

PUNTOIT



puntoit.eu



DO.IT NIS2

Una responsabilità di governance per il management e l'IT

Guida strategica all'attuazione 2026 – con scadenze operative certificate a cura di Punto IT

Introduzione

Perché la NIS2 è un tema di responsabilità aziendale

La Direttiva NIS2 nasce con l'obiettivo di rafforzare il livello complessivo di sicurezza informatica, ma il suo impatto va ben oltre la dimensione tecnica.

Per le organizzazioni rappresenta un passaggio strutturale: la cybersecurity viene formalmente riconosciuta come **tema di governance**, con responsabilità dirette in capo al management.

In questo scenario, Punto IT affianca le aziende nel trasformare l'obbligo normativo in un **percorso strutturato di adeguamento** e miglioramento continuo, che parte dall'**analisi del rischio** ma si concretizza soprattutto nella **remediation operativa**, nell'implementazione delle misure richieste e nella **gestione continuativa della sicurezza**.

La sicurezza non riguarda più solo l'IT, ma elementi centrali per il business:

- continuità dei servizi,
- resilienza operativa,
- affidabilità della filiera,
- tutela del valore aziendale.



La NIS2 come questione di business continuity e valore

La Direttiva introduce una visione estesa della sicurezza, collegandola direttamente alla tutela del valore economico e reputazionale dell'organizzazione.

La cybersecurity diventa una **leva strutturale della strategia aziendale**, non una funzione di supporto.

In questo contesto, Punto IT supporta le organizzazioni nel:

- analizzare l'impatto cyber sulla continuità dei servizi,
- identificare i processi realmente critici,
- collegare sicurezza, resilienza e obiettivi di business.

La NIS2 segna un cambio di paradigma: proteggere i sistemi significa proteggere la capacità dell'azienda di operare e crescere nel tempo.



Perché l'Unione Europea ha varato la Direttiva NIS2



La Direttiva NIS2 nasce come risposta concreta a un contesto sempre più critico dal punto di vista della sicurezza informatica. Negli ultimi anni, l'Unione Europea ha registrato un incremento esponenziale di attacchi informatici per gravità, frequenza e impatto economico, in particolare su infrastrutture critiche e aziende strategiche.

Le minacce cyber si sono evolute rapidamente:

- ransomware sempre più sofisticati,
- violazioni di dati su larga scala,
- attacchi alla supply chain con effetti a cascata,
- compromissione di servizi pubblici e sanitari.

Contemporaneamente, è emersa una forte inadeguatezza strutturale delle difese informatiche in molte aziende, soprattutto PMI. Le misure di sicurezza sono spesso frammentarie, sottodimensionate o non integrate con la governance aziendale.

La NIS2 intende quindi:

- armonizzare i requisiti di sicurezza tra gli Stati membri,
- garantire un livello minimo di protezione comune,
- stimolare le organizzazioni ad adottare un approccio proattivo alla gestione del rischio.

Con questo impianto normativo, la cybersecurity viene finalmente riconosciuta come un bene collettivo europeo, su cui costruire la fiducia nelle tecnologie digitali e nella resilienza dell'economia.

Un perimetro ampliato: più soggetti coinvolti

La NIS2 estende in modo significativo il numero di soggetti regolamentati, includendo anche organizzazioni classificate come “importanti”, sulla base di:

- dimensione aziendale,
- ruolo nella catena del valore,
- livello di digitalizzazione.

Molte aziende scoprono di essere coinvolte indirettamente, come fornitori o partner di soggetti regolamentati.

Punto IT affianca le imprese nella:

- valutazione del proprio perimetro di applicabilità,
- analisi dei rischi di coinvolgimento indiretto,
- verifica preventiva dei requisiti di compliance richiesti dalla filiera.

Ma, oltre alla valutazione del perimetro, Punto IT interviene nella definizione e nell'attuazione delle azioni correttive necessarie per colmare eventuali gap di sicurezza e compliance, accompagnando l'azienda fino alla piena implementazione delle misure richieste.



