
CYBEREDGE
INNOVAZIONE, SVILUPPO, SICUREZZA

CYBEREDGE

NIS2: una guida pratica

www.cyberedge.it

Riferimenti normativi

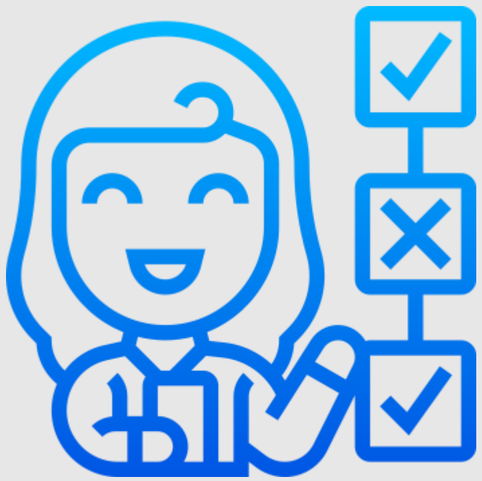
Il presupposto della Direttiva NIS2 è che, in un ambiente sempre più interconnesso, **le vulnerabilità di un elemento, possono ripercuotersi in maniera diretta e grave su tutti gli altri elementi del sistema**. La sicurezza è un requisito necessario per lo sviluppo economico dei Paesi dell'Unione Europea

- **DIRETTIVA (UE) 2022/2555 del 14 dicembre 2022**
- **Decreto Legislativo 138 / 2024**

“Sicurezza” (art. 2)

“**Sicurezza dei sistemi informatici e di rete**” è la **capacità** dei **sistemi informatici e di rete di resistere**, con un determinato livello di affidabilità, **agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti** da tali sistemi informatici e di rete o accessibili attraverso di essi.
“**Sicurezza informatica**” è l'insieme delle **attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone** interessate dalle minacce informatiche

Soggetti coinvolti



Regola generale

Rientrano nell’ambito di applicazione della normativa:

- *Società che prestano i loro servizi o svolgono le loro attività* ***all’interno dell’Unione Europea***
- *Soggetti* ***critici e altamente critici + PA + altri*** *(All I - IV)*
- *Aziende* ***medio - grandi*** *(che superano 10M euro di fatturato e con +50 dipendenti)* ***+ eccezioni***

Settori altamente critici (All. I)

Energia	Energia elettrica + Teleriscaldamento e Telraffrescamento + Petrolio + Gas + Idrogeno
Trasporti	Trasporto aereo + trasporto ferroviario + trasporto per vie d'acqua + trasporto su strada
Settore bancario	
Infrastrutture dei mercati finanziari	
Settore sanitario	
Acque potabili	
Acque reflue	
Infrastrutture digitali	
Gestione dei servizi TLC (B2B)	
Spazio	

Settori critici (All. II)

Servizi postali e di corriere	
Gestione dei rifiuti	
Fabbricazione, produzione e distribuzione di sostanze chimiche	
Produzione, trasformazione e distribuzione di alimenti	
Fabbricazione	Dispositivi medici e medico-diagnostici in vitro + Computer e prodotti di elettronica e ottica + apparecchiature elettriche + macchinari e apparecchiature n.c.a. + autoveicoli, rimorchi e semirimorchi + altri mezzi di trasporto
Fornitori di servizi digitali	mercati on line + motori di ricerca + piattaforme di Social network + servizi registrazione nomi dominio
Ricerca	

Pubblica amministrazione (All. III)

- Amministrazioni centrali
- Amministrazioni regionali
- Amministrazioni locali
- Altri soggetti pubblici

Altri soggetti (All IV)

- Soggetti che forniscono servizi di trasporto pubblico locale
- Istituti di istruzione che svolgono attività di ricerca
- Soggetti che svolgono attività di interesse culturale
- Società in house, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175.

