Deloitte.

Schema di decreto legislativo recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (Atto n. 164)

Memoria Deloitte

19 luglio 2024

1. Introduzione

La **Direttiva (UE) 2022/2555** del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (di seguito "Direttiva NIS2"), che abroga la precedente Direttiva NIS, rappresenta un tassello aggiuntivo nella tutela della cybersicurezza nell'Unione Europea. La NIS2 **introduce requisiti più rigorosi** per la gestione dei rischi e la notifica degli incidenti, mirando a rafforzare la resilienza Cyber dei settori strategici già presenti nella Direttiva NIS e introducendone allo stesso tempo di nuovi, **ampliando** così **l'ambito** di **applicazione**.

Lo stato italiano, come gli altri stati europei, è chiamato a recepire la Direttiva NIS2 nel proprio ordinamento **entro** il **17 ottobre 2024**.

Il presente documento mira a fornire **proposte integrative** a quanto già indicato all'interno dello schema di decreto legislativo per il recepimento della Direttiva (Atto di Governo n.164), in particolare rispetto ad uno degli aspetti chiave di confronto[1], ossia la definizione dell'**approccio per l'adozione da parte delle imprese** degli obblighi di cui al Capo IV[2] dello schema di decreto legislativo.

Le **proposte** di seguito descritte hanno l'obiettivo di **agevolare l'implementazione** degli **obblighi**, assicurando un buon bilanciamento tra gli obiettivi di cybersicurezza della nazione e l'impegno finanziario, amministrativo e tecnico-operativo richiesto ai soggetti inclusi in ambito. Queste si auspica che possano essere valutate rispetto a questo schema e/o provvedimenti attuativi, e alle successive determinazioni che lo stesso prevede all'art. 31 e più in generale al capo VI, art. 40 (Attuazione).

Quanto esposto è frutto di un'analisi condotta dagli specialisti **Deloitte** che, attraverso il costante impegno e l'esperienza maturata al fianco di aziende pubbliche e private coinvolte in progetti di conformità a regolamenti nazionali e internazionali di cybersicurezza, e grazie al confronto su diversi tavoli istituzionali e settoriali, ha acquisito una **prospettiva privilegiata** dell'ecosistema e una conoscenza approfondita delle principali implicazioni e sfide per le imprese.

Per quanto riguarda la Direttiva NIS2, e le sue trasposizioni nazionali, Deloitte ha avviato nel 2023 un tavolo di lavoro a livello europeo al fine di facilitare lo scambio di informazioni e il confronto sui requisiti normativi e sulle sfide poste dalla Direttiva stessa alle organizzazioni interessate. Tale tavolo di lavoro ha permesso di condividere esperienze, discutere best practices, armonizzare le interpretazioni normative e sviluppare strategie comuni per la Compliance alla Direttiva. Nell'ambito di questo tavolo, Deloitte ha recentemente pubblicato un white paper[3] che analizza lo stato di recepimento della Direttiva NIS2 in diversi paesi, tra cui Italia, Germania, Belgio e Austria, e mette in luce i principali aspetti delle leggi/proposte di legge per il recepimento della Direttiva negli ordinamenti nazionali.

Si precisa, inoltre, che i contenuti presentati sono stati oggetto di condivisione con operatori potenzialmente coinvolti nel perimetro di conformità; pertanto, non si esclude che questi possano essere stati proposti nell'ambito di altre consultazioni.

[1] La direttiva e lo schema di recepimento affrontano diversi ambiti oltre a quello indicato che include ad esempio la regolamentazione per la divulgazione coordinata delle vulnerabilità (CVD) e le specifiche funzioni di coordinamento attribuite a CSIRT nazionali; oppure l'implementazione delle misure di cooperazione, al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala.
[2] Obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente
[3] Il white paper "Navigating NIS2 Compliance. July 2024 - A current view on local NIS2 legislations for organizations with cross-border European operations" è disponibile al link Navigating NIS2 Compliance (deloitte.com)

2. Executive Summary

La sfida principale per l'Italia e gli altri Stati Membri dell'UE nell'attuare la Direttiva NIS2 consiste nel garantire che il raggiungimento degli obiettivi stabiliti dall'Unione in materia di cybersicurezza avvenga tutelando le imprese da oneri eccessivi e sproporzionati in termini di impegno e risorse.

In particolare, si evidenziano due aspetti peculiari da considerare:

- **L'eterogeneità dei soggetti coinvolti.** In ambito NIS2 ricadono settori molto diversi tra loro, ma anche soggetti molto differenti all'interno degli stessi settori;
- **La complessità attuativa richiesta** per l'adozione di misure di sicurezza su tutti i sistemi presenti all'interno dei soggetti, non solo sui sistemi associati ai servizi più critici[4]. Ciò impone come diretta conseguenza l'identificazione di ambiti, ad esempio sistemi e infrastrutture IT, OT[5] e/o IoT[6], differenziati per impatto e livello di rischio.

Lo schema di decreto legislativo prevede diversi elementi che hanno l'obiettivo di indirizzare queste sfide, come ad esempio all'interno dell'art. 24, comma 1, dove si richiamano i **principi di adeguatezza** e **proporzionalità** in relazione all'adozione di misure tecniche, operative e organizzative per gestire i rischi, o nell'ambito dell'art. 31, ove si menzionano criteri di **proporzionalità** e **gradualità** nella definizione degli obblighi in materia di gestione del rischio di sicurezza cibernetica e di notifica di incidenti.

Partendo da questi, si propongono elementi aggiuntivi da valutare, alcuni dei quali si ispirano a nuovi principi, altri invece che estendono e declinano ulteriormente quelli già previsti dallo schema di decreto:

- **Consistenza, comparabilità e ripetibilità nell'applicazione delle misure**. In riferimento all'art. 24, comma 1, si evidenzia che un Framework di misure che sia quello precedentemente adottato per la conformità alla Direttiva NIS e alla Legge 133/2019 (PSNC) agevolerebbe il percorso a quei soggetti che negli anni hanno già intrapreso un percorso di Compliance.
- **Proporzionalità. La proposta è di estendere i criteri di differenziazione di cui all'art. 31, introducendo obblighi e misure proporzionati alle caratteristiche del soggetto**. Concretamente, significa differenziare gli obblighi – e specificatamente misure e attività di elencazione - secondo ulteriori elementi, quali settore/sottosettore, tipologia di soggetto e individuazione del soggetto (i.e. essenziale o importante)[7], richiedendo adempimenti proporzionati in base a tale differenziazione.
- **Gradualità. La proposta è quella di estendere il principio di gradualità di cui all'art. 31, prevedendo dei modelli più basilari per poi progredire verso soluzioni più articolate e al tempo stesso anche complesse nella loro attuazione**. Concretamente, significa adottare un approccio per fasi che prevede in una prima fase di adottare misure avanzate sui sistemi e le reti o i servizi altamente critici di pertinenza del soggetto, in una seconda fase, adottare misure di base per il restante insieme dei servizi e sistemi appartenenti al soggetto e, in una ulteriore fase (eventuale), prevedere differenziazioni aggiuntive tra questi. Approccio analogo si suggerisce sia applicato anche per completare l'elencazione di attività e servizi svolti dai soggetti secondo quanto previsto dall'art. 30.
- **Flessibilità attuativa** in due specificazioni:
    - **possibilità per le imprese di adottare metodologie e approcci propri per la differenziazione all'interno dell'organizzazione dei sistemi** su cui applicare le misure di sicurezza (riferimento art. 30). Concretamente, significa lasciare al soggetto la facoltà di scegliere come effettuare la

[4] Il concetto è precisato nelle linee guida della Commissione Europea (i.e., Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive))
[5] Operational Technology
[6] Internet of Things
[7] Già previsti per modalità, termini e tempi di implementazione

categorizzazione di rilevanza sulla base di criteri di valutazione e scale identificati dallo stesso (e.g. Business Impact Analysis).

- possibilità per le imprese di adottare metodologie e approcci propri per la definizione, implementazione e verifica di efficacia delle misure di sicurezza. In pratica si propone di lasciare all'operatore la facoltà di definire quali soluzioni tecniche, organizzative e di processo adottare per rispondere alle singole misure previste dall'art. 24 in maniera autonoma e in accordo alla valutazione del rischio specifica da questo effettuata. Questo approccio è in coerenza con quanto già previsto dai principali standard e best practice di settore (es. ISO 27001), che lasciano ai soggetti la possibilità di applicare i processi di analisi del rischio più opportuni per giustificare che le scelte compiute, siano adeguate al livello di rischio e criticità delle attività e servizi che il soggetto svolge.

Restano valide linee guida e indicazioni che potranno essere eventualmente fornite per un'armonizzazione dei criteri.

- Priorità. La proposta è di prevedere tempistiche che permettano ai soggetti di focalizzarsi sui sistemi più critici, prevedendo l'adeguamento su tutti gli altri in modo graduale, secondo un approccio basato sul rischio. Concretamente, significa definire tempi di recepimento per le misure sulle risorse informatiche o i servizi più critici svolti dal soggetto e far partire i tempi per il recepimento delle misure sui sistemi meno critici al termine del piano di adeguamento che ha interessato i primi. Questo per consentire alle organizzazioni di prioritizzare al meglio gli impegni.

Si evidenziano inoltre ulteriori elementi rilevanti, alcuni dei quali potrebbero costituire elemento di riflessione sul più ampio tavolo di collaborazione Europeo:

Incentivi alle imprese: al fine di rendere meno onerosi gli adempimenti di conformità per i soggetti interessati, è auspicabile prevedere fondi e contributi per le imprese che possano agevolare l'implementazione delle misure.

Attività ispettive e di supervisione: considerate le soglie previste dal criterio di individuazione dei soggetti su base dimensionale di cui all'art. 3, e di conseguenza il numero di soggetti che in Italia ricadrà in ambito, potrebbero essere valutate, come fatto ad esempio da altri Paesi europei (es. Austria e Finlandia), soluzioni più scalabili che permettano di ottemperare alle disposizioni previste dal capo V "monitoraggio, vigilanza ed esecuzione" dello schema di Decreto.

Semplificazione degli obblighi di registrazione: valutare l'adozione di un approccio che consenta di alleggerire l'obbligo di registrazione dei soggetti in ambito, riconoscendo ai gruppi la possibilità di una gestione centralizzata delle registrazioni delle proprie Legal Entities che operano sul territorio nazionale.

Armonizzazione a livello Europeo delle modalità di adozione delle misure di sicurezza e di notifica degli incidenti di sicurezza: valutare le modalità più opportune di gestione degli obblighi di implementazione delle misure di sicurezza e notifica degli incidenti di sicurezza, tenendo in considerazione le specificità dei gruppi che operano su più paesi.

Ruolo delle Certificazioni di settore: è auspicabile comprendere quale sarà il ruolo di eventuali certificazioni sulla Sicurezza (es. ISO 27001, …) e considerarne il valore, eventualmente come sostituto dell'evidenza di Compliance, in particolare quando l'ambito di certificazione è costituito da tutti i sistemi aziendali.

3. Analisi delle Sfide per le Imprese

La Direttiva NIS2 e lo schema di recepimento italiano pongono in capo alle aziende pubbliche e private coinvolte numerose sfide per garantire la conformità.

Deloitte - attraverso il suo costante impegno e supporto su tematiche di cybersicurezza - ha acquisito una vista privilegiata dell'ecosistema dei soggetti coinvolti nella conformità alla Direttiva NIS1 e/o alla legge PSNC o dei nuovi soggetti coinvolti nella conformità alla NIS2 – che le ha permesso di identificare le principali implicazioni e sfide:

Chiara identificazione dell'ambito – lo schema prevede che le imprese si auto-dichiarino (differentemente dalla NIS1 che prevedeva una nomina diretta da parte dello Stato Membro) come soggetti essenziali o importanti. Ciò comporterà un impegno non indifferente per quelle realtà, come i gruppi e le società multi-Business o anche i gruppi internazionali, per i quali sarà necessario analizzare - a livello nazionale ed europeo - sia i settori di appartenenza delle singole società del Gruppo, ma anche la dimensione in termini di dipendenti e fatturato o bilancio annuo (i.e. tenendo conto potenzialmente anche di società collegate e/o associate), in accordo con quanto previsto dalla Raccomandazione 2003/361/CE. La considerazione delle società collegate e/o associate ai fini della qualifica dimensionale delle imprese determina a sua volta un ulteriore e significativo elemento di complessità, se si tiene conto che ciò potrebbe comportare un notevole ampliamento del perimetro di conformità a carico delle imprese in funzione di razionali pertinenti ad un diverso ambito normativo; la Raccomandazione 2003/361/CE si colloca, infatti, nell'ambito della disciplina europea in materia di aiuti di Stato alla cui base sussistono esigenze e considerazioni diverse da quelle proprie dei temi della resilienza e sicurezza informatica. L'applicazione sistematica del criterio dell'indipendenza dell'impresa in termini di sistemi informativi e di rete (i.e. clausola di salvaguardia di cui all'art. 3, comma 4, dello schema) assume pertanto un'importanza fondamentale nel garantire la proporzionalità, l'adeguatezza e la coerenza del perimetro di conformità agli obiettivi specifici della Direttiva NIS2.

Approcci e tempistiche di conformità differenti – la Direttiva NIS2 pur avendo l'obiettivo meritevole di definire il livello comune di cybersicurezza nell'Unione Europea lascia comunque agli Stati Membri la libertà di definire specifiche modalità e tempistiche di attuazione, con potenziali implicazioni in termini di armonizzazione a livello comunitario. I gruppi internazionali dovranno gestire diversi approcci (e.g. per implementazione delle misure di cybersicurezza o per la notifica degli incidenti) e tempistiche di conformità che potranno variare a seconda del paese in cui operano. Analogamente, all'interno di un singolo paese, ci potranno essere potenzialmente gruppi multi-Business con società chiamate ad ottemperare ai requisiti previsti per i soggetti essenziali e altre invece a quelli previsti per gli importanti. Saranno da vagliare infatti le implicazioni associate alle differenze tra settori, ma anche quelle tra soggetti all'interno dei singoli settori.

Complessità per l'implementazione delle misure di sicurezza su tutti i sistemi IT, OT e IoT – l'estensione dell'ambito di applicabilità a tutti gli asset aziendali, a differenza della NIS1 che circoscriveva unicamente alle risorse informatiche e ai servizi critici, implica un'importante estensione di ambito per tante imprese che erano già in NIS1, ma soprattutto comporta un ingente impegno per tutti i numerosi nuovi operatori NIS2. L'adozione delle misure di sicurezza sarà guidata dai principi di proporzionalità e adeguatezza direttamente richiamati dalla Direttiva, che richiederanno alle imprese coinvolte di:

- Completare valutazioni di impatto (i.e. BIA) su tutta l'organizzazione al fine di differenziare i sistemi in ragione della loro criticità;
- Definire, implementare e monitorare l'efficacia di soluzioni tecniche, organizzative, di processo adottate per rispondere alle misure richieste in maniera differenziata sulla base del rischio, sia sugli ambienti IT che su quelli OT.

Entrambe le attività risultano complesse in termini tecnici, di commitment e di risorse. Questo in particolare per imprese di medie dimensioni, con un livello di maturità iniziale in ambito cybersicurezza, ma anche per le grandi imprese che avranno un perimetro più ampio di conformità da gestire.

Nei capitoli successivi sono presentati i principi e aspetti che si ritiene possano agevolare i soggetti nell'indirizzare le sfide identificate.

4. Proposta per applicazione principio di Proporzionalità

Si premette quanto riportato nello schema di decreto che riprende la distinzione operata dalla Direttiva NIS2 tra le due categorie di soggetti: essenziali e importanti. Come noto, la differenziazione tra queste due categorie è subordinata al settore specifico di appartenenza del soggetto - come presentato negli Allegati I, II, III e IV dello schema di d.lgs. - e a criteri dimensionali (cioè, grandi imprese o medie imprese)[8]. Al momento, gli operatori dei settori degli Allegati I e III prevedono una differenziazione all'interno del settore stesso tra essenziali ed importanti, mentre i soggetti appartenenti ai settori dell'Allegato II non presentano distinzioni e sono tutti categorizzati come importanti, a meno di identificazioni puntuali effettuate dallo Stato. Ad esempio, il settore "Energia" prevede che le grandi aziende siano categorizzate come essenziali mentre le medie come importanti, mentre per la "Produzione, trasformazione e distribuzione di alimenti" o i "Servizi postali e di corriere" non si prevede alcuna differenziazione. I soggetti dell'Allegato IV, invece, dovranno essere identificati ed eventualmente categorizzati come essenziali dall'Autorità nazionale competente NIS.

Nello schema, all'art. 24 e specificatamente all'art. 31, il termine "proporzionalità" è stato associato ad entità differenti: i) obblighi; ii) termini, modalità e tempi di implementazione degli obblighi; iii) misure, prevedendo criteri di applicazione differenti per ciascuna di queste entità.

Per gli **obblighi**, di cui all'art. 31, comma 1, e per le **misure**, di cui all'art. 24, comma 1, lett. b), la proporzionalità è proposta secondo criteri di dimensione dei soggetti, esposizione dei soggetti a rischi e probabilità che si verifichino incidenti.

Per i **termini, modalità e tempi di implementazione degli obblighi**, di cui all'art. 31, comma 2, la proporzionalità è proposta invece rispetto alle caratteristiche del soggetto: categoria di rilevanza, settore/sottosettore, tipologia di soggetto e individuazione del soggetto (i.e. essenziale o importante).

Si **propone** di **rivedere** ed **estendere** la **lista dei criteri di proporzionalità** per gli **obblighi**[9], ad esempio prevedendo una maggiore e concreta considerazione della tipologia di soggetto (i.e. essenziale o importante) e/o del settore/sottosettore di appartenenza. Si suggerisce, ad esempio, di valutare una **differenziazione nell'ambito dei soggetti importanti**, che possa contemplare ulteriori gruppi per poter differenziare in maniera proporzionale gli obblighi, oltre alle prescrizioni per i regimi di supervisione.

La distinzione potrà essere eseguita applicando, ad esempio, uno o più dei seguenti criteri:

- **Dimensione del soggetto**, distinguendo tra grandi e medie imprese;
- **Settore/Tipologia** di appartenenza del soggetto, distinguendo fra settori/tipologie più e meno critici per la fornitura dei servizi e delle funzioni associati;
- **Soglie di criticità** per qualificare il grado di rilevanza delle imprese e dei rispettivi servizi erogati in funzione di criteri, quali ad esempio: copertura territoriale o dei cittadini serviti, soglie di produzione del prodotto/servizio, ecc.

A titolo esemplificativo, a valle della redazione degli elenchi da parte dell'Autorità nazionale competente NIS, si potrebbe considerare una semplice distinzione in **due gruppi per i soggetti identificati come importanti,** impiegando una combinazione dei primi due criteri che permetta di distinguere tra:

- **Soggetti Importanti a priorità alta:**
  - Grandi imprese che operano nell'ambito di settori classificati come strategici
  - Categorie di soggetti che, a prescindere dalle dimensioni, svolgono funzioni e/o erogano servizi considerati strategici
- **Soggetti Importanti a priorità bassa:**
  - Grandi e Medie imprese che operano nell'ambito di settori classificati come NON strategici

[8] Come disciplinato all'interno della Raccomandazione 2003/361/CE

[9] Obblighi di elencazione, caratterizzazione e categorizzazione delle attività e dei servizi (Art. 30), misure (Art. 24) e notifica incidenti (Art. 25), e altri

- Categorie di soggetti che, a prescindere dalle dimensioni, svolgono funzioni e/o erogano servizi considerati NON strategici

Analogamente a quanto già proposto per gli obblighi, si **propone** di **rivedere** ed **estendere** i **criteri** di **proporzionalità** applicati alle **misure tecniche, operative e organizzative** di cui all'art. 24, comma 1, prevedendo una maggiore e più specifica differenziazione per settore/sottosettore, tipologia di soggetto e individuazione del soggetto (i.e. essenziale o importante). Ad esempio, **prevedendo un numero e tipologia di misure da applicare ai soggetti essenziali differenziata da quelli importanti**, e **ulteriormente differenziata tra soggetti importanti**. Questo approccio è stato ad esempio previsto dal Belgio nella legge di recepimento, ove la proporzionalità è stata applicata a livello di misure distinte tra soggetti essenziali (elenco completo) e importanti (baseline).

Per i soggetti essenziali si potrà prevedere di implementare una lista di misure più ampia ed articolata, ad esempio, prendendo a riferimento quanto ad oggi previsto per la Legge 133/2019 (PSNC)[10], a garanzia di coerenza con le disposizioni precedentemente adottate; per i soggetti importanti si propone di prevedere una lista di misure inferiore per numero e complessità.

Infine, tema che merita una menzione specifica è legato alle **categorie di rilevanza** delle attività e dei servizi svolti dai soggetti. Introdotte nello schema all'art. 30, comma 2, e richiamate all'art. 31, comma 2, lett. a), ove sono considerate tra i criteri di proporzionalità per termini, modalità e tempi di implementazione degli obblighi, rappresentano un elemento di novità meritevole nel panorama Europeo, ma che contestualmente determina un ulteriore livello di complessità. In tal senso si propone di valutare un approccio semplificato, tale da non gravare sugli operatori, in particolare su coloro che avendo un livello di maturità più alto, hanno già attuato programmi di innalzamento dei livelli di cybersicurezza. Si suggerisce di valutare ad esempio la possibilità di applicare gli obblighi – incluse specificatamente misure e attività di elencazione – esclusivamente alle categorie più critiche, peraltro coerentemente con l'approccio utilizzato per la Legge 133/2019 (PSNC).

5. Proposta per applicazione principio di Gradualità

Si premette che quanto successivamente indicato presuppone che le categorie di rilevanza per le attività e i servizi svolti dai soggetti, implichino una differenziazione in termini di obblighi – incluse specificatamente misure e attività di elencazione.

Lo schema di d.lgs. menziona, come noto, il principio di adeguatezza per le misure di sicurezza dei sistemi informatici e di rete rispetto ai rischi esistenti. Integrando questo con il principio di gradualità nell'applicazione delle misure, si propone di adottare un approccio per fasi per la loro implementazione.

La proposta concretamente potrebbe essere quella di prevedere:

- Una **prima fase** in cui applicare le misure solamente alle risorse informatiche specifiche o ai servizi critici forniti dal soggetto, ad esempio i sistemi già inclusi in NIS1 e/o PSNC e tutti quelli che caratterizzano il soggetto come essenziale. Le misure si presume siano più numerose ed articolate (ovvero, misure denominate come **avanzate**).
- Una **seconda fase** in cui prevedere l'implementazione di un insieme di misure ridotto – per numero e complessità – rispetto a quello indicato al punto precedente, da applicare a tutti i sistemi appartenenti ad un soggetto essenziale (applicazione dei principi c.d. di Cyber Hygiene a tutta l'organizzazione; misure denominate come di **base**).

[10] Si precisa che questa lista sia l'estremo più alto da applicare ad esempio alle risorse informatiche specifiche o ai servizi critici forniti dal soggetto. Secondo il principio di gradualità si prevede che la lista sia ulteriormente ridotta e semplificata se si applica a servizi non critici.

- Una **terza fase** in cui prevedere l'implementazione di misure di livello intermedio rispetto a quelli definiti nelle due fasi precedenti, da applicarsi a sistemi non critici come quelli della prima fase ma neanche base come quelli della seconda (ovvero, misure denominate come **intermedie**).

Tale approccio può a sua volta esser declinato in modo differenziato tra soggetti essenziali e importanti prevedendo ad esempio fasi opzionali o un numero minore di queste.

Analogo approccio si suggerisce per completare l'elencazione delle attività e servizi svolti dai soggetti secondo quanto previsto dall'art. 30. Questo potrebbe prevedere ad esempio la comunicazione dell'elenco delle attività/servizi altamente critici in fase di prima applicazione, per poi rimandare a fasi successive un'elencazione più di dettaglio. L'obiettivo è quello di raccogliere le informazioni chiave legate ai servizi altamente critici per la nazione, riducendo l'onere tecnico/operativo in capo ai soggetti.

6. Proposta per applicazione principio di Flessibilità

Lo schema di d.lgs. all'art. 24 richiama, come già riportato, il principio di adeguatezza indicando che i soggetti devono adottare misure tecniche, operative e organizzative adeguate e proporzionate per:

- Gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che gli stessi utilizzano per la fornitura dei loro servizi; nonché per
- Prevenire o ridurre al minimo l'impatto di possibili incidenti sui destinatari dei loro servizi e su altri servizi.

Al tempo stesso però si precisa che è importante tenere conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione.

Questo bilanciamento esplicito tra raggiungimento dell'obiettivo e relativa fattibilità è alla base della proposta per l'applicazione di un principio di flessibilità.

La **prima proposta** è quella di dare la facoltà al soggetto di scegliere le **metodologie e approcci che ritiene più idonei per la categorizzazione di rilevanza**, prevista all'art. 30, comma 2, che implica **la differenziazione all'interno dell'organizzazione di attività e servizi, e relativi sistemi** su cui applicare le misure di sicurezza. Concretamente, significa lasciare al soggetto la facoltà di scegliere come effettuare la **categorizzazione di rilevanza** sulla base di criteri di valutazione e scale identificate dallo stesso (e.g. metodologie di Business Impact Analysis proprietarie). Restano valide linee guida e indicazioni che potranno essere eventualmente fornite per un'armonizzazione dei criteri.

La **seconda proposta** è quella di dare la facoltà al soggetto di scegliere le **metodologie e approcci che ritiene più idonei per la definizione, implementazione e verifica di efficacia delle modalità e soluzioni per rispondere alle misure** di sicurezza definite per gestire il livello di rischio. L'approccio è coerente con quanto già previsto dai principali standard e best practice di settore (e. g. ISO 27001), e implica di lasciare che i soggetti possano dimostrare l'esecuzione di processi di analisi del rischio a dimostrazione che le scelte compiute[11] siano adeguate al livello di rischio e criticità delle attività e servizi che il soggetto svolge. La raccomandazione è quella di fornire la lista delle misure – ad esempio le sottocategorie del Framework Nazionale – limitando vincoli in termini di modalità di implementazione della singola misura. Anche in tal caso restano valide linee guida e indicazioni che potranno essere eventualmente fornite per un'armonizzazione dei criteri.

Infine, in merito all'obbligo di garantire la cybersicurezza lungo la **catena di approvvigionamento** previsto dall'art. 24 dello schema di d.lgs., si propone di lasciare ai soggetti la possibilità di definire un approccio per la valutazione delle terze parti che sia **proporzionato al rischio** (risk-based), lasciando a questi la possibilità di valutare il rischio associato a ogni fornitore, ponendo un'attenzione particolare ai fornitori di servizi e tecnologie la cui compromissione potrebbe comportare un impatto significativo sul soggetto e/o sul servizio da esso fornito.

[11] soluzioni tecniche, organizzative e di processo adottare per rispondere alla singola misura previste dall'Art. 24

Quanto suggerito, permette di **valorizzare** le **strategie** e i **programmi** messi in atto dai **soggetti** negli anni passati, volti all'innalzamento dei livelli di resilienza e sicurezza dei servizi offerti, evitando di imporre un onere finanziario/amministrativo aggiuntivo a quanto già previsto. Questo a salvaguardia ulteriore della capacità competitiva del tessuto imprenditoriale italiano rispetto ai player internazionali.

7. Proposta per applicazione principio di Priorità

La Direttiva NIS2 non prevede tempistiche per l'adozione da parte di un soggetto essenziale o importante di obblighi e misure di sicurezza, la cui definizione di queste è demandata agli Stati Membri.

Il principio di priorità si pone l'obiettivo di **focalizzare impegno e risorse in relazione alla criticità del soggetto** e delle sue risorse informatiche o servizi, in linea con un approccio basato sul rischio.

La proposta è pertanto quella di definire tempi di adeguamento per gli obblighi e le misure sulle risorse informatiche o i servizi più critici forniti dal soggetto, e far partire i tempi per l'adeguamento sui sistemi meno critici al termine del piano di adeguamento che ha interessato i primi. Volendo prendere come riferimento le fasi presentate nella proposta per l'applicazione del principio di gradualità, prevedere che queste possano essere sequenziali e non parallele.

Si raccomanda inoltre una adozione di tempistiche di recepimento semplificata, non associando le tempistiche alla singola misura, ma a gruppi di queste per agevolare il programma di recepimento.

Infine, come considerazione generale si segnala l'importanza che le tempistiche di adeguamento per obblighi e misure devono essere avviate solamente a seguito della pubblicazione delle determinazioni che lo schema prevede all'art. 40.

8. Ulteriori proposte e considerazioni

Si segnalano, infine, ulteriori elementi rilevanti, alcuni dei quali potrebbero costituire elemento di riflessione sul più ampio tavolo di collaborazione Europeo:

- **Incentivi alle imprese**: la conformità ai requisiti normativi comporterà importanti sforzi e costi per le imprese. È auspicabile, come già avviene oggi per la Pubblica Amministrazione, l'identificazione di fondi e contributi per le imprese, che favoriscano e incentivino l'adozione di soluzioni e tecnologie di sicurezza, favorendo una crescita del livello di maturità, in primo luogo per quelle imprese che vedranno un importante estensione di ambito a tanti nuovi asset aziendali IT e OT, in secondo luogo per quelle imprese che per la prima volta ricadranno in ambito NIS.
- **Attività ispettive e di supervisione**: le soglie previste dal criterio di individuazione dei soggetti su base dimensionale di cui all'art. 3, comporteranno un numero elevato di soggetti che in Italia ricadrà in ambito NIS, con possibili implicazioni da considerare in riferimento alle attività ispettive e di supervisione. Appare opportuno considerare, come fatto ad esempio da altri Paesi europei (es. Austria e Finlandia) soluzioni più scalabili del processo di ispezione e supervisioni, che permettano di ottemperare alle disposizioni previste dal capo V "monitoraggio, vigilanza ed esecuzione" dello schema di Decreto.
- **Semplificazione degli obblighi di registrazione**: lo schema di decreto legislativo dispone l'obbligo per i soggetti in ambito di provvedere autonomamente alla propria registrazione sull'apposita piattaforma digitale, ai fini della produzione degli elenchi. Ciò comporta per i gruppi che operano all'interno dello stesso Paese un impegno non indifferente nel dover gestire contestualmente molteplici registrazioni per ciascuna Legal Entity operativa sul territorio nazionale. Si riporta, dunque, l'esigenza di definire un approccio che consenta

di ottimizzare e alleggerire tale obbligo, prevedendo, ad esempio, la possibilità per i gruppi di gestire a livello centralizzato la registrazione per tutte le società operative sul territorio nazionale.

- Armonizzazione a livello Europeo delle modalità di adozione delle misure di sicurezza e di notifica degli incidenti di sicurezza (artt. 21 e 23 della Direttiva): i gruppi Internazionali con sedi legali nei diversi stati Europei saranno tenuti a registrarsi nei Paesi in cui operano, e di conseguenza a adottare obblighi e misure di sicurezza richieste dalle leggi di recepimento di tali Paesi, in accordo con l'art. 21 della Direttiva. Questo implica sforzi importanti per mappare lo stato dell'arte e riportare alle autorità locali il livello di sicurezza secondo linee guida/Framework metodologici differenti. Inoltre, l'art. 23 della Direttiva richiede alle organizzazioni che offrono i propri servizi negli Stati Membri dell'UE di notificare gli incidenti Cyber alle autorità nazionali. Ciò comporta, per le organizzazioni che operano in più Paesi, la necessità di dover gestire la notifica degli incidenti verso molteplici autorità nazionali. Si riporta la necessità di definire un approccio armonizzato per gli obblighi di cui agli artt. 21 e 23, a tutela dei Gruppi che operano su più paesi.
- Ruolo delle Certificazioni di settore: è opportuno chiarire quale sarà il ruolo di eventuali certificazioni sulla Sicurezza (es. ISO 27001, …). Appare opportuno considerarne il valore, eventualmente come sostituto dell'evidenza di Compliance, in particolare quando l'ambito di certificazione è costituito da tutti i sistemi aziendali. In definitiva occorre porre l'attenzione sull'ambito di certificazione al fine di garantire che la certificazione possa effettivamente agire come sostituto di Compliance. Ad esempio, la bozza di legge di recepimento pubblicata dalla Polonia prevede che l'attestazione delle certificazioni ISO/IEC 27001 e ISO/IEC 22301 dimostrino anche la Compliance del soggetto ai requisiti dell'articolo 21, sezione 2 della Direttiva ("Misure di gestione dei rischi di cibersicurezza").

Deloitte.