UNIONE EUROPEA

DIRETTIVA NIS2

(Direttiva UE 2022/2555)

Misure per un livello comune elevato di cibersicurezza nell'Unione

Sintesi in italiano per CISO e responsabili della conformità

Riferimento del documento

Campo	Valore
Denominazione ufficiale	Direttiva (UE) 2022/2555
Data di adozione	14 dicembre 2022
Data di pubblicazione	27 dicembre 2022 (GU L 333/80)
Entrata in vigore	16 gennaio 2023
Termine di recepimento nazionale	17 ottobre 2024
Strumento abrogato	Direttiva (UE) 2016/1148 (NIS1)

> Il presente documento è una sintesi non ufficiale della Direttiva NIS2 dell'UE del 14 dicembre 2022; non costituisce una traduzione ufficiale. Per l'interpretazione vincolante, consultare il testo ufficiale pubblicato in GU L 333/80, 27.12.2022.

Indice

1. Sintesi esecutiva

La **Direttiva NIS2** (Direttiva UE 2022/2555), adottata dal Parlamento europeo e dal Consiglio il 14 dicembre 2022, è la direttiva quadro generale dell'UE in materia di cibersicurezza. Abroga e sostituisce la precedente Direttiva NIS1 2016/1148 con effetto dal 18 ottobre 2024.

Le revisioni hanno concluso che, sebbene NIS1 abbia contribuito ad aumentare il livello di ciberresilienza nell'Unione, si è rivelata insufficiente ad affrontare le minacce di cibersicurezza attuali e future. NIS2 amplia sostanzialmente l'ambito di applicazione, introduce criteri uniformi, rafforza gli obblighi di gestione dei rischi e di segnalazione degli incidenti, e prevede disposizioni sanzionatorie più dissuasive.

I cinque pilastri della direttiva

1. **Ambito ampliato**: più settori e aziende sottoposti a regolamentazione.
2. **Gestione dei rischi rafforzata**: 10 misure tecniche e organizzative minime rese obbligatorie ai sensi dell'Articolo 21.
3. **Segnalazione degli incidenti rapida e graduale**: preallarme entro 24 ore, notifica dell'incidente entro 72 ore, relazione finale entro 1 mese.
4. **Responsabilità degli organi di gestione**: i dirigenti di alto livello possono essere ritenuti personalmente responsabili.
5. **Sanzioni dissuasive**: sanzioni amministrative fino al 2% del fatturato globale annuo o 10 milioni di EUR.

2. Finalità e base giuridica

La base giuridica della direttiva è **l'articolo 114 del Trattato sul funzionamento dell'Unione europea (TFUE)**, che consente misure per il ravvicinamento delle normative nazionali al fine di instaurare e garantire il funzionamento del mercato interno.

Gli obiettivi principali della direttiva sono:

- Eliminare le grandi divergenze tra gli Stati membri e stabilire norme minime comuni in materia di cibersicurezza;
- Istituire meccanismi efficaci per la cooperazione transfrontaliera e la condivisione delle informazioni;
- Aggiornare l'elenco dei settori e delle attività soggetti agli obblighi di cibersicurezza per riflettere l'attuale panorama delle minacce;
- Prevedere meccanismi di applicazione e ricorso che garantiscano l'effettiva attuazione degli obblighi;
- Rafforzare le capacità di ciberresilienza degli operatori di infrastrutture critiche e dei fornitori di servizi digitali.

La direttiva si applica fatti salvi e nel rispetto del diritto dell'UE sulla protezione dei dati personali (GDPR, Regolamento UE 2016/679) e sulla privacy nelle comunicazioni elettroniche (Direttiva 2002/58/CE).

3. Da NIS1 a NIS2: perché un nuovo regolamento?

NIS1, entrata in vigore nel 2016, è stata la prima normativa orizzontale dell'UE in materia di cibersicurezza. Il processo di revisione ha rivelato differenze significative nell'attuazione tra gli Stati membri, con la determinazione dell'ambito di applicazione lasciata in larga misura alla discrezione degli stessi, frammentando di fatto il mercato interno.

Carenze individuate di NIS1

Area problematica	Situazione con NIS1	Soluzione con NIS2
Determinazione dell'ambito	Lasciata alla discrezione degli Stati membri; variazioni significative nella pratica.	Regola della "soglia di dimensione" uniforme in tutta l'UE (medie e grandi imprese).
Elenco dei settori	Numero limitato di settori; quota significativa dell'economia digitale esclusa.	Copertura settoriale molto più ampia; infrastrutture digitali, pubblica amministrazione, spazio ecc. inclusi.
Segnalazione degli incidenti	Fase unica; scadenze e contenuto variavano tra gli Stati membri.	Segnalazione multifase: preallarme 24h + notifica 72h + relazione finale entro 1 mese.
Gestione dei rischi	Formulazione generica; misure minime specifiche non chiare.	L'Articolo 21 elenca 10 categorie di misure minime obbligatorie.
Sanzioni	Implementate a livelli molto diversi tra gli Stati membri.	Massimali armonizzati a livello UE (10 milioni EUR / 2% del fatturato).
Responsabilità del management	Non chiara.	Organo di gestione personalmente responsabile della conformità; formazione obbligatoria.