Responsabilità dirette del management



Uno degli elementi più rilevanti della NIS2 è l'attribuzione di **responsabilità diretta agli organi di gestione**.

Il management:

- approva e supervisiona le misure di sicurezza,
- risponde della loro attuazione,
- può essere sanzionato in caso di gravi inadempienze.

La delega esclusiva all'IT non è più sufficiente.

Punto IT supporta le aziende nel **costruire un modello di governance chiaro**, in cui ruoli, responsabilità e flussi decisionali siano formalizzati e condivisi tra direzione e area tecnica.





La Direttiva non impone soluzioni predefinite, ma richiede misure **adeguate e proporzionate al rischio**.

Questo richiede un approccio strutturato che includa:

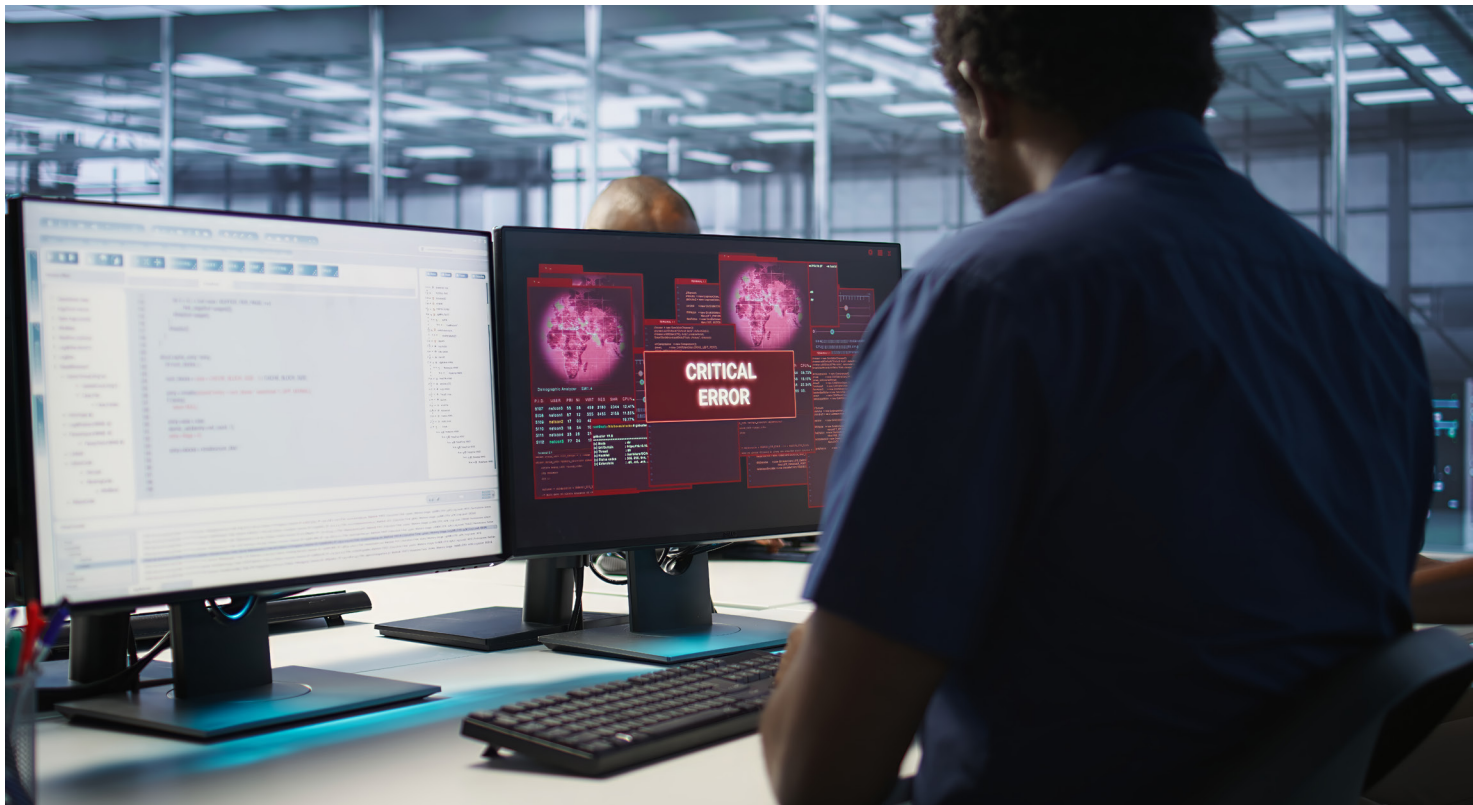
- identificazione dei processi critici,
- mappatura delle dipendenze digitali,
- valutazione degli impatti operativi e reputazionali,
- integrazione del rischio cyber nel risk management aziendale.

