COMMISSIONE
EUROPEA

Bruxelles, 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

ALLEGATO

della

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Sfruttare al meglio le reti e i sistemi informativi – verso l'efficace attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

IT

INDICE

ALLEGATO

1. Introduzione.

Il presente allegato è inteso a contribuire all'efficacia di applicazione, attuazione e controllo del rispetto della direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi nell'Unione (di seguito "direttiva NIS" o "direttiva")[1] e assistere gli Stati membri al fine di garantire l'efficace applicazione del diritto dell'UE. Più in particolare, gli obiettivi specifici sono tre: a) offrire una maggiore chiarezza alle autorità nazionali in merito agli obblighi contenuti nella direttiva ad esse applicabili, b) garantire l'effettivo rispetto degli obblighi della direttiva applicabili ai soggetti sottoposti agli obblighi di sicurezza e di notifica degli incidenti, e c) contribuire nel complesso ad instaurare la certezza giuridica per tutti gli attori pertinenti.

A tal fine il presente allegato fornisce orientamenti riguardanti gli aspetti indicati qui di seguito, che sono fondamentali per il raggiungimento dell'obiettivo della direttiva NIS, ossia garantire un elevato livello comune di sicurezza delle reti e dei sistemi informativi all'interno dell'UE in modo da aiutare il funzionamento della nostra società e della nostra economia:

- l'obbligo per gli Stati membri di adottare una strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi (sezione 2);
- l'istituzione di autorità nazionali competenti, punti di contatto unici e gruppi di intervento per la sicurezza informatica in caso di incidente (sezione 3);
- gli obblighi di sicurezza e di notifica degli incidenti applicabili agli operatori di servizi essenziali e ai fornitori di servizi digitali (sezione 4);
- il rapporto tra la direttiva NIS e altri atti legislativi (sezione 5).

Nell'elaborazione dei presenti orientamenti la Commissione si è avvalsa dei contributi e delle analisi raccolti durante l'elaborazione della direttiva e dei contributi dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) e del gruppo di cooperazione. Ha inoltre usato le esperienze di Stati membri specifici. Ove opportuno la Commissione ha tenuto conto dei principi guida per l'interpretazione del diritto dell'UE, vale a dire la formulazione, il contesto e gli obiettivi della direttiva NIS. Visto che la direttiva non è stata recepita, non vi sono ancora pronunce della Corte di giustizia dell'Unione europea (CGUE) né dei giudici nazionali. Non è pertanto possibile avvalersi della giurisprudenza come orientamento.

La raccolta di queste informazioni in un unico documento potrebbe consentire agli Stati membri di avere una buona panoramica della direttiva e di tenere in considerazione tali informazioni nell'elaborazione della normativa nazionale. La Commissione sottolinea però

[1] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. La direttiva è entrata in vigore l'8 agosto 2016.

che il presente allegato non è vincolante e non intende introdurre disposizioni nuove. La competenza nell'interpretazione del diritto dell'UE spetta in ultima analisi alla CGUE.

2. Strategia nazionale in materia di sicurezza della rete e dei sistemi informativi

A norma dell'articolo 7 della direttiva NIS, gli Stati membri sono tenuti ad adottare una strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi equiparabile alla "strategia nazionale di cibersicurezza (NCSS)". La funzione di una strategia nazionale è definire gli obiettivi strategici e le opportune azioni strategiche e regolamentari in relazione alla cibersicurezza. Il concetto di NCSS è ampiamente utilizzato a livello internazionale e in Europa, in particolare nel contesto delle attività che l'ENISA svolge con gli Stati membri in materia di strategie nazionali, il cui risultato recente è stato l'aggiornamento della guida alle buone pratiche per la NCSS[2].

Nella presente sezione la Commissione specifica in che modo la direttiva NIS aumenta la preparazione degli Stati membri prevedendo l'obbligo di dotarsi di solide strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi (articolo 7). Gli aspetti trattato riguardano a) l'ambito di applicazione della strategia e b) il contenuto e la procedura di adozione.

Come illustrato in maggior dettaglio infra, il corretto recepimento dell'articolo 7 della direttiva NIS è fondamentale ai fini del conseguimento degli obiettivi della direttiva e richiede l'assegnazione di adeguate risorse finanziarie e umane.