NIS2 non è un aggiornamento di NIS1; è una sostituzione concepita per produrre **un quadro di cibersicurezza armonizzato e applicabile in modo uniforme** in tutta l'Unione.

4. Ambito di applicazione e aree escluse

La direttiva riguarda principalmente i soggetti che operano nei settori di cui all'**Allegato I (alta criticità)** o all'**Allegato II (altra criticità)** all'interno dell'UE e che soddisfano la definizione di almeno media impresa. Ai sensi dell'Articolo 2 dell'allegato alla Raccomandazione 2003/361/CE della Commissione, una media impresa è quella con meno di 250 dipendenti e fatturato annuo non superiore a 50 milioni di EUR (o totale di bilancio non superiore a 43 milioni di EUR). NIS2 si applica ai soggetti pari o superiori alla soglia delle medie imprese: la soglia minima pratica per i soggetti rientranti nell'ambito è di 50 dipendenti o 10 milioni di EUR di fatturato (il limite superiore della "piccola impresa" ai sensi della stessa Raccomandazione).

Soggetti inclusi indipendentemente dalle dimensioni

- Fornitori di reti pubbliche di comunicazione elettronica e fornitori di servizi di comunicazione elettronica accessibili al pubblico;
- Prestatori di servizi fiduciari (ai sensi del Regolamento eIDAS UE 910/2014);
- Registri dei nomi di dominio di primo livello (TLD) e fornitori di servizi DNS;
- Soggetti che sono l'unico fornitore di un servizio in uno Stato membro o la cui interruzione del servizio potrebbe avere un impatto significativo sulla sicurezza pubblica, sulla salute o sull'incolumità;
- Tutti gli enti della pubblica amministrazione centrale (definiti a livello nazionale dagli Stati membri).

Aree escluse dall'ambito di applicazione

I soggetti pubblici le cui attività sono svolte principalmente nei settori della **sicurezza nazionale, della pubblica sicurezza, della difesa o dell'applicazione della legge** (prevenzione, indagine, accertamento e perseguimento di reati) sono esclusi dall'ambito di applicazione della direttiva. Sono altresì escluse le rappresentanze diplomatiche e consolari degli Stati membri nei paesi terzi e i servizi fiduciari utilizzati in sistemi chiusi.

5. Definizioni chiave

Alcuni concetti fondamentali devono essere chiaramente compresi per una corretta interpretazione della direttiva.

Termine	Definizione
Sistema informatico e di rete	Reti di comunicazione elettronica, qualsiasi dispositivo o gruppo di dispositivi che elabora dati digitali, e tutti i dati digitali elaborati per il funzionamento, l'uso, la protezione e la manutenzione degli stessi.
Cibersicurezza	Tutte le attività necessarie per proteggere i sistemi informatici e di rete, gli utenti e altre persone dalle minacce informatiche.
Incidente	Un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi.
Incidente significativo	Un incidente che ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato, o si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.
Minaccia informatica	Qualsiasi potenziale circostanza, evento o azione che potrebbe danneggiare, disturbare o altrimenti avere un impatto negativo sui sistemi informatici e di rete.
Minaccia informatica significativa	Una minaccia informatica che, in base alle sue caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informatici e di rete di un soggetto o degli utenti di tali servizi causando perdite materiali o immateriali considerevoli.
Vulnerabilità	Un punto debole, una suscettibilità o un difetto di prodotti TIC o servizi TIC che può essere sfruttato da una minaccia informatica.
Quasi incidente	Un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato.
CSIRT	Computer Security Incident Response Team (squadra di intervento per la sicurezza informatica in caso di incidente), il team tecnico responsabile della gestione degli incidenti.
ENISA	Agenzia dell'Unione europea per la cibersicurezza, svolge un ruolo centrale di consulenza e supporto nell'attuazione della direttiva.

6. Categorie di soggetti: soggetti essenziali e importanti

La direttiva suddivide tutti i soggetti rientranti nell'ambito in due categorie principali. Questa distinzione determina come si applicano gli obblighi e il regime di vigilanza/applicazione.

