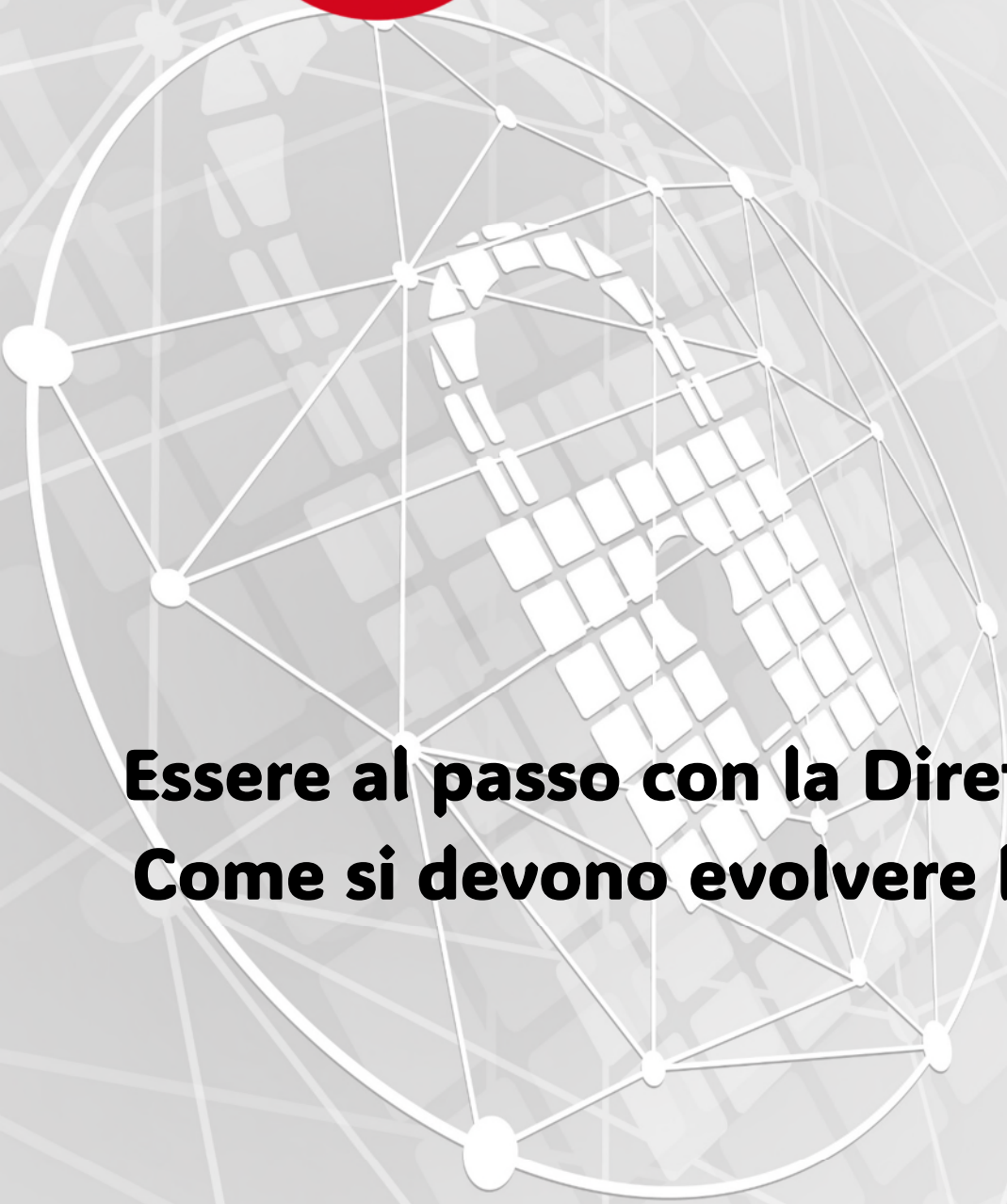
cyberto

Your cybersecurity partner



Essere al passo con la Direttiva NIS2: Come si devono evolvere le Aziende

www.cyberto.it

Socio Clusit
Associazione Italiana per la Sicurezza Informatica

Premessa: NIS2 Obbligo o Opportunità per le aziende?

La direttiva europea **NIS2**, o **Network and Information Security Directive 2**, rappresenta un importante quadro normativo per garantire la sicurezza delle reti e dei sistemi informativi nell'Unione Europea. Questa direttiva mira a migliorare la capacità di gestione delle minacce cibernetiche, promuovendo la collaborazione tra Stati membri dell'Unione e settori chiave per proteggere le infrastrutture digitali critiche di tutti i paesi.