2.1. Ambito di applicazione della strategia nazionale

A norma dell'articolo 7, l'obbligo di adottare una NCSS si applica unicamente ai "*settori di cui all'allegato II*" (ossia energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali) e "*ai servizi di cui all'allegato III*" (mercato online, motore di ricerca online e servizio di cloud computing).

L'articolo 3 della direttiva stabilisce specificamente il principio di armonizzazione minima, secondo il quale gli Stati membri possono adottare o mantenere in vigore disposizioni atte a conseguire un livello di sicurezza più elevato della rete e dei sistemi informativi. L'applicazione di tale principio all'obbligo di adottare una NCSS consente agli Stati membri di includere altri settori e servizi oltre a quelli contemplati negli allegati II e III della direttiva.

A giudizio della Commissione e alla luce dell'obiettivo della direttiva NIS - ossia raggiungere un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione[3] - sarebbe consigliabile elaborare una strategia nazionale che comprenda tutte le dimensioni pertinenti della società e dell'economia, e non solo i settori e i servizi digitali contemplati rispettivamente negli allegati II e III della direttiva NIS. Ciò è in linea con le migliori pratiche

[2] ENISA, *National Cyber-Security Strategy Good Practice Guide* (2016). Disponibile all'indirizzo https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
[3] Cfr. articolo 1, paragrafo 1.

internazionali (cfr. orientamenti dell'Unione internazionale delle telecomunicazioni (UIT) e analisi dell'Organizzazione per la cooperazione e lo sviluppo economici (OCSE) cui si fa riferimento infra) e con la direttiva NIS.

Come illustrato in maggior dettaglio infra, questo si verifica in particolare per le amministrazioni pubbliche responsabili di settori e servizi diversi da quelli elencati negli allegati II e III della direttiva. È possibile che le amministrazioni pubbliche elaborino informazioni sensibili, il che giustifica la necessità di ricomprenderle nella NCSS e di redigere piani di gestione che prevengano la fuga delle informazioni e ne garantiscano l'adeguata protezione.

2.2. Contenuto e procedura di adozione delle strategie nazionali

A norma dell'articolo 7 della direttiva NIS, la NCSS deve includere almeno i seguenti elementi:

i) gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi;
ii) un quadro di governance per conseguire gli obiettivi e le priorità della strategia nazionale;
iii) l'individuazione delle misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato;
iv) l'indicazione di programmi di formazione, sensibilizzazione e istruzione pertinenti;
v) un'indicazione di piani di ricerca e sviluppo;
vi) un piano di valutazione dei rischi per individuare i rischi;
vii) un elenco degli attori coinvolti nell'attuazione della strategia.

Né l'articolo 7 né il corrispondente considerando 29 specificano i requisiti per l'adozione della NCSS né scendono in maggiori particolari quanto al suo contenuto. Per quanto riguarda il processo e gli altri elementi del contenuto della NCSS, la Commissione ritiene che l'approccio delineato di seguito costituisca un modo adeguato per adottare una NCSS. L'approccio si basa sull'analisi delle esperienze maturate dagli Stati membri e da paesi terzi sul modo in cui gli Stati membri hanno adottato la rispettiva strategia. Un'altra risorsa informativa è costituita dallo strumento di formazione sulle NCSS dell'ENISA, disponibile sotto forma di video e media scaricabili dal sito web dell'Agenzia[4].

2.3. Processo e aspetti da trattare

Il processo di elaborazione e di successiva adozione della strategia nazionale è complesso e sfaccettato, e per essere efficace ed avere successo richiede un coinvolgimento prolungato di esperti di cibersicurezza, della società civile e del processo politico nazionale. Una condizione imprescindibile è un sostegno amministrativo di alto livello, almeno a livello di sottosegretario di Stato o equivalente, nel ministero guida, così come una sponsorizzazione

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool.

politica. Ai fini di un'adozione riuscita della NCSS, è possibile ipotizzare il processo in cinque fasi illustrato qui di seguito(cfr. figura 1).

Prima fase – **Definizione di principi guida e obiettivi strategici derivanti dalla strategia**

Prima di tutto le autorità nazionali competenti dovrebbero definire alcuni elementi chiave da includere nella NCSS, vale a dire i risultati desiderati - gli "*obiettivi e priorità*" nel linguaggio della direttiva (articolo 7, paragrafo 1, lettera a) -, il modo in cui tali risultati integrano le politiche sociali ed economiche nazionali e la loro compatibilità con i privilegi e gli obblighi derivanti dall'appartenenza all'Unione europea. Gli obiettivi dovrebbero essere specifici, misurabili, attuabili, realistici e temporalmente definiti (SMART). Un esempio illustrativo è il seguente: "Provvederemo affinché la presente strategia [temporalmente definita] si fondi su una serie rigorosa e completa di parametri a fronte dei quali misureremo i progressi verso i risultati che dobbiamo raggiungere"[5].