Punto IT accompagna le organizzazioni in questo percorso, affiancando **all'analisi del rischio la progettazione e la realizzazione degli interventi di remediation, fino alla gestione operativa e continuativa delle misure di sicurezza adottate.**

Gestione del rischio come pratica organizzativa



Gestione degli incidenti e obblighi di notifica



Dal 1° gennaio 2026 diventa obbligatoria la notifica degli incidenti significativi entro 24 ore dalla rilevazione, con:

- pre-notifica entro 24 ore (ove possibile),
- notifica dettagliata entro 72 ore,
- follow-up finale successivo.

Con la **Determinazione ACN n. 379907/2025**, in vigore dal **15 gennaio 2026**, le modalità operative sono pienamente applicabili.

Queste scadenze hanno un impatto diretto su:

- coordinamento interno,
- gestione della comunicazione,
- reputazione aziendale.

Punto IT supporta le aziende non solo nella **definizione dei processi di incident management**, ma anche nell'**attivazione delle tecnologie**, dei **presidi di monitoraggio** e dei servizi gestiti necessari a garantire la rilevazione e la **risposta agli incidenti nei tempi previsti dalla normativa**.



Le difese richieste dalla NIS2: come le realizza Punto IT

La Direttiva NIS2 impone misure tecniche e organizzative che spaziano dalla protezione degli endpoint alla gestione degli accessi, fino alla business continuity e alla governance. Si tratta di un approccio integrato alla sicurezza, che richiede non solo attività di analisi, ma anche interventi concreti di adeguamento, implementazione tecnologica e gestione continuativa.

Per rispondere in modo strutturato a questi requisiti, **Punto IT ha sviluppato un modello di servizi integrati che unisce assessment, remediation e presidio operativo, con soluzioni modulari e scalabili già allineate agli standard richiesti dalla Direttiva.**

DO.IT NIS2: pacchetto verticale dedicato a Security e Compliance per le aziende soggette alla Direttiva NIS2.

Progettato per accompagnare le organizzazioni in un percorso completo di adeguamento, DO.IT NIS2 unisce:

- strumenti per la compliance normativa, audit di rete, password management e supporto GDPR;
- soluzioni di protezione avanzata di dispositivi, email e rete, con firewall UTM, autenticazione multi-fattore e attività di vulnerability assessment.

L'approccio non si limita alla verifica dei requisiti, ma include la **remediation delle eventuali non conformità, l'implementazione delle misure di sicurezza e la loro gestione continuativa nel tempo.**

A completamento del modello, Punto IT mette a disposizione ulteriori servizi specialistici che contribuiscono al rafforzamento della postura di sicurezza e della resilienza operativa:

- DO.IT Backup.IT: soluzioni di backup e disaster recovery per dati locali e cloud, con funzionalità di legal hold e ripristino rapido.
- DO.IT Realize.IT: gestione centralizzata delle postazioni di lavoro e dei servizi Microsoft 365, con SLA garantiti.
- DO.IT Talk: sistemi di comunicazione sicuri basati su VoIP e integrazione con Microsoft Teams.
- DO.IT Managed Workplace: postazione "chiavi in mano" con hardware garantito, device management, sicurezza e supporto inclusi.