Con il recepimento imminente da parte degli Stati Membri entro il **17 ottobre 2024**, i soggetti coinvolti saranno tenuti ad aderire ai requisiti relativi alla governance, alla continuità operativa, al controllo della catena di approvvigionamento, alla segnalazione degli incidenti e, in generale, alla gestione dei rischi. Pensata in risposta a vari attacchi informatici ampiamente noti e dannosi, la Direttiva NIS2 rafforza i requisiti di sicurezza, semplifica gli obblighi di segnalazione e introduce misure di supervisione più rigorose e requisiti di applicazione più severi. Per imprenditori, CEO e esperti informatici,

Tutti i 27 Stati membri dell'UE sono tenuti a ratificare la Direttiva NIS2 entro il 17 ottobre 2024.

È stato appena pubblicato in Gazzetta Ufficiale l'attesissimo decreto legislativo (del 4 settembre 2024, n. 138) di recepimento in Italia della **Direttiva NIS2**, il quale mira a garantire l'aumento del livello di sicurezza informatica del tessuto produttivo e delle Pubbliche Amministrazioni del Paese, in armonia con gli altri Stati membri dell'Unione Europea.

Quali sono realmente gli obblighi a cui gli attori privati e pubblici dovranno adempiere e in quali relativi termini?

La **Direttiva NIS2** 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.

Cosa fare per adeguarsi alla Direttiva NIS2

Innanzitutto, l'art. 21 definisce al paragrafo 1 che i soggetti obbligati dovranno adottare misure **tecniche, operative e organizzative adeguate** e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e delle reti che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Vediamo quindi di entrare un po' più nel pratico indicando quali potrebbero essere gli **step fondamentali** da seguire.

A chi si rivolge la NIS2: Ambito di Applicazione

La portata di applicazione della NIS2 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" pubblici o privati**. Si concentra su tutti i soggetti in base anche alle loro dimensioni, al loro impatto e al loro settore (vedere art.3) includendo tutte le Grandi Imprese e le Medie Imprese. Inoltre, occorre identificare se si rientra fra le tipologie di soggetti essenziali e importanti, ovvero quelli che svolgono **attività fondamentali per il funzionamento** della società o dell'economia.

Vengono dunque escluse nell'ambito di applicazione della Direttiva, con qualche eccezione, solamente alcune piccole imprese e le microimprese

GRANDE IMPRESA

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 grandi imprese, definite come quelle con più di 250 dipendenti e un fatturato annuo superiore a 50 milioni di euro e un bilancio superiore ai 43 milioni di euro o le imprese che superano i massimali delle medie imprese nei settori specificati negli allegati I e II della Direttiva.

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 e un bilancio inferiore ai 43 milioni di euro.

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.

Schema degli ambiti di applicazione

* Possibile identificazione governativa come essenziali

** Possibile identificazione governativa come importanti o essenziali

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia	19 tipologie di soggetto	Essenziali	Importanti *	Fuori ambito **
Trasporti	10 tipologie di soggetto			
Settore bancario	DORA Lex specialis			
Infrastrutture dei mercati finanziari				
Settore sanitario	5 tipologie di soggetto			
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto		Importanti *	Fuori ambito **
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto	Importanti *		Fuori ambito **
Gestione dei rifiuti	1 tipologia di soggetto			
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto			
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto			
Fabbricazione	6 tipologie di soggetto			
Fornitori di servizi digitali	4 tipologie di soggetto			
Ricerca	2 tipologie di soggetto	Importanti *		Fuori ambito **
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale	4 categorie di PA	Essenziali		
Pubblica Amministrazione regionale e locale	11 categorie di PA	Importanti *		
Ulteriori tipologie di soggetti	4 tipologie di soggetti	Identificazione governativa		

SUPPLY CHAIN (la catena d'approvvigionamento)

La direttiva NIS2 di fatto coinvolgerà tutti i fornitori che interagiscono con reti, sistemi e servizi ICT dei soggetti in scope, in virtù dei requisiti che la direttiva impone per l'adozione di misure di sicurezza della catena dell'approvvigionamento, che porteranno a verifiche sulla security in base al principio di responsabilità e adeguatezza.

