste misure includono:

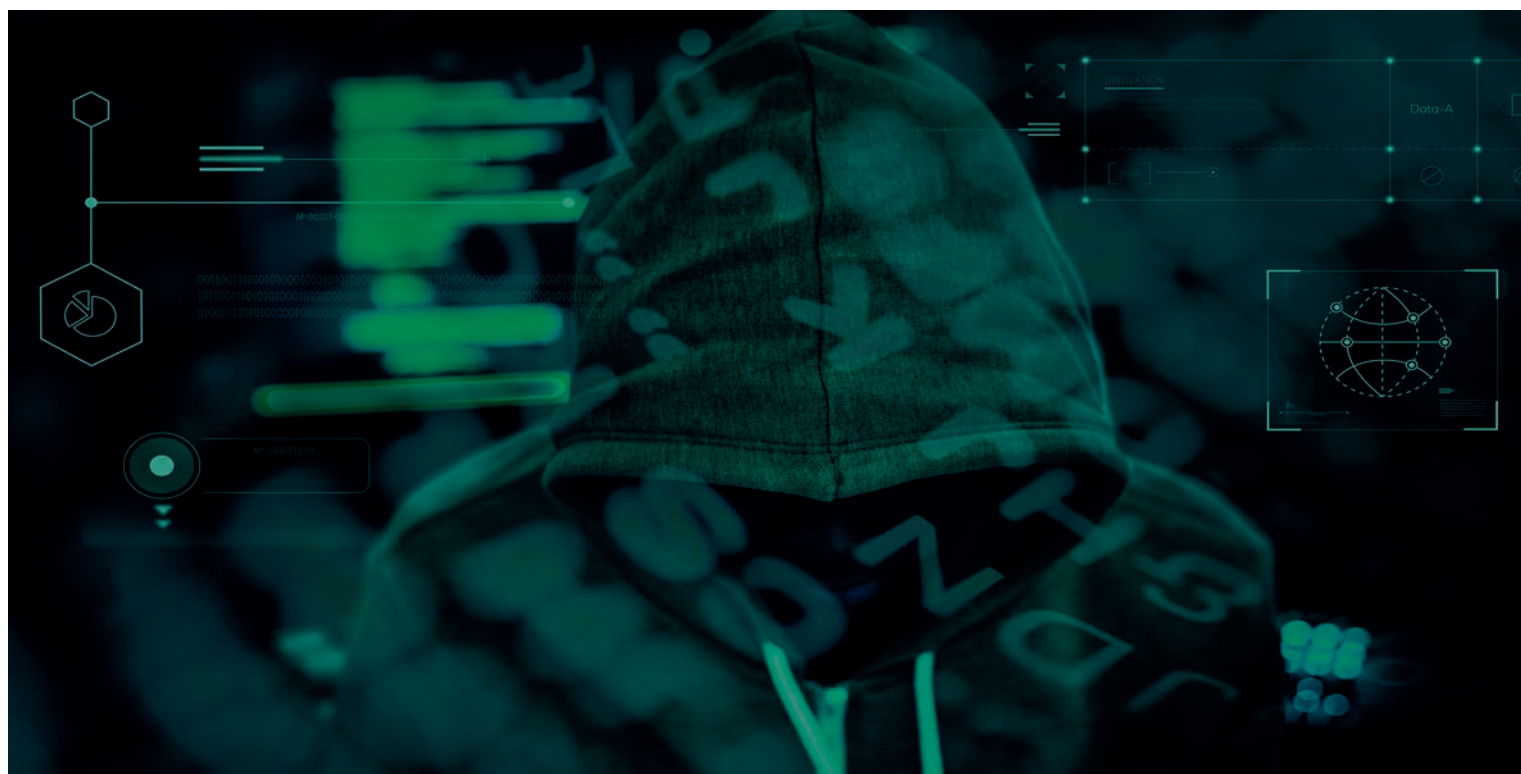
- L'autenticazione a più fattori.
- La crittografia.
- L'implementazione di pratiche di igiene informatica di base e di sviluppo sicuro.
- Il potenziamento della sicurezza delle risorse umane.
- L'adozione di strategie di controllo dell'accesso e di gestione degli attivi.

Segnalazione e gestione degli incidenti

La Direttiva NIS 2 introduce obblighi più rigidi per la reportistica sugli incidenti

Le entità critiche devono ora:

- Dare notifica iniziale di un incidente di sicurezza significativo entro 24 ore dal rilevamento.
- Fornire una valutazione iniziale dell'incidente entro 72 ore dal rilevamento.
- Creare un report finale dettagliato entro un mese dal rilevamento.



Sanzioni

La Direttiva NIS 2 impone sanzioni onerose

I criteri adottati per stabilire l'importo delle sanzioni rispecchia quello di altre normative europee come, ad esempio, il Regolamento Europeo per la Protezione dei Dati Personali (GDPR):

- In caso di non conformità rispetto all'adozione delle misure di gestione dei rischi di cybersicurezza e/o agli obblighi di segnalazione degli incidenti, i soggetti essenziali possono incorrere in sanzioni "pari a un massimo di almeno 10 000 000 EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo."
- Per le medesime violazioni, i soggetti importanti possono incorrere in sanzioni "pari a un massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo."



Via Brandizzo, 20
10099 San Mauro T.se (TO), Italia

Telefono: (+39) 011 22 38 774

Fax: (+39) 011 27 30 938