Aggiunte

INDIPENDENTEMENTE DALLE DIMENSIONI

Si applicano le disposizioni di legge anche a:

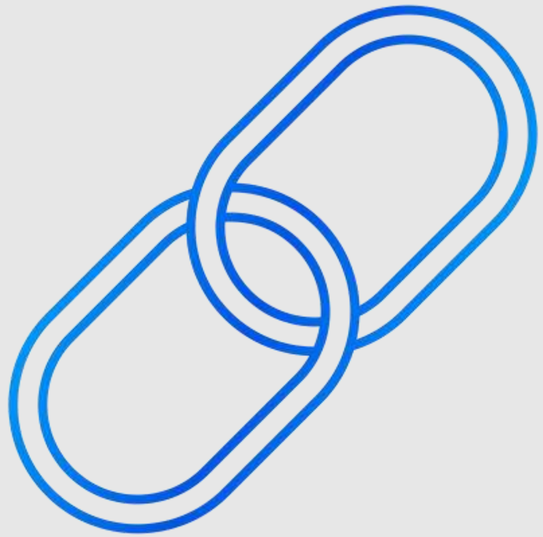
- fornitori di reti pubbliche di comunicazione elettronica o di **servizi di comunicazione elettronica** accessibili al pubblico;
- **prestatori di servizi fiduciari** (ossia quei soggetti che forniscono servizi che garantiscono l’integrità e la sicurezza delle transazioni digitali);
- gestori di **registri dei nomi di dominio** di primo livello e fornitori di servizi di sistema dei nomi di dominio;
- fornitori di **servizi di registrazione dei nomi di dominio**.

“Imprese collegate” (art 3)

INDIPENDENTEMENTE DALLE DIMENSIONI

Il decreto si applica anche all'impresa collegata ad un soggetto essenziale o importante, **fatte salve le clausole di salvaguardia**, se soddisfa almeno uno dei seguenti criteri:

- adotta decisioni o esercita una influenza dominante sulle **decisioni relative alle misure di gestione del rischio per la sicurezza informatica** di un soggetto importante o essenziale
- detiene o **gestisce sistemi informativi e di rete** da cui dipende la fornitura dei servizi del soggetto importante o essenziale
- effettua **operazioni di sicurezza informatica** del soggetto importante o essenziale
- **fornisce servizi TIC o di sicurezza**, anche gestiti, al soggetto importante o essenziale



Obblighi

Registrazione (art. 7)

Entro FEBBRAIO 2025 le Aziende che rientrano nei parametri previsi devono REGISTRARSI sul PORTALE ACN.

I **dati da inserire** sul portale sono:

- il proprio nome
- il settore, il sottosettore e il tipo di soggetto di cui agli allegati I - IV
- l'indirizzo dello stabilimento principale e degli altri stabilimenti legali del soggetto nell'Unione o, se non è stabilito nell'Unione, del suo rappresentante
- i dati di contatto aggiornati e, se opportuno, del suo rappresentante
- gli Stati membri in cui il soggetto fornisce i suoi servizi
- le serie di IP del soggetto.

Accountability del management (art. 23)

Gli organi di gestione dei soggetti essenziali ed importanti hanno una **responsabilità diretta nell’approvazione e applicazione delle misure previste dal regolamento NIS2**.
Sono **responsabili delle violazioni** alla normativa
Sono inoltre tenuti a seguire **percorsi di formazione** e ad incoraggiare la formazione per tutti i dipendenti.

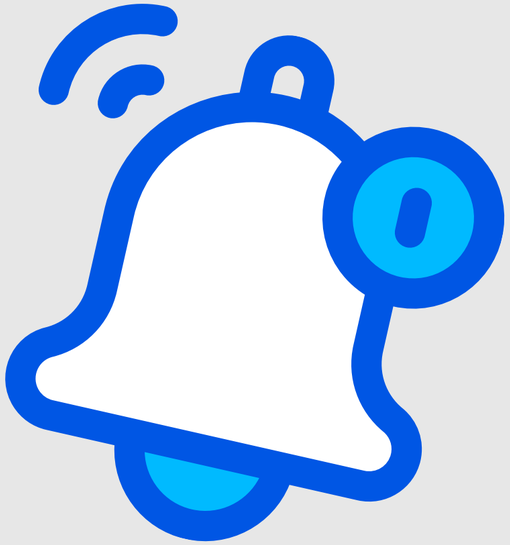
Gestione del rischio (art. 24)