Il criterio della dimensione non si applica alle Pubbliche Amministrazioni. Infatti, **sono soggette agli obblighi della NIS2 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 Direttiva NIS2 gli enti della pubblica amministrazione che operano nei settori della sicurezza nazionale, pubblica sicurezza, difesa, contrasto, prevenzione, indagini, accertamento e perseguimento dei reati.**

La Direttiva NIS2 introduce requisiti di cybersecurity e la gestione del rischio

L'articolo 21 della Direttiva NIS2 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:

- politiche di **analisi dei rischi** e di **sicurezza dei sistemi informatici**;
- gestione e **reportistica degli incidenti**;
- **continuità operativa, gestione del backup** ripristino in caso di evento disastroso;
- **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;
- **sicurezza dell'acquisizione**, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
- strategie e procedure per valutare l'efficacia delle misure di **gestione dei rischi** di sicurezza informatica;
- **best practices di igiene informatica** di base e formazione in materia di sicurezza informatica;
- policy e procedure relative **all'uso della crittografia** e, se del caso, della anonimizzazione o pseudomizzazione;
- **sicurezza delle risorse** umane, strategie di **controllo dell'accesso** e gestione dei varchi attivi;
- 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.

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.

Obblighi

A differenza della Direttiva originaria, i requisiti di cybersecurity della **Direttiva NIS2** si applicano non solo alle organizzazioni che operano all'interno della sua definizione estesa di "critica" e ai loro fornitori 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 confrontarsi a rigorosi requisiti**, che possono essere categorizzati in cinque macro-aree:

Governance

Continuità Operativa

Presidio della catena di fornitura

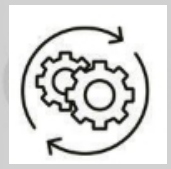
Segnalazione e gestione degli incidenti

Misure per la gestione dei rischi per la cybersecurity

GOVERNANCE

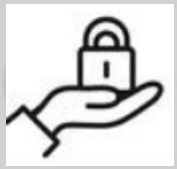
I vertici delle entità essenziali e rilevanti, come il Consiglio di

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.



CONTINUITA 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. "Influisce o può influire su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli."

b. "Provoca o può provocare una grave interruzione operativa dei servizi o perdite finanziarie significative per il soggetto coinvolto."

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:

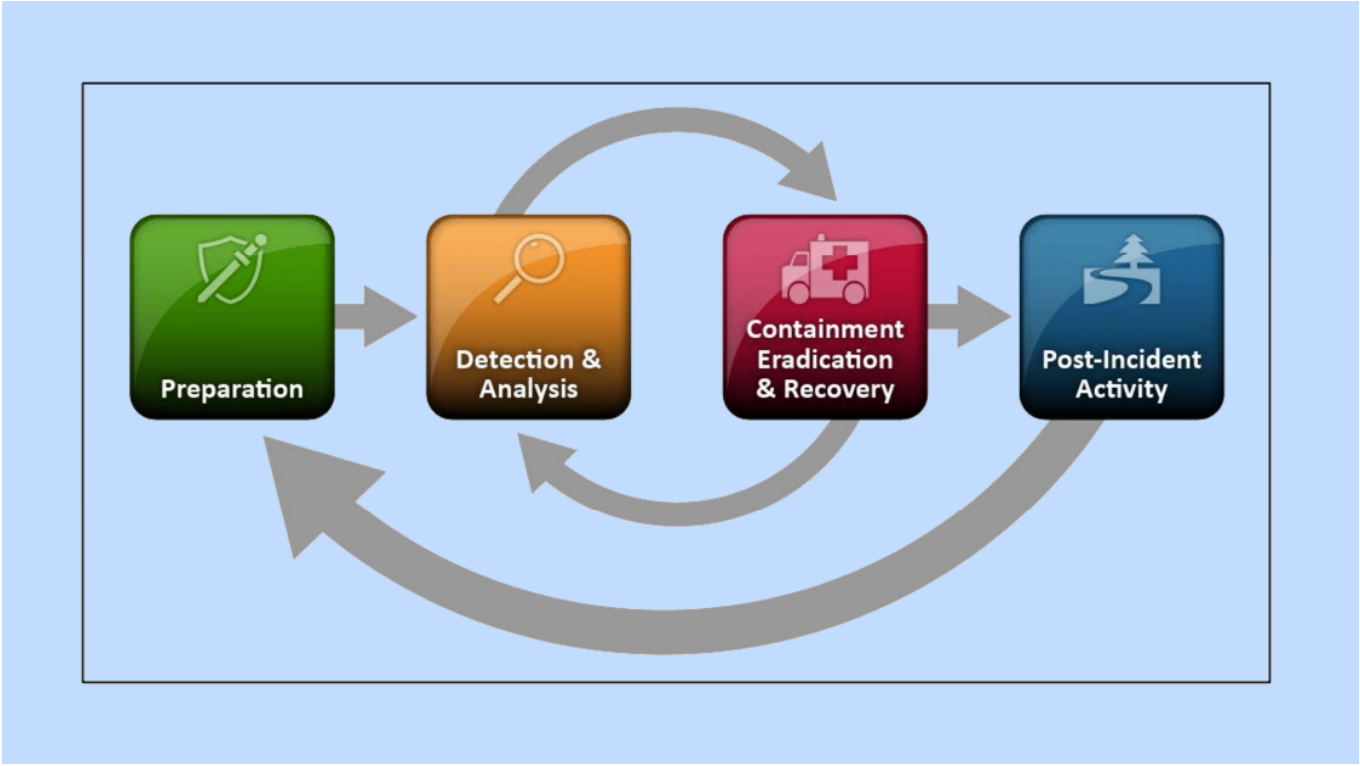
- L'autenticazione a più fattori.
- La crittografia.
- L'implementazione di pratiche di igiene informatica di base e di sviluppo sicuro.
- Il potenziamento della sicurezza delle risorse umane.
- L'adozione di strategie di controllo dell'accesso e di gestione degli attivi.