Criterio	Soggetti essenziali	Soggetti importanti
Settore	Allegato I, settori ad alta criticità	Allegato II, altri settori critici (e medie imprese nell'Allegato I)
Dimensioni	Grandi imprese (250+ dipendenti o 50+ milioni EUR di fatturato)	Medie imprese (da 50 a 249 dipendenti)
Regime di vigilanza	Sia ex-ante sia ex-post	Solo ex-post su prove o reclami
Sanzione amministrativa massima	10 milioni di EUR o 2% del fatturato annuo globale (si applica il valore più alto)	7 milioni di EUR o 1,4% del fatturato annuo globale (si applica il valore più alto)
Sanzioni per i dirigenti	Può essere applicato il divieto temporaneo di gestione	Il divieto temporaneo di gestione non si applica

> **Nota importante:** Se un soggetto era stato identificato come "operatore di servizi essenziali" ai sensi di NIS1, lo Stato membro può decidere che tale soggetto sia direttamente un soggetto essenziale ai sensi di NIS2. Inoltre, tutti i soggetti identificati come "soggetti critici" ai sensi della Direttiva 2022/2557 (CER) sono automaticamente considerati soggetti essenziali ai sensi di NIS2.

7. Settori rientranti nell'ambito di applicazione (Allegato I e Allegato II)

Allegato I, settori ad alta criticità

Le grandi imprese di questi settori sono soggetti essenziali; le medie imprese sono soggetti importanti.

Settore	Sottosettore / Tipo di soggetto
Energia	Energia elettrica (produzione, trasmissione, distribuzione, fornitura); Riscaldamento/raffreddamento urbano; Petrolio (condotte, produzione, stoccaggio, trasmissione); Gas naturale; Produzione, stoccaggio e trasmissione di idrogeno
Trasporti	Aereo (compagnie aeree, aeroporti, ATC); Ferroviario (gestori dell'infrastruttura, operatori ferroviari); Marittimo (operatori marittimi/per vie d'acqua interne); Stradale (sistemi di trasporto intelligenti, operatori stradali)
Settore bancario	Enti creditizi ai sensi del Regolamento (UE) 575/2013
Infrastrutture dei mercati finanziari	Sedi di negoziazione (borse) e controparti centrali (CCP)
Salute	Prestatori di assistenza sanitaria; Laboratori di riferimento UE; Soggetti che conducono R&S di medicinali; Produttori di medicinali; Fabbricanti di dispositivi medici considerati critici durante le emergenze sanitarie pubbliche (ai sensi del Regolamento (UE) 2022/123)
Acque potabili	Fornitori e distributori di acqua destinata al consumo umano
Acque reflue	Soggetti che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali
Infrastrutture digitali	Punti di interscambio internet (IXP); Fornitori di servizi DNS (escluso il DNS radice); Registri dei nomi TLD; Fornitori di servizi di cloud computing; Fornitori di servizi di data center; Fornitori di reti di distribuzione dei contenuti (CDN); Prestatori di servizi fiduciari; Fornitori di reti/servizi pubblici di comunicazione elettronica
Gestione dei servizi TIC (B2B)	Fornitori di servizi gestiti (MSP); Fornitori di servizi di sicurezza gestiti (MSSP)
Pubblica amministrazione	Enti governativi centrali e regionali definiti dagli Stati membri
Spazio	Operatori di infrastrutture di terra gestite dallo Stato membro o dal settore privato

Allegato II, altri settori critici

Settore	Sottosettore / Tipo di soggetto
Servizi postali e di corriere	Fornitori di servizi postali (compresi i servizi di corriere)
Gestione dei rifiuti	Soggetti che forniscono servizi di raccolta, riciclaggio e smaltimento dei rifiuti
Sostanze chimiche	Soggetti impegnati nella produzione, trasformazione e distribuzione di sostanze chimiche
Alimenti	Grandi imprese impegnate nella produzione, trasformazione e distribuzione all'ingrosso di alimenti
Produzione manifatturiera	Dispositivi medici/diagnostici in vitro; Prodotti informatici, elettronici e ottici; Apparecchiature elettriche; Macchinari e apparecchiature n.c.a.; Autoveicoli, rimorchi e semirimorchi; Fabbricazione di altri mezzi di trasporto
Fornitori digitali	Mercati online; Motori di ricerca online; Piattaforme di servizi di social network
Ricerca	Organismi di ricerca che conducono ricerca a fini commerciali

8. Obblighi degli Stati membri

La direttiva pone obblighi sia agli Stati membri sia ai soggetti del settore privato. Ogni Stato membro deve adottare le seguenti misure:

Strategia nazionale per la cibersicurezza. Adottare una strategia nazionale per la cibersicurezza con obiettivi strategici chiari, priorità e un quadro di governance. La strategia tratta temi quali la sicurezza della catena di approvvigionamento, il ransomware, il supporto alle PMI, l'open source e la difesa informatica attiva.