Rientra in questo processo anche una valutazione politica della possibilità di ottenere un bilancio consistente che permetta di destinare le risorse necessarie all'attuazione della strategia. È inclusa altresì una descrizione dell'ambito di applicazione desiderato della strategia e delle varie categorie di parti interessate dei settori pubblico e privato che dovrebbero essere coinvolte nell'elaborazione dei vari obiettivi e delle varie misure.

Questa prima fase potrebbe essere realizzata attraverso seminari mirati destinati ad alti funzionari ministeriali e politici e moderati da specialisti del settore cibernetico con competenze di comunicazione professionali, in modo da mettere in evidenza le implicazioni che la mancanza di cibersicurezza o una sua debolezza hanno per l'economia e la società digitali moderne.

Seconda fase – **Elaborazione del contenuto della strategia**

La strategia dovrebbe contenere misure di attivazione, azioni temporalmente definite e indicatori chiave di prestazione ai fini delle conseguenti attività di valutazione, rifinitura e miglioramento dopo un determinato periodo di attuazione. Tali misure dovrebbero sostenere l'obiettivo, le priorità e i risultati definiti come principi guida. La necessità di includere misure di attivazione è prevista all'articolo 7, paragrafo 1, lettera c), della direttiva NIS.

Si raccomanda di istituire un gruppo direttivo presieduto dal ministero guida al fine di gestire il processo di redazione e facilitare la presentazione di contributi. Tale risultato potrebbe essere raggiunto attraverso diversi gruppi di redazione, costituiti da funzionari ed esperti, che di dedichino a temi generici fondamentali, ad esempio la valutazione del rischio, la pianificazione per le emergenze, la gestione degli incidenti, lo sviluppo di competenze, la sensibilizzazione, la ricerca e lo sviluppo industriale, ecc. Ogni settore (per esempio l'energia, i trasporti, ecc.) sarebbe separatamente invitato a valutare le implicazioni della sua inclusione, anche in termini di assegnazione delle risorse, e coinvolgerebbe determinati operatori di servizi essenziali e fornitori di servizi digitali chiave nella determinazione delle priorità e

[5] Estratto dalla strategia nazionale di cibersicurezza del Regno Unito, 2016-2021, pagina 67.

nella presentazione di proposte per il processo di redazione. Il coinvolgimento delle parti interessate settoriali è essenziale, tenendo conto anche della necessità di garantire un'attuazione armonizzata della direttiva nei diversi settori consentendo allo stesso tempo la specificità settoriale.

Terza fase – **Elaborazione di un quadro di governance**

Per essere efficiente ed efficace il quadro di governance dovrebbe basarsi sulle parti interessate fondamentali, sulle priorità individuate nel processo di redazione e sui vincoli e sul contesto delle strutture amministrative e politiche nazionali. Sarebbe auspicabile disporre di un canale di comunicazione diretto a livello politico, in cui il quadro sia dotato di capacità decisionali e di assegnazione delle risorse, e dei contributi di esperti di cibersicurezza e di parti interessate del settore. L'articolo 7, paragrafo 1, lettera b), della direttiva NIS fa riferimento al quadro di governance e prevede specificamente "*le responsabilità degli organismi pubblici e degli altri attori pertinenti*".

Quarta fase – **Compilazione ed esame della bozza di strategia**

In questa fase la bozza di strategia dovrebbe essere compilata ed esaminata usando l'analisi dei punti di forza, dei punti di debolezza, delle opportunità e dei rischi (SWOT), in modo da stabilire se sia necessario rivedere il contenuto. In esito all'esame interno dovrebbero essere consultate le parti interessate. Sarebbe essenziale avviare anche una consultazione pubblica al fine di evidenziare l'importanza della strategia proposta presso il pubblico, ricevere contributi da tutte le fonti possibili e cercare sostegno per l'assegnazione delle risorse necessarie ai fini della successiva attuazione della strategia.