Segnalazione e gestione degli incidenti

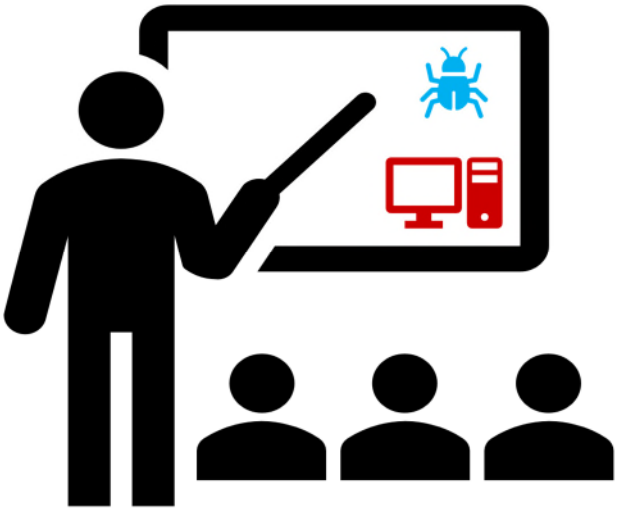
Molto importante è anche definire un **Data Breach Recovery Plan**.

La normativa prevede che, in caso di incidente significativo, si debba rispettare un **iter di notifica** alle autorità competenti organizzato in più fasi, il quale iter prevede la trasmissione di:

1. **un preallarme entro 24 ore** da quando si è venuti a conoscenza dell'incidente;
2. **una notifica entro 72 ore** dalla conoscenza dell'incidente, che aggiorni – se necessario – le informazioni del preallarme;
3. **una relazione finale** entro un mese dalla trasmissione della notifica, il cui contenuto minimo sarà dettagliato dal legislatore dello stato membro in fase di recepimento.



In quali sanzioni s'incorre



La Direttiva NIS è stata creata con l'obiettivo di migliorare la sicurezza informatica nell'Unione Europea e non quindi per rimpinguare le casse pubbliche o per aggiungere altra burocrazia. Le **sanzioni** possono essere di natura **amministrativa** o **penale.** Un "listino" preciso delle sanzioni non c'è nel testo della Direttiva NIS2 (vedi Art.50), in quanto lascia agli Stati Membri la facoltà di legiferare in materia adattando il regime sanzionatorio alla propria legislazione.

Già la mancata registrazione all'ACN è una violazione assistita da una sanzione amministrativa pecuniaria con un importo fino al 0.1% del fatturato annuo su scala mondiale del soggetto.

La Direttiva prevede comunque dei **limiti massimi** in funzione del fatto che un operatore sia qualificato come essenziale o come **importante**.

Gli operatori essenziali potranno essere sottoposti a sanzioni pecuniarie amministrative pari a un massimo di **10 Milioni di €uro o il 2% del totale** del fatturato mondiale globale.

Gli **operatori importanti**, invece, potranno essere soggetti a sanzioni pari a un massimo di **7 Milioni di €uro** o a fino ad un massimo del **1,4 % del totale del fatturato** mondiale globale.

