Nuova normativa NIS 2 per la sicurezza informatica

Dal 16 ottobre 2024 è in vigore la nuova normativa Network and Information Security (direttiva NIS) di derivazione europea, recepita con il dlgs 138/2024.

La sicurezza informatica è un obiettivo fondamentale dell'Unione europea, che sta proseguendo la sua azione per elevare il livello di cybersecurity nel suo complesso.

L'UE sta proseguendo, e intensificando, un percorso normativo a sostegno della sicurezza comune, adottando una serie di misure per ridurre le vulnerabilità e aumentare la resilienza dei soggetti critici, sia per quanto riguarda i rischi informatici che quelli non informatici. In particolare, sono state adottate importanti misure per sviluppare mezzi e capacità di prevenzione, individuazione e risposta rapida alle sempre più numerose minacce cyber e per favorire la sinergia tra gli operatori del settore pubblico e privato in un'azione condivisa verso un obiettivo comune.

La Direttiva NIS2 (Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla sicurezza delle reti e delle informazioni, l'acronimo NIS sta per Network and Information Security) è entrata in vigore il 17 gennaio 2023, rappresentando un passo significativo nella definizione della strategia dell'UE per la cybersecurity.

La NIS2 intende eliminare divergenze nell'attuazione della normativa tra gli Stati membri, promuovendo un quadro normativo più uniforme e coordinato, anche grazie a una maggiore cooperazione tra gli Stati e all'aggiornamento dell'elenco dei settori e delle attività soggetti agli obblighi in materia di cybersecurity.

Tale Direttiva detta disposizioni di rilevante impatto per le imprese in merito all'adozione di misure per gestire i rischi connessi alla sicurezza dei sistemi informatici e delle reti.

Sulla G.U. del 1° ottobre 2024 è stato pubblicato il D.Lgs. n. 138/2024, che ha recepito la Direttiva (UE) 2022/2555, recante misure per un livello comune elevato di cybersicurezza nell'Unione europea (c.d. "Direttiva NIS2").

La Direttiva NIS2 è entrata in vigore in Italia il 18 ottobre 2024. Nel frattempo, gli operatori di servizi essenziali e digitali rimangono soggetti alla Direttiva NIS già in vigore dal 2016.

La Direttiva NIS2 ha quindi come obiettivo quello di rafforzare la sicurezza delle reti e dei sistemi informativi, migliorando la resilienza delle infrastrutture critiche e la capacità di risposta a incidenti informatici.

Gli attori interessati dovranno prepararsi e allineare le loro organizzazioni e i loro processi ai nuovi obblighi di sicurezza.

La direttiva essenzialmente impone agli enti pubblici e alle imprese di adottare misure di sicurezza specifiche, di notificare di incidenti e di collaborare con le autorità competenti.

La NIS2 si applica, in via prioritaria, alle organizzazioni di medie e grandi dimensioni, con esclusione delle imprese con meno di 50 dipendenti o un fatturato annuo inferiore a 10 milioni di euro, a meno che non siano ritenute di importanza critica per la società e, in tal caso, dovranno soddisfare requisiti e misure di vigilanza più severe.

La piccola impresa potrebbe essere interessata anche in quanto elemento della catena di approvvigionamento di soggetti essenziali o importanti.

AMBITO DI APPLICAZIONE

Il d.lgs. n. 138/2024 (decreto NIS) indica all'articolo 3 il suo ambito di applicazione. In particolare, vi rientrano i soggetti pubblici e privati delle tipologie di cui agli allegati I, II, III e IV, che sono sottoposti alla giurisdizione nazionale.

Nell'allegato I del decreto sono elencati i settori altamente critici.

Nell'allegato II sono elencati gli altri settori critici.

Nell'allegato III sono elencate le categorie di pubbliche amministrazioni alle quali si applica il decreto.

Nell'allegato IV sono elencate le ulteriori tipologie di sog-

Finanza agevolata ed innovazione
Francesco Angeletti
Tel. 071 29048218

getti a cui si applica il decreto a seguito di identificazione governativa.