Autorità competente(i). Designare o istituire una o più autorità competenti per garantire l'attuazione e la vigilanza della direttiva.

Punto di contatto unico (SPOC). Designare un punto di contatto unico responsabile del coordinamento transfrontaliero a livello UE.

CSIRT. Istituire o designare uno o più CSIRT responsabili della gestione degli incidenti, del monitoraggio proattivo, della divulgazione coordinata delle vulnerabilità e della cooperazione nazionale/internazionale.

Elenco dei soggetti. Mantenere, aggiornare periodicamente e trasmettere alla Commissione un elenco dei soggetti essenziali e importanti e dei soggetti che forniscono servizi di registrazione dei nomi di dominio.

Divulgazione coordinata delle vulnerabilità. Designare un CSIRT come coordinatore; promuovere la chiarezza giuridica per i ricercatori di vulnerabilità.

Assistenza reciproca. Fornire assistenza reciproca agli altri Stati membri nella vigilanza e nell'applicazione transfrontaliera.

Supporto alle PMI. Fornire orientamenti, strumenti gratuiti e un punto di contatto nazionale/regionale per le piccole e microimprese.

9. Misure di gestione dei rischi di cibersicurezza (Articolo 21)

La disposizione tecnica più importante della direttiva è l'Articolo 21. Elenca le misure tecniche, operative e organizzative minime che i soggetti essenziali e importanti devono attuare. L'approccio si basa su una **prospettiva "multirischio"**; non solo gli attacchi informatici ma anche minacce quali danni fisici, catastrofi naturali, guasti alle apparecchiature ed errori umani rientrano nell'ambito.

Articolo 21, dieci misure minime

N.	Misura	Descrizione
1	Politiche di analisi dei rischi e di sicurezza dei sistemi informatici	Analisi di tutti i rischi e predisposizione scritta di politiche generali di sicurezza delle informazioni.
2	Gestione degli incidenti	Processi per la prevenzione, il rilevamento, la risposta e il ripristino in caso di incidenti.
3	Continuità operativa	Gestione del backup, ripristino in caso di disastro e gestione delle crisi.
4	Sicurezza della catena di approvvigionamento	Incluse le pratiche di sicurezza dei fornitori; disposizioni di cibersicurezza nei contratti con i fornitori diretti.
5	Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete	Sicurezza durante tutto il ciclo di vita, inclusa la gestione e la divulgazione delle vulnerabilità.
6	Valutazione dell'efficacia delle misure	Valutazione periodica dell'efficacia delle misure di gestione dei rischi.
7	Pratiche di igiene informatica di base e formazione in materia di cibersicurezza	Pratiche di igiene informatica e formazione sulla consapevolezza per il personale.
8	Crittografia e cifratura	Politiche sull'uso della crittografia; cifratura end-to-end ove opportuno.
9	Sicurezza delle risorse umane, controllo degli accessi e gestione degli attivi	Controlli del personale, autorizzazioni e inventario degli attivi.
10	Autenticazione a più fattori e comunicazioni protette	MFA ove opportuno, autenticazione continua, comunicazioni vocali/video/testuali protette e sistemi di comunicazione di emergenza protetti.

Tali misure sono applicate secondo il **principio di proporzionalità**, tenendo conto dell'esposizione al rischio del soggetto, delle sue dimensioni, dell'importanza settoriale e dell'impatto potenziale degli incidenti.

10. Obblighi di segnalazione degli incidenti (Articolo 23)

La più importante innovazione operativa della direttiva è il regime di segnalazione degli incidenti a più fasi. I soggetti essenziali o importanti devono segnalare gli **incidenti significativi**, definiti come quelli che causano gravi perturbazioni operative, perdite finanziarie o un impatto sostanziale su altre persone, al CSIRT o all'autorità competente entro i seguenti termini.

Fase	Scadenza	Contenuto
Preallarme	Entro 24 ore dalla conoscenza dell'incidente	Sospetto che l'incidente sia causato da un'azione illegittima o malevola; possibilità di impatto transfrontaliero; informazioni di base che consentano la consapevolezza del CSIRT.
Notifica dell'incidente	Entro 72 ore dalla conoscenza dell'incidente	Aggiornamento del preallarme; gravità, impatto e, ove disponibili, indicatori di compromissione (IoC).
Relazione intermedia/finale	Entro 1 mese dalla trasmissione della notifica dell'incidente	Descrizione dettagliata dell'incidente, della sua gravità e del suo impatto; tipo di minaccia sfruttata; misure di mitigazione adottate e pianificate; impatto transfrontaliero se del caso.
Relazione di avanzamento	Se l'incidente è ancora in corso alla scadenza della relazione finale	Relazione sullo stato attuale dell'incidente; relazione finale entro 1 mese dal completamento della gestione dell'incidente.