Le misure che possono essere adottate già da oggi includono:

1. **Verificare se la propria Organizzazione rientri già nel perimetro** di applicabilità della Direttiva Lo si fa con la registrazione sul portale dell'ACN;

2. **Valutare il proprio livello di conformità attuale** rispetto ai requisiti esplicitati nel testo della Direttiva;

3. **Identificare eventuali lacune** e pianificare i necessari interventi migliorativi;

4. **Informare il personale competente**, inclusi gli organi di gestione, sugli obblighi imposti dalla Direttiva e sulle azioni di adeguamento pianificate dall'Organizzazione.

Prepararsi alla Direttiva NIS2: quali sono i termini degli obblighi discendenti dal decreto di recepimento

Alla luce di ciò, appare opportuno sintetizzare i principali adempimenti derivanti dal decreto, ordinandoli per data.

In particolare, preliminarmente occorre sapere che:

- **entro il 31 dicembre 2024**, aziende e pubbliche amministrazioni dovranno svolgere un assessment per comprendere se siano o meno soggette agli obblighi della Direttiva NIS2, seguendo il dettato degli artt. 6 e 7, degli Allegati I, II, III e IV, nonché di ogni altro atto che verrà emanato;

- **tra il 1° gennaio e il 28 febbraio 2025**, i soggetti privati e pubblici – che a seguito dell'assessment ritengano di rientrare nell'ambito di applicazione del decreto – dovranno registrarsi sulla piattaforma digitale resa disponibile da ACN fornendo le informazioni richieste dalla normativa.

- **entro il 17 gennaio 2025**, dovranno registrarsi sulla piattaforma i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network;

- **entro il 31 marzo 2025**, l'ACN redigerà l'elenco dei soggetti essenziali e dei soggetti importanti sulla base delle registrazioni ricevute attraverso la piattaforma;

- **tra il 1° aprile 2025 e il 15 aprile 2025**, attraverso la piattaforma, l'ACN comunicherà ai soggetti registrati l'inserimento nell'elenco dei soggetti essenziali o importanti;

- **entro il 15 aprile 2025**, i soggetti che avranno ricevuto la comunicazione dovranno nominare con un apposito atto un soggetto che abbia la responsabilità dell'adempimento degli obblighi del decreto;

- **tra il 15 aprile e il 31 maggio 2025**, i soggetti che avranno ricevuto la comunicazione attraverso la piattaforma dovranno fornire le ulteriori informazioni richieste dalla normativa.

Chiusa questa fase preliminare, le aziende e le pubbliche amministrazioni che avranno ricevuto la comunicazione di inclusione da parte dell'ACN dovranno procedere con gli ulteriori adempimenti previsti nel decreto. A tal proposito, a titolo esemplificativo:

- **a partire dal 1° gennaio 2026**, si dovrà adempiere all'obbligo di notifica degli incidenti;

- **entro il 1° ottobre 2026**, si dovrà adempiere:

  - agli obblighi degli organi di amministrazione e direttivi;
  - agli obblighi in materia di misure di sicurezza;
  - all'obbligo di raccolta e mantenimento di una banca dei dati di registrazione dei nomi di dominio, laddove applicabile.

Recepimento e attuazione

Recepimento e attuazione

FEBBRAIO 23 - METÀ OTTOBRE 24

Recepimento

Avvio di alcuni tavoli settoriali
7 agosto 2024: adozione definitiva in CDM
1° ottobre 2024: pubblicazione in Gazzetta Ufficiale
16 ottobre 2024: entrata in vigore

METÀ OTTOBRE 24 – METÀ APRILE 25

Prima fase attuativa

Avvio formale di tutti i tavoli settoriali
Entro febbraio 2025: censimento e registrazione dei soggetti
Entro marzo 2025: adozione dell'elenco dei soggetti NIS
Entro aprile 2025: notifica ai soggetti NIS
Entro aprile 2025: elaborazione e adozione obblighi di base

METÀ APRILE 25 – METÀ APRILE 26

Seconda fase attuativa

Monitoraggio e supporto
A partire da gennaio 2026: obbligo di notifica di base
Entro aprile 2026: elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
Entro aprile 2026: elaborazione e adozione degli obblighi a lungo termine
Entro settembre 2026: completa implementazione delle misure di sicurezza di base

DA METÀ APRILE 26

Terza fase attuativa

Categorizzazione delle attività e dei servizi
Implementazione degli obblighi a lungo termine