La maggior parte dei soggetti pubblici e privati rientrano nell'ambito di applicazione sulla base dei criteri (dimensioni e tipologia di soggetto) stabiliti dal decreto, mentre un numero limitato di ulteriori soggetti può essere inserito nell'ambito di applicazione in esito all'identificazione da parte dell'Autorità nazionale competente NIS, su proposta delle Autorità di settore competenti.

A seconda del livello di criticità intrinseca dei settori e delle tipologie di soggetti in relazione al rischio informatico, **i soggetti poi sono distinti tra "essenziali" e "importanti".** Tale distinzione è utile **ai fini dell'applicazione proporzionale degli obblighi** nonché dell'esercizio dei poteri ispettivi e sanzionatori dell'Autorità nazionale competente NIS.

I **soggetti essenziali** sono enti e organizzazioni che operano in settori considerati critici per il funzionamento della società e dell'economia. La loro interruzione avrebbe un impatto significativo sulla sicurezza, sull'economia, sulla salute pubblica o sulla società in generale.

Sono soggette a requisiti normativi più rigorosi per il monitoraggio della conformità, obblighi di segnalazione degli incidenti e misure di applicazione dei sistemi informativi.

Per i settori riportati nella norma, le grandi e medie imprese sono da considerarsi come essenziali o importanti. Le Piccole e micro imprese non dovrebbero rientrare (a meno che ACN non le individui in modo specifico come essenziali o importanti).

Scopri gli ambiti di applicazione suddivisi in base ai settori, sottosettori o tipologie di soggetti.

https://www.acn.gov.it/portale/documents/d/guest/faq-1-5_dettaglio-ambiti-di-applicazione

SETTORE DELLA FABBRICAZIONE

Per quanto riguarda in particolare il settore della **fabbricazione**, sono inclusi:

- Fabbricazione di dispositivi medici e di dispositivi medico diagnostici in vitro
- Fabbricazione di computer e prodotti di elettronica e ottica (Imprese che svolgono attività economiche di cui alla sezione C, divisione 26, della NACE Rev. 2)
- Fabbricazione di apparecchiature elettriche (Imprese che svolgono attività economiche di cui alla sezione C, divisione 27, della NACE Rev. 2)
- Fabbricazione di macchinari e apparecchiature n.c.a. (Imprese che svolgono attività economiche di cui alla sezione C, divisione 28, della NACE)
- Fabbricazione di autoveicoli, rimorchi e semirimorchi (Imprese che svolgono attività economiche di cui alla sezione C, divisione 29, della NACE Rev. 2)
- Fabbricazione di altri mezzi di trasporto (Imprese che svolgono attività economiche di cui alla sezione C, divisione 30, della NACE Rev. 2)

PICCOLE IMPRESE

In linea generale, salvo specifiche eccezioni, le organizzazioni che non superano i massimali per le categorie delle micro e piccole imprese, ai sensi della Raccomandazione 2003/361, non rientrano nell'ambito di applicazione del decreto legislativo 134/2024 (cd. decreto NIS). Tuttavia, tenuto conto della specificità di alcune tipologie di soggetto, sono ricomprese nell'ambito di applicazione le organizzazioni assimilabili a micro e piccole imprese le cui attività sono riconducibili a:

[ex articolo 3, comma 5, lettera b] fornitori di reti pubbliche di comunicazione elettronica;

[ex articolo 3, comma 5, lettera b] fornitori di servizi di comunicazione elettronica accessibili al pubblico;

[ex articolo 3, comma 5, lettera c] prestatori di servizi fiduciari;

[ex articolo 3, comma 5, lettera d] gestori di registri dei nomi di dominio di primo livello;

[ex articolo 3, comma 5, lettera d] fornitori di servizi di sistema dei nomi di dominio;

[ex articolo 3, comma 5, lettera e] fornitori di servizi di registrazione dei nomi di dominio.