Notifica ai destinatari del servizio: Quando è probabile che si verifichi una minaccia informatica significativa, i soggetti devono notificare senza indebito ritardo e gratuitamente ai destinatari dei propri servizi le possibili misure di mitigazione e, ove opportuno, la minaccia stessa in un linguaggio chiaro e comprensibile.

Quasi incidenti e segnalazione volontaria

Oltre agli incidenti, i soggetti **possono segnalare volontariamente quasi incidenti e minacce informatiche significative** al CSIRT o all'autorità competente. Anche i soggetti non rientranti nell'ambito della direttiva possono segnalare volontariamente. La segnalazione volontaria non impone obblighi aggiuntivi al segnalante.

> **Impatto pratico:** Il preallarme entro 24 ore obbliga i soggetti ad avere un piano di risposta agli incidenti informatici e un flusso di comunicazione pronti per essere attivati immediatamente al momento del rilevamento dell'incidente. Rispettare questa scadenza attraverso processi manuali e frammentati è estremamente difficile.

11. Sicurezza della catena di approvvigionamento

La maggior parte dei grandi attacchi informatici degli ultimi anni ha raggiunto le organizzazioni bersaglio attraverso fornitori e produttori di software, non tramite un attacco diretto all'organizzazione stessa. La direttiva pone pertanto il rischio della catena di approvvigionamento al centro degli obblighi di gestione dei rischi.

- I soggetti devono valutare la **qualità, le pratiche di sicurezza e i processi di sviluppo sicuro** dei prodotti/servizi dei propri fornitori e prestatori di servizi.
- **I requisiti di cibersicurezza devono essere inclusi nei contratti** con i fornitori diretti.
- Occorre esercitare una speciale diligenza nella selezione dei **fornitori di servizi di sicurezza gestiti (MSSP)**; questi fornitori sono obiettivi ad alto valore per gli attaccanti.
- Il gruppo di cooperazione, insieme alla Commissione e all'ENISA, effettua **valutazioni coordinate dei rischi per la sicurezza** delle catene di approvvigionamento critiche (come è stato fatto per le reti 5G).
- I **fattori di rischio non tecnici** rientrano anch'essi nell'ambito della valutazione, inclusa la potenziale indebita influenza di paesi terzi sui fornitori, vulnerabilità nascoste/backdoor e dipendenza dal fornitore.

12. Responsabilità degli organi di gestione

La direttiva garantisce che la cibersicurezza esca dall'ambito dei soli reparti tecnici e diventi **responsabilità diretta dell'alta direzione**. Ai sensi dell'Articolo 20, gli organi di gestione dei soggetti essenziali e importanti:

- Sono responsabili dell'**approvazione delle misure di gestione dei rischi** ai sensi dell'Articolo 21 e della supervisione della loro attuazione;
- Possono essere **ritenuti personalmente responsabili** per le violazioni di tali obblighi;
- Devono ricevere periodicamente formazione in materia di cibersicurezza per acquisire conoscenze e competenze sufficienti;
- Dovrebbero incoraggiare una formazione analoga per il proprio personale.

> **Importante:** Nei soggetti essenziali, l'autorità competente può richiedere l'applicazione di **divieti temporanei di gestione** ai dirigenti di alto livello (a livello di amministratore delegato o rappresentante legale). Si tratta di una misura di ultima istanza, applicabile solo dopo che tutte le altre opzioni di applicazione sono state esaurite.

13. Strutture di cooperazione a livello UE

La direttiva disciplina o rafforza varie strutture che garantiscono una cooperazione efficace tra gli Stati membri:

Struttura	Funzione
Gruppo di cooperazione	Supporta la cooperazione a livello strategico; predispone programmi di lavoro biennali; pubblica documenti di orientamento; effettua valutazioni coordinate dei rischi per le catene di approvvigionamento critiche.
Rete dei CSIRT	Cooperazione a livello operativo; condivisione di informazioni sugli incidenti; assistenza reciproca; risposta congiunta.
EU-CyCLONe	Rete europea di collegamento per le crisi informatiche; fa da ponte tra il livello tecnico e quello politico negli incidenti e nelle crisi su larga scala; predispone analisi di impatto.
ENISA	Istituisce e mantiene la banca dati europea delle vulnerabilità; fornisce supporto tecnico; sviluppa orientamenti; monitora le politiche degli Stati membri in materia di igiene informatica.
Meccanismi IPCR	Meccanismi di risposta politica integrata alle crisi (Decisione di esecuzione del Consiglio 2018/1993), gestione delle crisi a livello di Unione per crisi su larga scala.
Coordinatore CVD EU-CSIRT	Un CSIRT di ogni Stato membro è designato coordinatore per gestire la divulgazione coordinata delle vulnerabilità transfrontaliere.