L'obiettivo è rendere la conformità NIS2 un processo strutturato, affidabile e sostenibile, trasformando un obbligo normativo in un percorso concreto di rafforzamento della sicurezza e maturità organizzativa.

Scadenze operative 2026 – riferimenti normativi

1° gennaio 2026

Avvio obbligo di notifica incidenti significativi

Fonte: ACN – Determinazione 379907/2025

15 gennaio 2026

Entrata in vigore delle regole operative ACN per la gestione degli incidenti

1–28 febbraio 2026

Finestra annuale per registrazione o aggiornamento dati sul portale ACN

Fonte: Determinazione 379887/2025

Entro 31 ottobre 2026

Implementazione delle misure di sicurezza di base

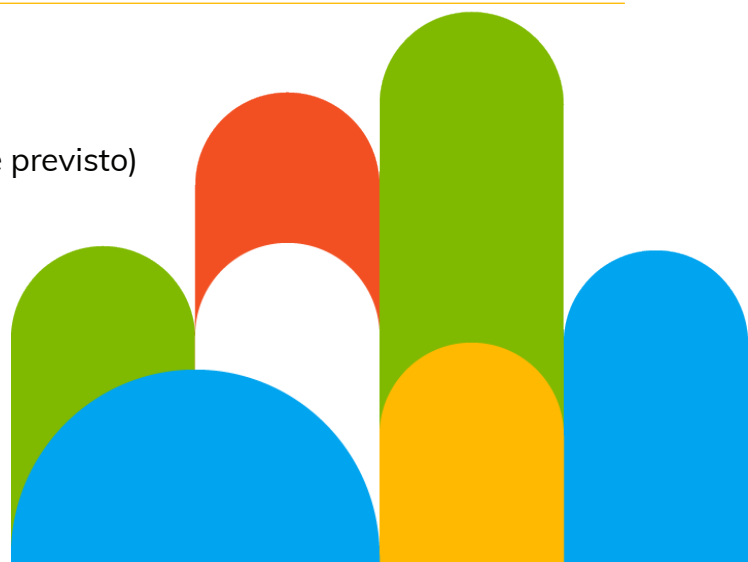
Fonte: analisi coerente con tempistiche ACN (18 mesi)

Entro fine 2026

Conformità completa per molti soggetti inseriti in elenco nel 2025

Entro 31 dicembre 2027

Adeguamento finale per soggetti “importanti” (se previsto)



Sanzioni e impatti: il costo della non conformità

Le sanzioni possono arrivare fino a 10 milioni di euro o al 2% del fatturato annuo globale, ma il rischio principale è rappresentato da:

- perdita di continuità operativa,
- danni reputazionali,
- esclusione da bandi o supply chain strategiche.

Affrontare la NIS2 in modo frammentato espone l'azienda a rischi che vanno oltre l'aspetto sanzionatorio.



Fonti ufficiali e normative

ACN – Portale ufficiale NIS

Determinazione ACN n. 379907/2025 – gestione incidenti

Determinazione ACN n. 379887/2025 – portale e registrazione

Decreto Legislativo 138/2024 – Recepimento Direttiva NIS2



Un approccio strutturato alla NIS2 consente alle organizzazioni di chiarire ruoli e responsabilità interne, rafforzare il dialogo tra direzione e area IT e aumentare la resilienza complessiva.

Con il supporto di Punto IT, la compliance si trasforma in un percorso di crescita organizzativa, non solo in un adempimento normativo.

Vuoi capire come applicare concretamente la direttiva NIS2 nella tua realtà?

Contattaci e prenota una consulenza con uno specialista per valutare il tuo livello di maturità e definire i prossimi passi.



+39 0461
1637322



www.puntoit.eu
info@puntoit.eu



Via A. Pranzelores 29,
38121 Trento



PUNTOIT