Infine, rimane ferma la facoltà per l'Autorità nazionale competente NIS, su proposta delle Autorità di settore interessate, di individuare anche piccole e micro-imprese che operano nei settori, sotto-settori o che svolgono attività riconducibili alle tipologie di soggetto di cui agli allegati I, II, III e IV, del decreto NIS (ex. articolo 9), quali soggetti importanti o essenziali. In tal caso, queste organizzazioni

riceveranno una notifica al proprio domicilio digitale (ex. articolo 3, comma 13, del decreto NIS).

Da notare infine che la norma pone in capo ai soggetti destinatari un obbligo di valutazione in termini di sicurezza della **catena di approvvigionamento**, compresi gli aspetti riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori. Di conseguenza, anche i soggetti non direttamente interessati dall'applicazione della NIS 2 dovranno attivarsi e adottare misure idonee a garantire ai loro clienti un livello di sicurezza adeguato.

ATTUAZIONE DELLA NORMA

ACN coordina l'attuazione della nuova normativa in qualità di Autorità nazionale competente NIS. Per garantire un'implementazione efficace, sono previste alcune tappe fondamentali.

La prima è la registrazione tramite il portale dei servizi (https://portale.acn.gov.it/login) dell'Agenzia per la cybersicurezza nazionale, da parte delle organizzazioni pubbliche o private che possiedono i requisiti specifici previsti dalla normativa NIS.

La registrazione avviene:

entro il 17 gennaio 2025: per i soggetti di cui all'articolo 42, comma 1, lettera a), tra cui i fornitori di cloud computing, data center, servizi (anche di sicurezza) gestiti e mercati online;

entro il 28 febbraio 2025: per tutti gli altri soggetti inclusi nell'ambito di applicazione del decreto.

La registrazione è funzionale a consentire ad ACN di censire i soggetti operanti nei settori NIS, anche al fine di fornire loro supporto in fase di implementazione degli obblighi, attraverso le articolate attività di monitoraggio e ausilio nel loro percorso condiviso di crescita. Sul sito dell'ACN sono disponibili le informazioni relative ai settori e sottosettori inclusi nel mondo NIS e le modalità per determinare se un'organizzazione è "essenziale" o "importante".

L'Agenzia, entro metà aprile, notificherà a tutti i soggetti registrati se sono stati inseriti, o meno, nell'elenco dei soggetti NIS e pubblicherà gli obblighi di base in materia di notifica di incidenti e di misure di sicurezza informatica.

I soggetti NIS dovranno:

- **a partire da gennaio 2026,** notificare gli incidenti;
- **entro ottobre 2026**, completare le misure di sicurezza informatica di base.

Prepararsi per tempo è fondamentale per gestire con successo l'implementazione della nuova normativa volta ad aumentare la sicurezza informatica delle reti e dei sistemi informativi dei soggetti NIS.

Tappe fondamentali per le Aziende

- Assessment iniziale: Tutte le aziende dovrebbero svolgere un assessment per valutare se rientrano negli obblighi della direttiva NIS2, verificando i requisiti di sicurezza informatica applicabili
- Nomina di un Punto di Contatto: Prima della registrazione le aziende identificate come soggetti essenziali devono nominare un responsabile interno per la conformità;
- Registrazione sulla piattaforma ACN entro il 28 febbraio 2025 per le aziende che risultano soggette alla direttiva
- Obbligo di notifica degli incidenti: Dal 1° gennaio 2026.
- Adempimenti amministrativi ed applicazione delle necessarie misure di sicurezza: Entro il 1° ottobre 2026

OBBLIGHI DERIVATI DALLA NIS2

I soggetti destinatari dovranno adottare misure tecniche, organizzative e operative adeguate e proporzionate alla tipologia specifica di attività svolta e idonee a ridurre il rischio di incidenti.

L'approccio indicato richiede l'implementazione di politiche aziendali di analisi del rischio e l'adozione di presidi tecnici ma anche organizzativi idonei a ridurre il rischio.

Governance

Se analizziamo un incidente ci accorgiamo che, nella maggior parte dei casi, questo si verifica a causa di misure di sicurezza inadeguate, anche fondamentali, prima che da fattori esterni.