Cooperazione con i paesi terzi: L'UE può concludere accordi internazionali con paesi terzi o organizzazioni internazionali ai sensi dell'Articolo 218 TFUE. Tali accordi possono, nel rispetto degli interessi dell'Unione e della protezione dei dati, consentire a tali parti di partecipare alle attività del gruppo di cooperazione, della rete dei CSIRT o di EU-CyCLONe.

14. Vigilanza e applicazione

La direttiva prevede regimi di vigilanza diversi per le due categorie di soggetti. I **soggetti essenziali** sono soggetti sia a vigilanza ex-ante sia ex-post, mentre i **soggetti importanti** sono vigilati solo ex-post, su prove o reclami.

Poteri di vigilanza delle autorità competenti

- Effettuare ispezioni in loco e vigilanza a distanza;
- Richiedere audit di sicurezza mirati (con possibile addebito dei costi al soggetto);
- Ordinare scansioni di sicurezza;
- Richiedere documentazione della conformità alle misure di gestione dei rischi;
- Richiedere informazioni su atti sospettati di violare la direttiva;
- Richiedere informazioni che richiedano accesso a dati personali e dati di traffico ove necessario.

Misure di applicazione applicabili

- Emettere avvertimenti e istruzioni vincolanti;
- Ordinare misure specifiche o la correzione di vulnerabilità da attuare entro un termine specificato;
- Ordinare un audit indipendente per verificare le misure di gestione dei rischi;
- Ordinare ai soggetti di informare i destinatari del servizio sulla natura della violazione;
- Rilasciare dichiarazioni pubbliche (rivelando il nome del soggetto e la natura della violazione);
- Per i soggetti essenziali (ultima istanza): sospensione temporanea di certificazioni o autorizzazioni e divieti temporanei di gestione per i dirigenti di alto livello;
- Irrogare o richiedere l'irrogazione di sanzioni amministrative.

15. Sanzioni amministrative

La direttiva stabilisce **massimali armonizzati a livello UE** per le sanzioni amministrative applicate dagli Stati membri. Tali massimali sono correlati al fatturato globale del soggetto, in modo analogo al GDPR.

Tipo di soggetto	Importo massimo (si applica il valore più alto)
Soggetti essenziali	10.000.000 EUR o 2% del fatturato annuo globale
Soggetti importanti	7.000.000 EUR o 1,4% del fatturato annuo globale

Fattori nella determinazione delle sanzioni

- Natura, gravità e durata della violazione;
- Perdite materiali o immateriali causate;
- Se la violazione è stata intenzionale o colposa;
- Misure adottate per prevenire o attenuare il danno;
- Grado di responsabilità e violazioni precedenti;
- Grado di cooperazione con l'autorità competente;
- Altri fattori aggravanti o attenuanti.

Le sanzioni devono essere **proporzionate** e nella loro applicazione devono essere rispettati i diritti fondamentali quali il diritto di difesa, la presunzione di innocenza e il diritto a un ricorso effettivo. Gli Stati membri possono altresì prevedere sanzioni penali per le violazioni del diritto nazionale; tuttavia, nessuna persona può essere punita due volte per lo stesso atto in violazione del principio del **ne bis in idem**.

16. Calendario di attuazione e periodo transitorio

Data	Evento
14 dicembre 2022	Adozione della direttiva da parte del Parlamento europeo e del Consiglio
27 dicembre 2022	Pubblicazione nella Gazzetta ufficiale dell'UE (GU L 333/80)
16 gennaio 2023	Entrata in vigore della direttiva (20 giorni dopo la pubblicazione)
17 ottobre 2024	Termine per il recepimento della direttiva nel diritto nazionale degli Stati membri
18 ottobre 2024	Inizio dell'applicazione della direttiva
18 ottobre 2024	Abrogazione della Direttiva (UE) 2016/1148 (NIS1)
17 aprile 2025	Termine per la trasmissione alla Commissione dell'elenco dei soggetti essenziali e importanti da parte degli Stati membri
Dal 17 ottobre 2027 in poi	Revisione periodica dell'attuazione della direttiva da parte della Commissione (ogni 36 mesi)

> **Importante:** NIS2 è una direttiva; non si applica direttamente. Ogni Stato membro deve recepire la direttiva nel proprio diritto nazionale. Pertanto, gli obblighi e le sanzioni precisi applicabili a un soggetto dipendono dall'atto di recepimento nazionale adottato dallo Stato membro in cui opera.

17. Implicazioni per le imprese non UE

Sebbene NIS2 sia una direttiva dell'UE, ha implicazioni sostanziali per le imprese non UE, in particolare per quelle che servono il mercato UE o che forniscono prodotti/servizi a soggetti critici con sede nell'UE:

Imprese non UE direttamente interessate

- **Fornitori DNS, fornitori di servizi cloud, operatori di data center, fornitori CDN, fornitori di servizi gestiti e di sicurezza gestiti, mercati online, motori di ricerca e piattaforme di social network** non UE che offrono servizi nell'UE devono nominare un rappresentante nell'UE e conformarsi agli obblighi della direttiva;
- Le società non UE con filiali o succursali nell'UE possono essere soggette alla direttiva attraverso tali unità;
- I fornitori non UE di prodotti/servizi a soggetti essenziali o importanti UE saranno soggetti ai **requisiti contrattuali di sicurezza della catena di approvvigionamento** imposti dai propri clienti (Articolo 21, paragrafo 2, lettera d));
- Gli MSP/MSSP non UE che servono infrastrutture digitali o soggetti finanziari UE possono rientrare direttamente nell'ambito di applicazione.

Effetti indiretti

- Le valutazioni del rischio della catena di approvvigionamento da parte dei clienti UE obbligano i fornitori non UE ad innalzare i propri standard di cibersicurezza;
- Gli standard introdotti dalla direttiva (ISO/IEC 27001, orientamenti ENISA, ecc.) stanno diventando **punti di riferimento de facto** nel mercato globale;
- Le giurisdizioni non UE utilizzano sempre più NIS2 come riferimento nello sviluppo della propria legislazione in materia di cibersicurezza.

18. Tabella di marcia per la conformità pratica (10 fasi)

La seguente tabella di marcia in 10 fasi costituisce una guida pratica sia per le imprese che operano nell'UE sia per quelle che desiderano allinearsi volontariamente agli standard NIS2.

Fase	Attività
1. Determinazione dell'ambito	Determinare se l'azienda rientra nei settori dell'Allegato I o dell'Allegato II, verifica dei criteri dimensionali e identificazione della categoria (essenziale/importante).
2. Analisi dei gap	Valutare il sistema di gestione della sicurezza delle informazioni esistente rispetto alle 10 categorie di misure dell'Articolo 21; mappare i gap.
3. Struttura di governance	Stabilire responsabilità, linee gerarchiche e processi di approvazione a livello di consiglio/alta direzione; istituire un programma periodico di formazione.
4. Politiche e documentazione	Predisporre o aggiornare la politica di sicurezza delle informazioni, la politica di gestione dei rischi, la politica di risposta agli incidenti, la politica di utilizzo accettabile e altri documenti.
5. Valutazione del rischio	Effettuare l'inventario degli attivi, l'analisi delle minacce e la valutazione del rischio con approccio multirischio; stabilire i criteri di accettazione del rischio.
6. Implementazione dei controlli tecnici	Implementare MFA, crittografia, segmentazione della rete, architettura zero-trust, gestione dei log, SIEM, EDR/XDR, soluzioni di backup e disaster recovery.
7. Capacità di risposta agli incidenti	Documentare il piano di risposta agli incidenti; assegnare ruoli e responsabilità; stabilire il flusso di comunicazione per il preallarme entro 24 ore; condurre esercitazioni di tipo tabletop.
8. Gestione della catena di approvvigionamento	Effettuare l'inventario dei fornitori; classificarli per livello di rischio; aggiungere disposizioni di cibersicurezza ai modelli di contratto; condurre audit periodici.
9. Formazione e sensibilizzazione	Organizzare formazione annuale sull'igiene informatica per tutto il personale; fornire formazione specializzata per l'organo di gestione; condurre simulazioni di phishing.
10. Miglioramento continuo	Condurre audit interni ed esterni; monitorare i KPI; imparare da ogni incidente; aggiornare annualmente la valutazione del rischio; perseguire la certificazione (ISO/IEC 27001, certificazione di cibersicurezza UE).

19. Conclusioni e valutazione

La Direttiva NIS2 innalza sostanzialmente il livello base di cibersicurezza dell'Unione europea. Non si limita a imporre requisiti tecnici; rende la cibersicurezza **parte integrante della struttura di governance e delle operazioni aziendali** delle imprese.

Punti di forza della direttiva

- **Ampia portata**: circa 18 settori e oltre 100.000 soggetti rientranti nell'ambito in tutta l'UE-27;
- **Armonizzazione**: condizioni di parità nel mercato interno grazie a criteri uniformi e a un regime di applicazione uniforme in tutta l'UE;
- **Focus sulla governance**: rendendo l'alta direzione responsabile, garantisce che la cibersicurezza permei tutti i livelli dell'azienda;
- **Enfasi sulla catena di approvvigionamento**: risponde alla realtà che la maggior parte degli attacchi moderni proviene dalla catena di approvvigionamento;
- **Strutture di cooperazione**: coordinamento a livello UE su più livelli attraverso il gruppo di cooperazione, la rete dei CSIRT e EU-CyCLONe.

Critiche e sfide

- Ritardi e divergenze nel recepimento da parte degli Stati membri; in pratica, un'attuazione uniforme in tutta l'UE-27 è disomogenea;
- In particolare per le medie imprese, il costo della conformità e il colmare il divario di capacità tecnica rappresentano una sfida seria;
- L'attuazione della scadenza del preallarme entro 24 ore prima che sia raggiunta una sufficiente maturità può portare a flussi di segnalazione superficiali o errati;
- Le aree di sovrapposizione con le normative settoriali (DORA, finanza; eIDAS, servizi fiduciari; normative settoriali dell'aviazione ecc.) possono creare complessità per i soggetti.

Valutazione complessiva

NIS2 ridefinisce la cibersicurezza da preoccupazione tecnica a questione di **continuità operativa, governance aziendale e fiducia dei clienti**. Per i soggetti che operano o interagiscono con l'UE, la conformità è sia un obbligo giuridico sia un mezzo per rafforzare la resilienza operativa.

Per le imprese non UE, NIS2 sta stabilendo un nuovo **standard de facto** per l'accesso al mercato UE e sta innalzando le aspettative in materia di cibersicurezza a livello globale. Una conformità anticipata facilita il rispetto degli obblighi contrattuali e migliora la ciberresilienza complessiva.

> **Nota finale:** Il presente documento sintetizza le principali disposizioni della direttiva per i lettori di lingua italiana. Per i requisiti di conformità specifici della propria organizzazione, consultare il testo ufficiale (GU L 333/80, 27.12.2022), l'atto di recepimento nazionale del proprio Stato membro e le normative settoriali specifiche; ricorrere ove opportuno a consulenza legale e in materia di cibersicurezza.

Fonti

- Direttiva (UE) 2022/2555, numero CELEX EUR-Lex 32022L2555
- Gazzetta ufficiale dell'UE L 333/80, 27 dicembre 2022
- ENISA, Agenzia dell'Unione europea per la cibersicurezza (www.enisa.europa.eu)
- Portale della strategia digitale della Commissione europea (digital-strategy.ec.europa.eu)

Approfondimenti su NIS2 da Rediacc

Questa sintesi illustra la struttura e gli obblighi della direttiva. Le guide di accompagnamento su rediacc.com traducono quegli obblighi in decisioni operative e di procurement concrete.

Tre guide di accompagnamento

- **Articolo 21(2)(d) e self-hosting.** Perché il registro TIC di terze parti si riduce quando il piano dati non lascia mai il proprio tenant. Per CISO e responsabili degli acquisti che rinegoziamo i DPA nel 2026.
- **Efficacia continua senza teatro.** Articolo 21(2)(e), (f) e 23 letti insieme. Il fork a tempo costante che rende realistici i test settimanali, e la timeline di segnalazione dell'Articolo 23 che non puoi rispettare senza artefatti di qualità forense. Per SRE e responsabili delle operazioni.
- **Il costo strutturale della conformità NIS2.** Lo stack a cinque strumenti che le medie imprese essenziali stanno silenziosamente assemblando, cosa riduce un piano di controllo self-hosted, e le voci di costo che restano comunque a carico. Per CFO e acquirenti che si avvicinano a un ciclo di rinnovo.

Dove trovarle

Tutte e tre le guide, insieme a questa sintesi come PDF scaricabile, sono disponibili su:

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ è una piattaforma di infrastruttura self-hosted registrata in Estonia (Codice registro 17363830, IVA EE102920091). Il prodotto non sostituisce un programma di sicurezza; è uno strato di strumenti che elimina il rischio del fornitore del piano dati che gli strumenti tradizionali di backup, DR e dati di test non possono eliminare. Livello Community gratuito e livelli a pagamento a partire da 349 $/mese.

> Il presente documento e le sue guide di accompagnamento sono materiale didattico. Le decisioni di conformità specifiche per la propria organizzazione richiedono consulenza legale e il riferimento all'atto di recepimento nazionale nella propria giurisdizione.