Quinta fase – **Adozione formale**

Questa fase finale include l'adozione formale a livello politico con un bilancio congruo che rispecchi la rilevanza attribuita alla cibersicurezza dallo Stato membro interessato. Al fine di raggiungere gli obiettivi della direttiva NIS, la Commissione incoraggia gli Stati membri a fornirle informazioni riguardanti il bilancio nella comunicazione del documento sulla strategia nazionale conformemente all'articolo 7, paragrafo 3. Gli impegni in termini di bilancio e di risorse umane necessarie sono assolutamente essenziali per l'attuazione efficace della strategia e della direttiva. Visto che la cibersicurezza è ancora un settore dell'ordine pubblico abbastanza nuovo e in rapida espansione, nella maggior parte dei casi sono necessari nuovi investimenti anche se la situazione complessiva delle finanze pubbliche richiede tagli e risparmi.

Varie fonti pubbliche e accademiche offrono consulenza in merito al processo e al contenuto delle strategie nazionali, ad esempio l'ENISA[6], l'UIT[7], l'OCSE[8], il Global Forum on Cyber Expertise e l'Università di Oxford[9].

2.4. Iniziative concrete chieste agli Stati membri prima del termine di recepimento.

Prima dell'adozione della direttiva quasi tutti gli Stati membri[10] avevano già pubblicato documenti definiti come NCSS. La sezione 6 del presente allegato elenca le strategie attualmente in essere in ogni Stato membro[11], che solitamente includono principi strategici, orientamenti, obiettivi e in alcuni casi misure specifiche volte a mitigare i rischi associati alla cibersicurezza.

Visto che alcune di queste strategie risalgono a prima dell'adozione della direttiva NIS, potrebbero non contenere tutti gli elementi di cui all'articolo 7. Al fine di garantire il corretto recepimento, gli Stati membri dovranno intraprendere un'analisi delle lacune mappando il contenuto della rispettiva NCSS rispetto ai sette requisiti distinti elencati all'articolo 7 in tutto lo spettro di settori elencati nell'allegato II e di servizi elencati nell'allegato III della direttiva. Le lacune individuate possono quindi essere colmate attraverso una revisione delle NCSS esistenti o decidendo di ripartire da zero con una revisione completa dei principi della strategia NIS nazionale. Gli orientamenti indicati per il processo di adozione della NCSS sono pertinenti anche per la revisione e l'aggiornamento delle NCSS esistenti.

---

[6] ENISA, *National Cyber-Security Strategy Good Practice Guide* (2016). Disponibile all'indirizzo https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[7] UIT, *National Cybersecurity Strategy Guide* (2011). Disponibile all'indirizzo http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.
L'UIT pubblicherà anche uno strumentario per le strategie nazionali di cibersicurezza (National Cyber Security Strategy Toolkit) nel 2017 (cfr. presentazione all'indirizzo http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