Questo è dovuto soprattutto ad una scarsa percezione della criticità dei rischi cyber da parte del Management che ne demanda la gestione alla Direzione IT nell'ambito del budget assegnato.

La Direttiva NIS2 interviene su questo problema in modo molto diretto, coinvolgendo esplicitamente l'organo di gestione (ad esempio, il consiglio d'amministrazione) nella governance del rischio di cyber security, attribuendogli delle responsabilità specifiche.

Art. 20 NIS2 - Gli Organi di amministrazione e direttivi dei Soggetti Essenziali e Importanti:

- Approvano le modalità di implementazione delle misure di sicurezza
- Sovrintendono all'implementazione degli obblighi
- Sono responsabili delle eventuali violazioni
- Sono tenuti a seguire una formazione in materia di cybersicurezza
- Promuovono la formazione dei propri dipendenti

La NIS2 impone l'obbligo formativo sulla popolazione aziendale e sui soggetti dirigenziali sui temi della sicurezza informatica. Il phishing e il fattore umano rappresentano oggi uno dei rischi più elevato per le aziende.

Una strategia di sicurezza aziendale efficace dovrebbe prevedere la formazione dei dipendenti su argomenti come ad esempio:

- Phishing
- Password Security
- Social Engineering
- Malware
- Removable Media
- Physical Security
- Working Remotely
- Mobile Security
- Safe Web Browsing
- UsoMFA e crittografia

Risk Assessment

Art. 21 NIS2 - Le misure di gestione dei rischi di cibersicurezza sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete da incidenti e comprendono almeno gli elementi seguenti:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;

b) gestione degli incidenti;

c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;

h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;

j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

Un primo passo consiste nell'analisi degli impatti delle predette novità normative sul business e sui processi aziendali, mediante la conduzione di attività di risk assessment, volte a valutare i profili di rischio e le vulnerabilità dei sistemi informatici. Alla luce degli esiti delle attività di mappatura e valutazione dei rischi, è opportuno procedere all'adozione e alla concreta implementazione di presidi di prevenzione e controllo, integrando le procedure.

L'approccio "multirischio" da seguire non si limita a un singolo rischio (ad esempio, un attacco informatico), ma considera l'intera gamma di minacce che possono compromettere i sistemi e le reti, incluse minacce fisiche, digitali, naturali e accidentali.

Occorre combinare misure tecniche, operative, organizzative e procedurali per affrontare i rischi in maniera coordinata e integrata.

Deve prevedere che i rischi sono in continua evoluzione e richiede aggiornamenti regolari alle valutazioni e alle misure di sicurezza.

Le misure per prevenire o ridurre al minimo l'impatto degli incidenti devono:

- Assicurare un livello di sicurezza dei sistemi informativi e di reti adeguato ai rischi esistenti e, dove applicabile, pertinenti alle norme nazionali, europee e internazionali
- Essere proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti e alla loro gravità

La gestione degli incidenti

La gestione del rischio non potrà prescindere dalla gestione degli incidenti, con l'adozione di policy aziendali finalizzate a ridurre i rischi di incidenti ma anche a porvi rimedio in tempi rapidi qualora si verifichino, al fine di ridurne l'impatto e garantire la continuità aziendale e quindi del servizio fornito.

I soggetti destinatari dovranno inoltre dotarsi di procedure per la notifica degli incidenti nei tempi indicati assai stretti indicati dal D.lgs. 138/2024.

Art. 23 NIS2: Obbligo di segnalazione di incidenti "significativi" al CSIRT

Un incidente è considerato significativo se:

- Ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
- Si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Business Continuity

La Business Continuity si riferisce alla capacità di un'organizzazione di continuare a operare e fornire i propri servizi critici anche durante o dopo eventi imprevisti, come cyberattacchi, disastri naturali o guasti tecnologici.

La definizione di un Business Continuity Plan deve essere allineato con le strategie del business e l'evoluzione IT richiede un complessivo insieme di processi, policies e informazioni documentate.