La norma si basa su un **approccio multi-rischio**, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti. **Le misure adottate devono prevedere:**

- Analisi del rischio
- Gestione degli incidenti
- Continuità operativa e disaster recovery
- Sicurezza nella catena di approvvigionamento compresi i rapporti coi diversi fornitori
- Sicurezza nell’acquisizione e manutenzione dei sistemi informatici e di rete
- Procedure per valutare efficacia delle misure di gestione del rischio
- Formazione
- Procedure relative all’uso di crittografia e / o cifratura
- Sicurezza del personale e controllo degli accessi
- Soluzioni di autenticazione a più fattori e sistemi di comunicazione protetta

Obbligo di notifica (art. 25)

Gli incidenti di sicurezza vanno notificati alle autorità competenti ed eventualmente ai destinatari dei loro servizi se questi possono essere impattati dalla minaccia informatica.



Tempistiche:

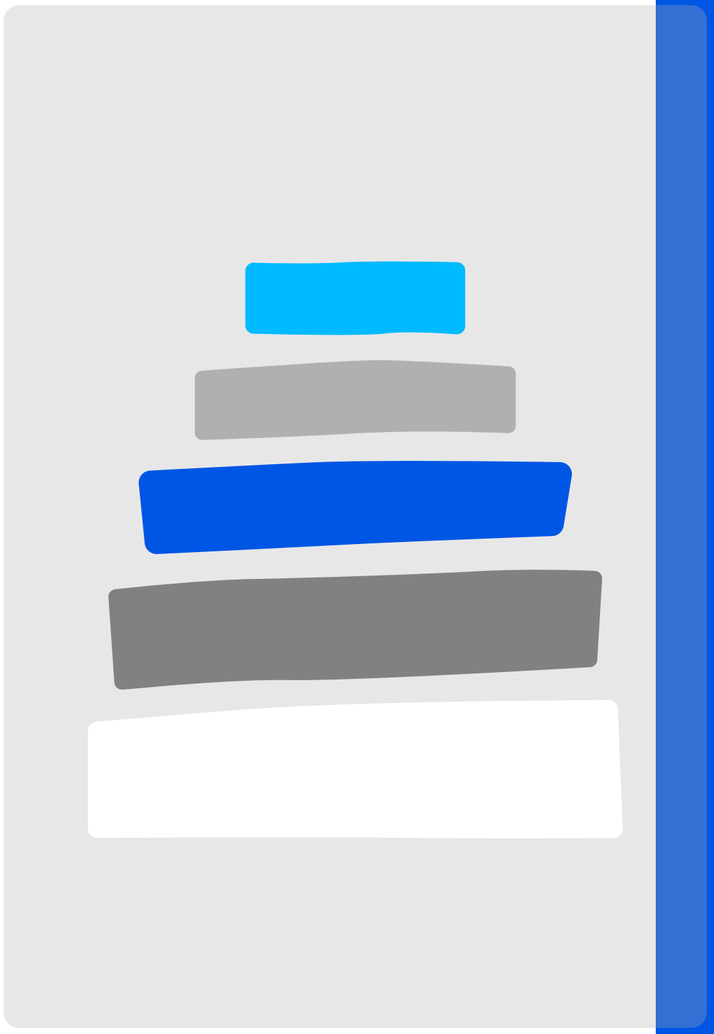
- **Entro 24h** da conoscenza di evento significativo va **comunicato preallarme** indicando se la causa sono atti malevoli e/o se incidente può avere conseguenze transfrontaliere
- **Entro 72h** da conoscenza di evento va inviata una **notifica con indicazione della gravità** dell'incidente e impatto
- **Entro 1 mese: relazione finale** con cause incidente, misure adottate, impatto incidente sia locale che transfrontaliero

Tassonomia (TC-ACN)

In un panorama di Cybersicurezza in continua evoluzione è fondamentale identificare, definire e caratterizzare gli eventi cyber attraverso **un’unica classificazione** rilevante a livello nazionale e armonizzata con quella internazionale

La Tassonomia Cyber dell’Agenzia per la Cybersicurezza Nazionale (TC-ACN) prevede:

- **4 macrocategorie** composte da un gruppo di predicati con caratteristiche affini;
- **22 predicati**, ossia lemmi che raccolgono un sottoinsieme di valori in base alleloro proprietà e caratteristiche intrinseche;
- **144 valori**, ossia gli elementi granulari con determinate caratteristiche relative a un evento cyber.



Macrocategorie

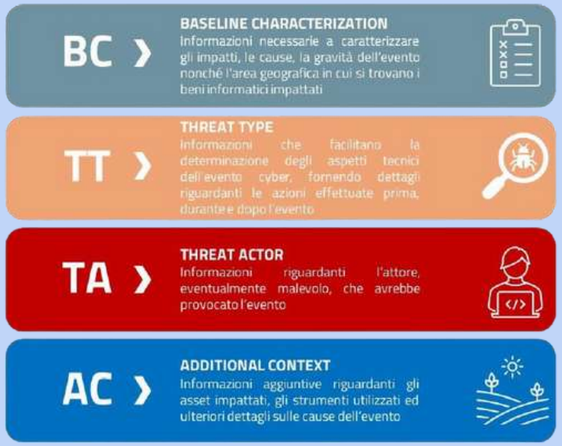


Figura 1: Struttura della tassonomia degli eventi cyber - Macrocategorie

Predicati

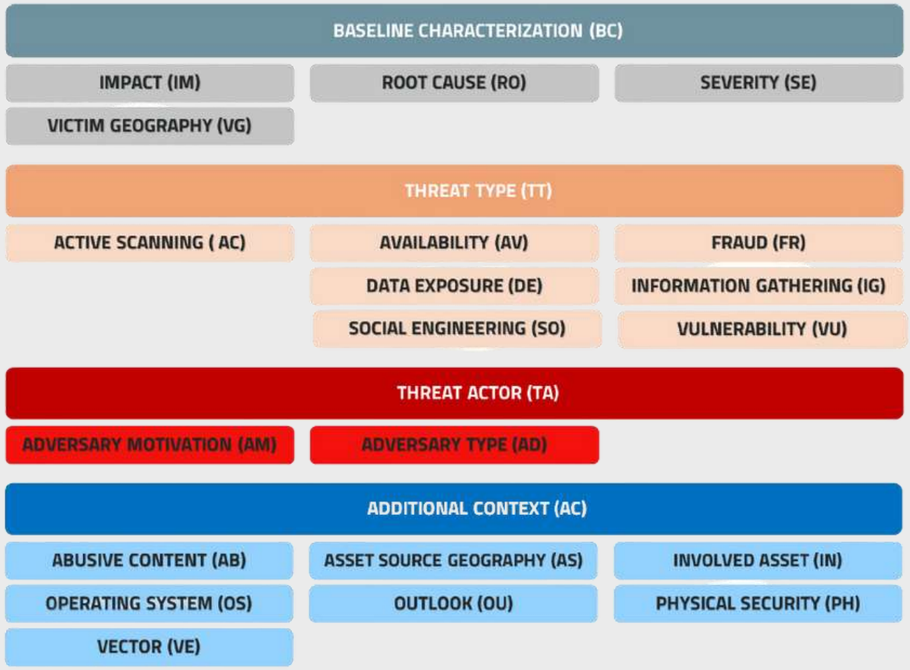


Figura 2: Struttura della tassonomia degli eventi cyber - Predicati

***Esempio**: il"valore" ransomware ricadrà nel predicato "malicious code", il quale, a sua volta, sarà ricompreso nella macrocategoria "Threat Type".*

Note:

Per le specifiche dei **144 valori** si rimanda al sito https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn

L'ACN ha reso disponibile un **TOOL** on-line per creare la corretta tassonomia relativa alle segnalazioni di incidenti, disponibile a questo link: https://tassonomia-acn.utilia.it/

Vigilanza e sanzioni

Vigilanza (artt. 34 - 37)

L’Autorità competente nello svolgimento del compito di vigilanza può adottare le seguenti misure:

- **ispezioni** in loco e **vigilanza a distanza**
- **audit sulla sicurezza** periodici e mirati oppure ad hoc
- **scansioni di sicurezza** basate sulla valutazione del rischio
- **richieste di informazioni** per valutare la validità delle misure di sicurezza adottate
- **richieste di accesso a dati o informazioni** necessarie per valutare l’effettiva attuazione delle misure di cybersicurezza

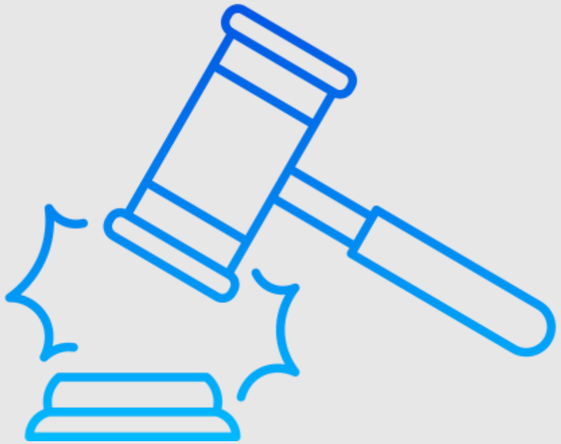
I costi degli audit sono a carico del soggetto sottoposto all’audit stesso

Sanzioni (art. 38)

In caso di **VIOLAZIONI GRAVI** quali mancata osservanza delle disposizioni di legge e/o inottemperanza delle disposizioni dell'Autorità a seguito di monitoraggi e ispezioni >> **Sanzioni pecuniarie fino a 10 MEUR o 2% del fatturato annuo mondiale per soggetti essenziali e fino a 7 MEUR o 1,4% del fatturato annuo mondiale per soggetti importanti**

In caso di **ALTRE VIOLAZIONI** quali mancata registrazione o comunicazione dei dati, mancata collaborazione con ANC e altri >> **Sanzioni pecuniarie fino a 0,1% del fatturato annuo mondiale per soggetti essenziali e fino a 0,07% del fatturato annuo mondiale per soggetti importanti**

Sono previste maggiorazioni in caso di re-iterazioni



Scadenze

Prima fase attuativa

Entro febbraio 2025: censimento e **registrazione dei soggetti sulla piattaforma ACN**
https://www.acn.gov.it/portale/nis/registrazione
Entro marzo 2025: adozione dell'elenco dei soggetti NIS
Entro aprile 2025: notifica ai soggetti NIS : ACN dirà se il soggetto è effettivamente un soggetto a cui si applica la NIS2
Entro aprile 2025: elaborazione e adozione obblighi di base

Seconda fase attuativa

A partire da 1° gennaio 2026: adeguamento a all'articolo 25 relativo alla **notifica degli incidenti**; questo richiede come minimo di stabilire il processo di gestione degli incidenti
A partire da 1° gennaio 2026: adeguamento a all'articolo 30 relativo all'**aggiornamento delle informazioni** sulla piattaforma ANC
Entro aprile 2026: elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
Entro settembre 2026: completa implementazione delle misure di sicurezza di base

Terza fase attuativa

Entro ottobre 2026: adeguamento agli articoli 23 (sugli obblighi degli organi di amministrazione e direttivi), 24 (gestione dei rischi e implementazione delle misure di sicurezza) e 29 (relativo alla banca dati dei nomi a dominio).

CONTATTI

E-MAIL

commerciale@cyberedge.it

TEL

+39 039 2847438

WEBSITE

www.cyberedge.it