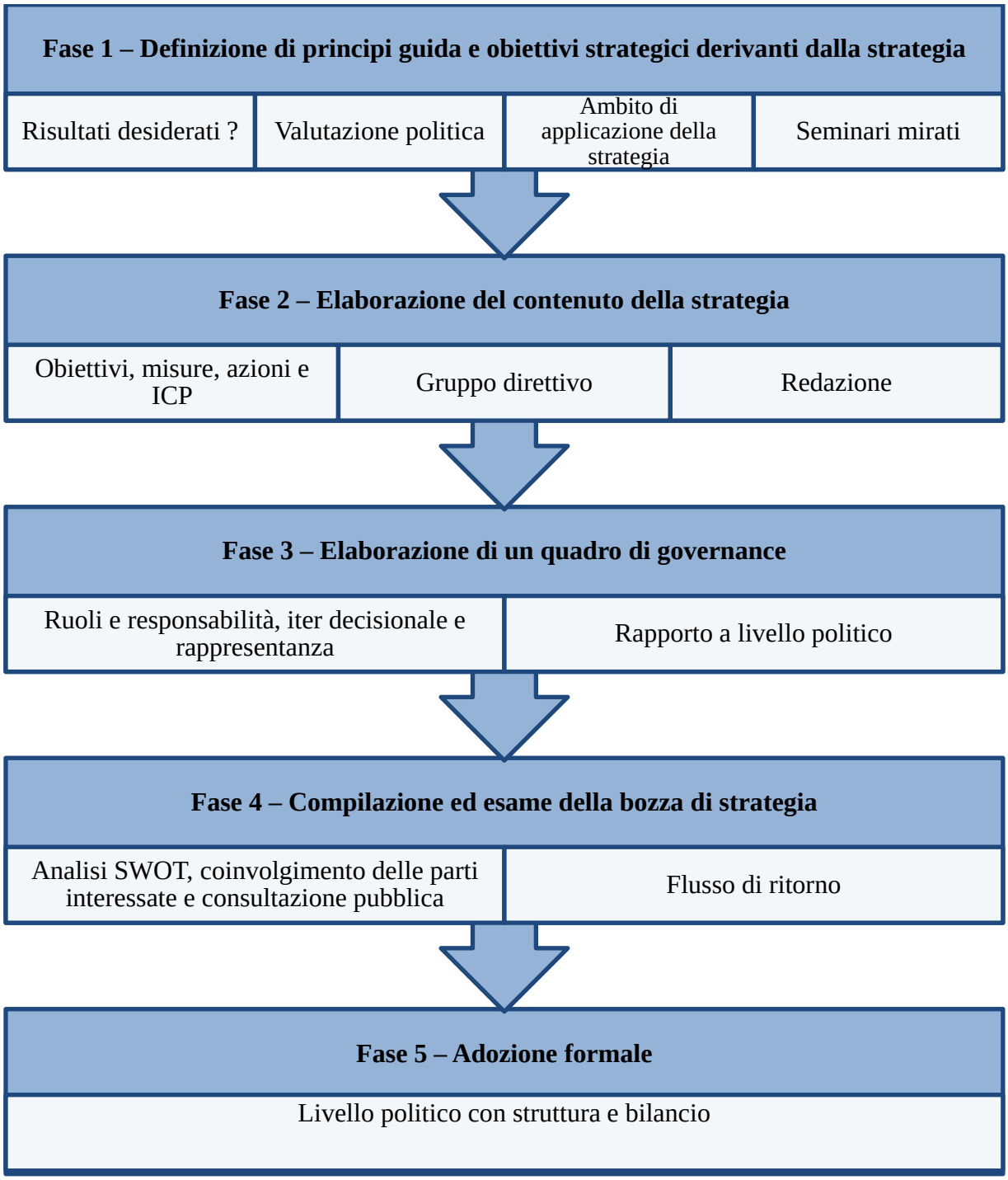
[8] OCSE, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (2012). Disponibile all'indirizzo: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[9] Global Cyber Security Capacity Centre e Università di Oxford, *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* (2016). Disponibile all'indirizzo: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf.

[10] Esclusa la Grecia, dove una strategia nazionale di cibersicurezza è in fase di elaborazione dal 2014 (cfr. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Informazione basata sulla panoramica delle NCSS fornita dall'ENISA all'indirizzo https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

Figura 1 - Iter in 5 fasi per l'adozione della NCSS



3. Direttiva NIS - Autorità nazionali competenti, punti di contatto unici e gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)

A norma dell'articolo 8, paragrafo 1, della direttiva, gli Stati membri sono tenuti a designare una o più autorità nazionali competenti, che si occupino almeno dei settori di cui all'allegato II e dei servizi di cui all'allegato III, con il compito di controllare l'applicazione della direttiva. Gli Stati membri possono affidare questo ruolo a una o più autorità esistenti.

La presente sezione verte sul modo in cui la direttiva NIS aumenta la preparazione degli Stati membri prevedendo l'obbligo di dotarsi di autorità nazionali competenti e gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) efficaci. Più precisamente, tratta dell'obbligo di designare le autorità nazionali competenti, compreso il ruolo del punto di contatto unico. Affronta tre argomenti: a) possibili strutture nazionali di governance (ad esempio modelli centralizzati, decentrati, ecc.) e altri requisiti; b) ruolo del punto di contatto unico e c) gruppi di intervento per la sicurezza informatica in caso di incidente.

3.1. Tipo di autorità

L'articolo 8 della direttiva NIS prevede che gli Stati membri designino autorità nazionali competenti in materia di sicurezza delle reti e dei sistemi informativi, riconoscendo esplicitamente la possibilità di designare "*una o più autorità nazionali competenti*". Il considerando 30 della direttiva spiega tale scelta strategica: "*In considerazione delle differenze esistenti tra le strutture di governance nazionali e al fine di salvaguardare gli accordi settoriali già esistenti o gli organismi di vigilanza e di regolamentazione dell'Unione ed evitare duplicazioni, è opportuno che gli Stati membri abbiano la facoltà di designare più di un'autorità nazionale competente responsabile di soddisfare i compiti connessi alla sicurezza delle reti e dei sistemi informativi degli operatori di servizi essenziali e dei fornitori di servizi digitali di cui alla presente direttiva*".

Di conseguenza, gli Stati membri sono liberi di nominare un'unica autorità centrale che si occupi di tutti i settori e i servizi contemplati dalla direttiva oppure diverse autorità, ad esempio in base al tipo di settore.

Nel decidere l'approccio gli Stati membri possono attingere all'esperienza derivante dagli approcci nazionali usati nel contesto della normativa vigente in materia di protezione delle infrastrutture critiche (CIIP). Come descritto nella tabella 1, nel caso della CIIP gli Stati membri hanno optato per un approccio centralizzato o per uno decentrato al momento dell'assegnazione delle competenze a livello nazionale. Gli esempi nazionali citati nella presente sezione hanno esclusivamente scopi illustrativi e intendono portare i quadri organizzativi esistenti all'attenzione degli Stati membri. Pertanto la Commissione non suggerisce che il modello usato dai rispettivi paesi per la CIIP debba essere necessariamente utilizzato nel recepimento della direttiva NIS.

Gli Stati membri potrebbero anche optare per meccanismi ibridi che includano elementi di entrambi gli approcci (centralizzato e decentrato). Si può scegliere di allinearsi ai processi nazionali di governance preesistenti nei vari settori e servizi contemplati dalla direttiva o di far delineare processi nuovi da parte alle autorità interessate e alle parti interessate identificate come operatori di servizi essenziali e fornitori di servizi digitali. Anche l'esistenza di competenze specifiche in materia di cibersicurezza, le considerazioni in termini di assegnazione delle risorse, i rapporti tra le parti interessate e gli interessi nazionali (per esempio lo sviluppo economico, la sicurezza pubblica, ecc.) potrebbero essere fattori importanti che contribuiscono alle scelte fatte dagli Stati membri.

3.2 Pubblicità e altri aspetti pertinenti

A norma dell'articolo 8, paragrafo 7, gli Stati membri devono comunicare alla Commissione la designazione delle autorità competenti e i compiti loro attribuiti. Tale comunicazione deve avvenire entro il termine di recepimento.

Gli articoli 15 e 17 della direttiva NIS chiedono agli Stati membri di provvedere a che le autorità competenti siano dotate dei poteri specifici e dei mezzi necessari per svolgere i compiti ivi descritti.

La designazione di soggetti specifici quali autorità nazionali competenti deve essere resa pubblica, ma la direttiva non specifica in che modo. Visto che l'obiettivo di quest'obbligo è informare doviziosamente gli attori contemplati dalla direttiva NIS e il pubblico in generale, e in base alle esperienze maturate in altri settori (telecomunicazioni, banche, medicinali), la Commissione ritiene che l'obbligo di pubblicazione possa essere soddisfatto, ad esempio, attraverso un portale ben pubblicizzato.

L'articolo 8, paragrafo 5, della direttiva NIS prevede che dette autorità siano dotate di "risorse adeguate" per svolgere i compiti assegnati loro dalla direttiva.

Tabella 1 - Approcci nazionali alla protezione delle infrastrutture critiche informatizzate (CIIP)

Nel 2016 l'ENISA ha pubblicato uno studio[12] riguardante i diversi approcci seguiti dagli Stati membri per proteggere le infrastrutture critiche informatizzate. Sono descritti due profili di governance della CIIP negli Stati membri che possono essere traslati nel recepimento della direttiva NIS.

Profilo 1 - Approccio decentrato – con molteplici autorità settoriali competenti dei settori e servizi specifici di cui agli allegati II e III della direttiva

L'approccio decentrato è caratterizzato da:

(i) principio di sussidiarietà
(ii) forte cooperazione tra le agenzie pubbliche
(iii)normativa settoriale.

Principio di sussidiarietà

Invece di istituire o designare un'unica agenzia avente la responsabilità globale, l'approccio decentrato segue il principio di sussidiarietà. Ciò significa che la responsabilità dell'attuazione è nelle mani di un'autorità settoriale, che comprende al meglio il settore locale e ha già un rapporto consolidato con le parti interessate. Secondo questo principio le decisioni sono prese da chi è più vicino ai soggetti che ne subiscono gli effetti.