E' necessario valutare le possibili strategie da adottare per una corretta continuità operativa dell'azienda, in primis, è necessario mappare i processi critici, come ad esempio:

- Clienti e partner;
- Servizi e prodotti;
- Le catene di logistica;
- Le catene di fornitura e servizi;
- Le risorse umane per la continuità del business;
- Le risorse economiche e finanziarie necessarie per la Business Continuity;
- Le risorse IT e di telecomunicazione fondamentali;
- Le infrastrutture fisiche fondamentali e le necessità energetiche necessarie;
- I rischi di compliance e legali che possano porre l'azienda in situazioni di difficoltà

Un Business Continuity Plan per essere efficace va testato regolarmente e ne vanno valutati i possibili miglioramenti in situazioni di normalità al fine di verificarne il regolare funzionamento.

Third Parties Management

La Direttiva NIS2 rende obbligatoria la gestione del rischio lungo la supply chain.

Occorre quindi definire una strategia per la gestione del rischio di terze parti ICT e analizzare e revisionare i contratti con le terze parti esistenti e rilevanti, utilizzando un approccio Risk Based.

Perché valutare i rischi dei fornitori?

- Minimizzare i rischi di attacchi alla supply chain.
- Garantire la conformità alla NIS2 e prevenire data breach e sanzioni.
- Proteggere la continuità operativa.
- Preservare la reputazione aziendale da incidenti informatici

Quali fornitori dobbiamo controllare?

Per individuare le catene di approvvigionamento che dovrebbero essere monitorati e valutati, occorre (oltre ad un analisi dei processi) considerare i seguenti criteri:

- In che misura i soggetti essenziali e importanti ricorrono e si affidano a specifici servizi TIC (tecnologie dell'informazione e della comunicazione)

- La pertinenza di questi servizi/sistemi/prodotti per lo svolgimenti di funzioni critiche o sensibili, compreso il trattamento di dati personali
- La disponibilità di servizi alternativi
- La resilienza dell'intera catena di approvvigionamento di tali servizi durante il loro ciclo di vita e la loro importanza futura per le attività dei soggetti.

Che misure di tutela si devono adottare per la catena di fornitura?

- Identificazione dei rischi legati alla supply chain, mappare i propri fornitori critici (compresi i subfornitori) e comprendere i rischi a cui potrebbero essere esposte attraverso la loro interazione con questi attori esterni.
- Effettuare un analisi del rischio verso i fornitori
- Utilizzo dei contratti per rispettare gli obiettivi del piano di gestione del rischio della supply chain. Definire obblighi di sicurezza nei contratti, prevedendo la possibilità di effettuare audit ed exit strategies in caso di non adempimento (per evitare il lock-in tecnologico)
- Effettuare verifiche e audit verso i forntori
- Pianificazione e verifica della risposta e di piani di ripristino insieme ai fornitori
- Differenziare ove possibile la fornitura

Le sanzioni

L'Agenzia per la cybersicurezza nazionale (ACN) ha poteri ispettivi e di verifica nei confronti dei soggetti destinatari e può sottoporre questi ultimi a verifiche della documentazione e delle informazioni trasmesse, ispezioni in loco e a distanza, richieste di accesso a documenti, dati e altre informazioni ritenute rilevanti.

All'ACN è affidata l'erogazione di sanzioni che possono essere pecuniare ma anche interdittive.

I soggetti essenziali (escluse le PA) sono punti con sanzioni pecuniarie fino a un massimo di 10 milioni di € o del 2% del fatturato annuo mondiale relativo all'esercizio precedente.

I soggetti importanti (escluse le PA) sono puniti con sanzioni pecuniarie fino a un massimo di 7 milioni di € o del 1,4% del fatturato annuo mondiale relativo all'esercizio precedente.

Si ritengono poi particolarmente rilevanti le sanzioni a carico degli organi direttivi.

Gli artt. 23 e 39 del D.Lgs. 138/2024 prevedono che gli organi di amministrazione e gli organi direttivi assicurano il rispetto delle disposizioni del decreto e sono responsabili delle violazioni del decreto da parte del soggetto di cui hanno la rappresentanza.

Nei loro confronti l'ACN può erogare la sanzioni amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto.