Insights

protiviti®
Global Business Consulting

Technology Consulting

Luglio 2024

Direttiva NIS 2 (Network and Information Security): i punti chiave per l'applicazione

A cura di:

Enrico Ferretti

Nicola Dalla Benetta

La **Direttiva (UE) 2022/2555 (NIS 2),** recepita in Italia tramite Decreto Legislativo approvato da parte del Consiglio dei Ministri lo scorso **10 Giugno 2024**, rappresenta un'evoluzione significativa nell'ambito della cybersecurity a livello europeo, sottolineando il ruolo cruciale degli Stati membri nella creazione e nel mantenimento di un ecosistema digitale sicuro e resiliente, in un contesto geopolitico caratterizzato da numerosi conflitti che non si limitano all'ambito fisico, ma coinvolgono in maniera sempre più rilevante il cyber spazio.

Tra gli obiettivi principali della NIS 2 rientrano il **potenziamento della resilienza delle infrastrutture critiche** e la **promozione della cooperazione tra gli Stati membri**. La direttiva mira altresì a garantire una **risposta transfrontaliera coordinata** alle minacce informatiche e ad **aumentare la trasparenza e la responsabilità** nelle organizzazioni considerate critiche.

Il recepimento della Direttiva NIS 2 da parte degli Stati membri è previsto **entro il 17 ottobre 2024**, definendo e pubblicando le misure necessarie, informando le organizzazioni interessate e monitorando l'effettiva implementazione delle misure volte alla gestione dei rischi e delle minacce di cyber security.

Contesto Normativo

La Direttiva NIS 2, recepita in Italia tramite Decreto Legislativo approvato da parte del Consiglio dei Ministri lo scorso 10 Giugno 2024, si inserisce in un quadro più ampio di adattamento e risposta alle sfide determinate dalla digitalizzazione, confermando l'impegno transfrontaliero dell'Unione Europea nel promuovere una **cyber-resilienza** efficace e coordinata a livello continentale.

La NIS 2 **sostituisce** la precedente Direttiva NIS del 2016, recepita in Italia nel 2018 e rafforzata, attraverso l'istituzione del Perimetro di Sicurezza Nazionale Cibernetica (**PSNC**), arricchendo in maniera sinergica il fitto quadro normativo europeo in materia di Cyber Security e Resilience delle Infrastrutture Critiche che comprende, tra gli altri, il Digital Operational Resilience Act (**DORA**), il **Cybersecurity Act**, il General Data Protection Regulation (**GDPR**) e la recente Direttiva sulla Resilienza delle infrastrutture critiche (**CER, Critical Entities Resilience**).

Punti chiave per l'applicazione

Rispetto alla NIS, la nuova Direttiva supera la distinzione tra Operatori di Servizi Essenziali **(OSE)** e Fornitori di Servizi Digitali **(FSD),** introducendo le categorie di **Soggetti Essenziali** e **Soggetti Importanti** ed ampliando così la lista dei settori di servizi essenziali coinvolti.

Mentre la NIS lasciava agli Stati membri una certa discrezionalità nella specifica identificazione degli operatori, la NIS 2 stabilisce criteri più chiari per l'individuazione dei soggetti rientranti nell'ambito di applicazione[1]. In particolare, sono inclusi soggetti pubblici o privati dei settori definiti ad "**Alta criticità**" (**Allegato I**) e "**Altri settori critici**" (**Allegato II**), che rientrano almeno nella categoria delle medie imprese[2].

Allegato I – Settori ad Alta Criticità
Energia (energia elettrica, teleriscaldamento e tele raffrescamento, petrolio, gas, idrogeno)
Trasporti (aereo, ferroviario, per via d'acqua, su strada)
Settore bancario
Infrastrutture dei mercati finanziari
Settore sanitario
Acqua potabile
Acque reflue
Infrastrutture digitali
Gestione dei servizi TIC
Pubblica Amministrazione
Spazio

Allegato II – Altri Settori Critici
Servizi postali e di corriere
Gestione dei rifiuti
Fabbricazione produzione e distribuzione di sostanze chimiche
Produzione, trasformazione e distribuzione di alimenti
Fabbricazioni di dispositivi medici e medico diagnostici in vitro, di computer e prodotti di elettronica e ottica, di apparecchiature elettriche, di macchinari e apparecchiature, di autoveicoli, rimorchi e semirimorchi, di altri mezzi di trasporto
Fornitori di servizi digitali
Ricerca
Settore dei servizi postali e di corriere
Fornitori di servizi digitali
Ricerca

[1] *La Direttiva conferisce allo Stato membro, Art.3 e), di identificare qualsiasi altro soggetto di cui all'allegato I o II come soggetto essenziali*

[2] *Si definisce media impresa una impresa con meno di 250 dipendenti, il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio annuo non supera i 43 milioni di EUR*

Si riporta di seguito una sintesi dei criteri per identificare i **Soggetti Essenziali** e i **Soggetti Importanti** secondo la Direttiva NIS 2:

Entro il **17 aprile 2025** gli Stati membri sono tenuti a definire un elenco dei **Soggetti Essenziali e Importanti**.

Tale elenco dovrà essere riesaminato periodicamente, **almeno ogni due anni**, e aggiornato quando necessario. La Direttiva NIS 2 stabilisce che gli Stati membri debbano garantire che i soggetti inclusi nel campo di applicazione implementino una serie di misure organizzative e tecniche.

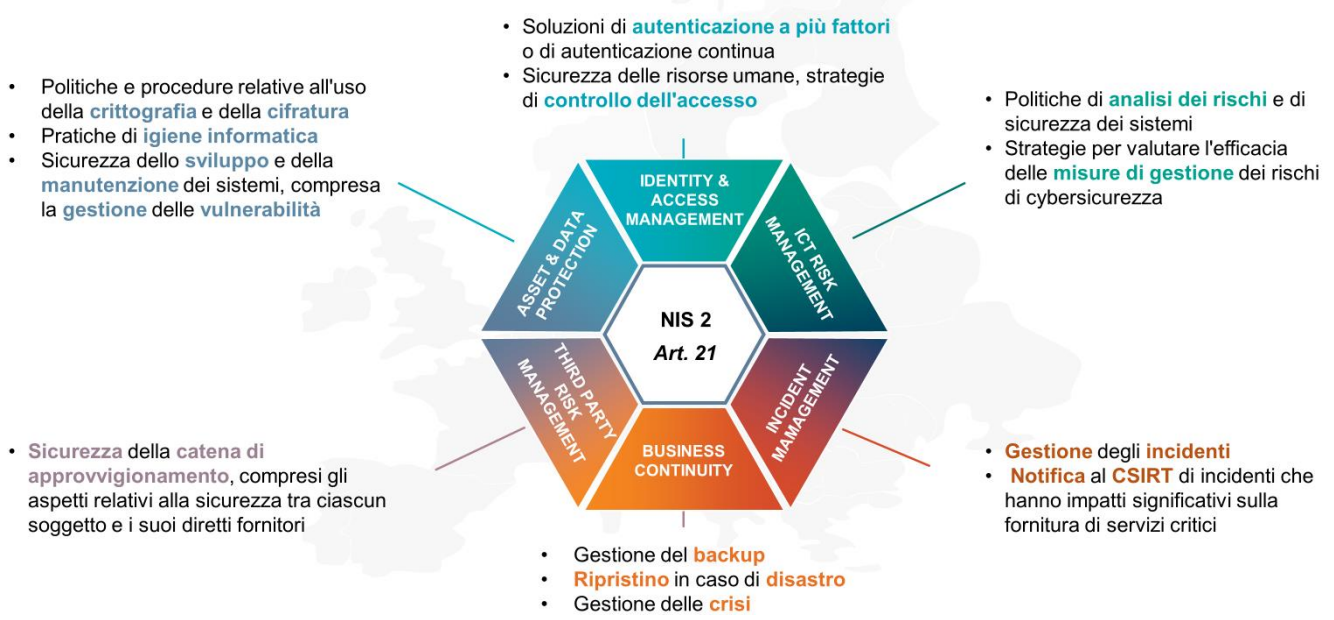
Al riguardo, è necessario assicurare:

- la partecipazione attiva della **governance** dei Soggetti Essenziali e Importanti nella gestione dei rischi legati alla sicurezza informatica **(Art. 20)**;
- l'adozione di **misure per la gestione dei rischi di sicurezza** informatica da parte dei Soggetti Essenziali e Importanti, utilizzando un approccio che integri aspetti tecnici, operativi e organizzativi **(Art 21)**;
- la **segnalazione tempestiva** da parte dei Soggetti Essenziali e Importanti di qualsiasi incidente significativo **(Art 23)**.

Per conseguire il rispetto delle misure di gestione dei rischi legati alla sicurezza informatica, la Direttiva NIS 2 permette a ogni Stato membro di decidere se imporre ai Soggetti Essenziali e Importanti l'uso di specifici prodotti, servizi e processi ICT, sviluppati internamente o acquisiti da terzi, che siano certificati secondo i **sistemi europei di certificazione della sicurezza informatica (Art 24)**.

Le misure dovranno includere, tra l'altro, l'implementazione di **protocolli** di comunicazione sicura, la **formazione continua** del personale in materia di cybersecurity, l'adozione di **tecnologie** di rilevamento e risposta agli incidenti, lo sviluppo di **piani** di continuità operativa e di ripristino, e la **collaborazione** con le autorità nazionali per garantire una risposta tempestiva e coordinata agli incidenti.

Di seguito i **punti chiave** dei requisiti stabiliti dall'Articolo 21:



L'obiettivo è prevenire o ridurre al minimo l'impatto degli incidenti non solo per i destinatari dei servizi dei Soggetti Essenziali e Importanti ma anche per altre **infrastrutture e servizi interconnessi**, assicurando così la resilienza complessiva dell'Unione Europea.

Regime Sanzionatorio

La Direttiva NIS 2 definisce un **sistema di vigilanza** più rigoroso per la sicurezza informatica e sanzioni più severe per i soggetti inadempienti.

Le organizzazioni in ambito saranno sottoposte a **controlli** più frequenti e approfonditi e dovranno **notificare** tempestivamente qualsiasi incidente informatico che abbia un impatto significativo sulla fornitura dei propri servizi e, in particolare, presentare al relativo CSIRT o se del caso l'autorità competente:

- un **preallarme** entro 24 ore dal momento in cui sono stati informati dell'incidente significativo;
- una **notifica** entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo;
- una **relazione finale** dettagliata entro un mese dalla trasmissione della notifica dell'incidente di cui al punto precedente.

Il mancato rispetto degli obblighi previsti comporterà sanzioni pecuniarie amministrative che potranno arrivare fino al maggiore tra **€ 10.000.000** o **2%** del fatturato mondiale annuo dell'azienda per i **Soggetti Essenziali** e **€ 7.000.000** o **1,4%** del fatturato mondiale annuo per i **Soggetti Importanti**.

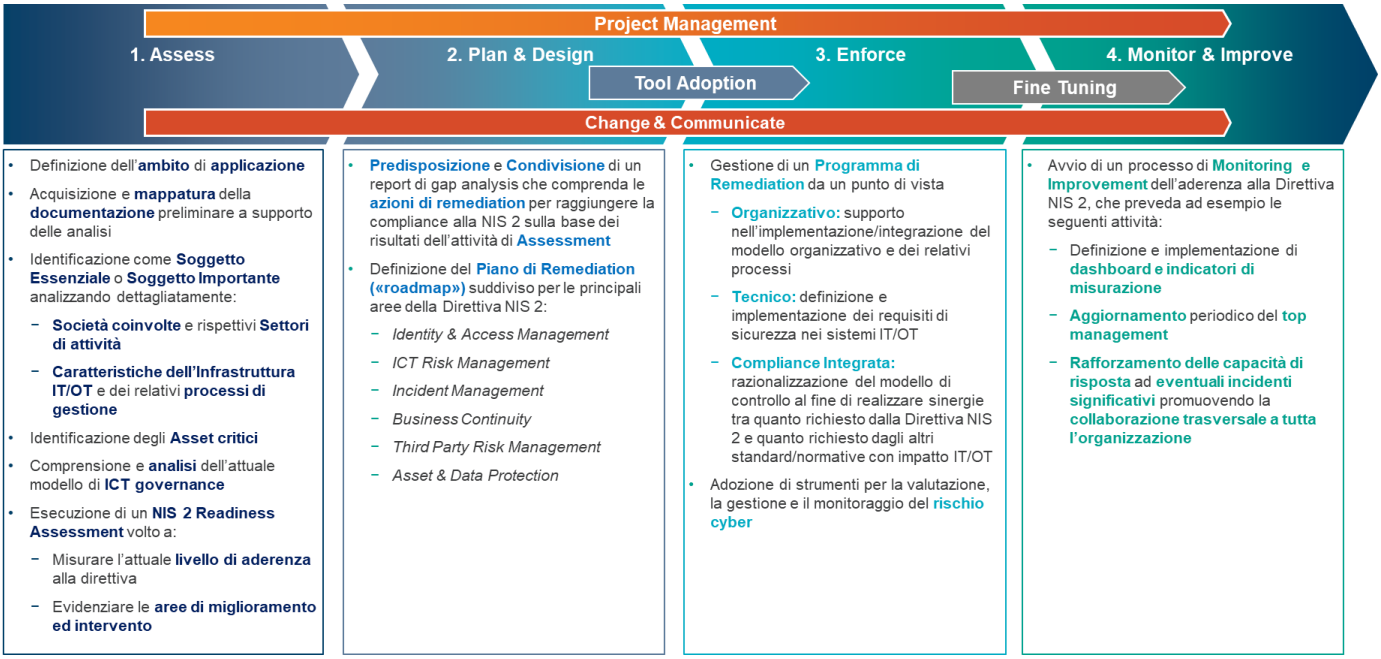
Le autorità preposte sono inoltre tenute a segnalare tempestivamente al Garante per la Protezione dei Dati Personali qualsiasi violazione da parte di un soggetto NIS che possa potenzialmente mettere a rischio i dati dei cittadini.

Il Garante, a sua volta, ha il potere di irrogare ulteriori sanzioni al soggetto inadempiente

Approccio Protiviti

Sulla base della vasta esperienza sviluppata in materia di gestione del rischio e di compliance, con particolare riferimento agli ambiti Cyber Security, Information & Operation Technology, Protiviti ha definito un approccio specifico per l'adeguamento alla Direttiva NIS 2.

Tale approccio viene adattato al contesto e al business del cliente, analizzando le **caratteristiche della società** (o delle società coinvolte nel caso di gruppi), il - o i loro - rispettivi **settori di attività**, l'**infrastruttura IT/OT** e i relativi **processi di gestione**.



Al fine di supportare le organizzazioni nel raggiungimento della compliance e nella sua gestione nel continuo, Protiviti si avvale di specifici strumenti che consentono di avere una visione completa del **livello di conformità** dell'organizzazione e ne permettono il monitoraggio, anche attraverso **dashboard dedicate** e **report personalizzati** sulla base delle esigenze specifiche (es. report per il top management).

Più nel dettaglio, il **NIS 2 Readiness Framework**, consente l'esecuzione di una valutazione del livello di maturità dell'azienda sui diversi ambiti d'intervento previsti (*Identity & Access Management, Ict Risk Management, Incident Management, Business Continuity, Third Party Risk Management, Asset & Data Protection*) rispetto ai requisiti richiesti dalla Direttiva e l'identificazione delle azioni da intraprendere per il raggiungimento della compliance.

Poiché la NIS 2 coinvolge diversi ambiti e funzioni aziendali, l'approccio mira a favorire la collaborazione trasversale a tutta l'organizzazione, in modo da **rafforzare la capacità di risposta a eventuali incidenti significativi** garantendo al contempo sia la compliance alla Direttiva che la resilienza del business.

Infine, il **NIS 2 Readiness Framework** di Protiviti supporta le organizzazioni nella gestione delle comunicazioni con le autorità competenti - rafforzando l'attività dell'Information Sharing - e nell'identificazione delle interconnessioni tra requisiti normativi di diversi standard e/o normative di settore, razionalizzando in un'ottica di compliance integrata i sistemi di governo e controllo, in modo da rendere più sostenibile ed efficace la loro gestione.

CONTATTI

Enrico Ferretti | Managing Director | enrico.ferretti@protiviti.it

Nicola Dalla Benetta | Associate Director | nicola.dallabenetta@protiviti.it

Raffaele Lambiase | Manager | raffaele.lambiase@protiviti.it