Forte cooperazione tra le agenzie pubbliche

Alla luce della varietà di agenzie pubbliche coinvolte nella CIIP, molti Stati membri hanno elaborato programmi di cooperazione volti a coordinare il lavoro e le iniziative delle diverse autorità. Tali programmi di cooperazione possono assumere la forma di reti informali oppure di forum o intese più istituzionalizzati. La loro finalità è tuttavia unicamente lo scambio di informazioni e il coordinamento tra le diverse agenzie pubbliche, senza che si possa esercitare alcuna autorità sulle stesse.

Normativa settoriale

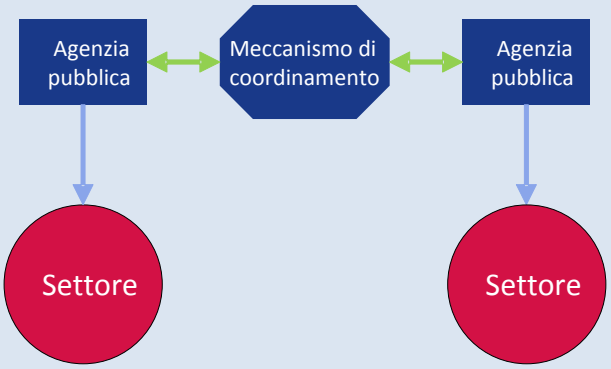
Spesso i paesi che seguono l'approccio decentrato nei vari settori critici evitano di legiferare ai fini della CIIP. L'adozione di leggi e regolamenti rimane invece settoriale e pertanto può variare enormemente tra i diversi settori. Quest'approccio avrebbe il vantaggio di allineare le misure legate al NIS con le regolamentazioni settoriali esistenti, così da migliorare sia l'accettazione da parte del settore che l'efficacia del controllo da parte dell'autorità competente.

In caso di approccio decentrato puro esiste un rischio rilevante di ridurre la coerenza nell'applicazione della direttiva fra i vari settori e servizi. Per parare a questo rischio la direttiva prevede un punto di contatto nazionale unico che funge da collegamento per le

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (2016). Disponibile all'indirizzo: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis.

questioni transfrontaliere; lo Stato membro interessato potrebbe anche incaricare tale soggetto del coordinamento e della cooperazione interni tra le diverse autorità nazionali competenti, in conformità all'articolo 10 della direttiva.

Figura 2 – Approccio decentrato



Esempi di approccio decentrato

La Svezia è un buon esempio di paese che segue un approccio decentrato nella CIIP. Il paese adotta una "prospettiva di sistema", il che significa che i principali compiti della CIIP, come l'identificazione di servizi essenziali e infrastrutture critiche, il coordinamento e il sostegno agli operatori, i compiti normativi e le misure per la preparazione in caso di emergenza, sono responsabilità di agenzie e comuni diversi. Tra queste agenzie rientrano l'Agenzia svedese per le emergenze civili (MSB), l'Agenzia svedese delle poste e telecomunicazioni (PTS) e diverse agenzie svedesi per la difesa, militari e di contrasto.

Al fine di coordinare le azioni tra le diverse agenzie ed enti pubblici, il governo svedese ha sviluppato una rete di cooperazione composta da autorità "con specifiche responsabilità sociali di sicurezza informativa". Il gruppo di cooperazione per la sicurezza informativa (SAMFI) è composto da rappresentanti delle diverse autorità e si riunisce diverse volte l'anno per discutere questioni legate alla sicurezza informativa nazionale. I settori di competenza del SAMFI sono principalmente riscontrabili in settori politico-strategici e riguardano argomenti come questioni tecniche e normalizzazione, sviluppi nazionali e internazionali nel campo della sicurezza informativa o gestione e prevenzione degli incidenti informatici (Agenzia svedese per le emergenze civili (MSB) 2015).

La Svezia non ha emanato a livello centrale una legge per la CIIP applicabile trasversalmente agli operatori di infrastrutture critiche informatizzate (CII) nei vari settori. Al contrario, la promulgazione di norme che prevedono gli obblighi cui sono sottoposte le imprese nei diversi settori è responsabilità delle rispettive autorità pubbliche Ad esempio, l'MSB ha il diritto di promulgare regolamenti per le autorità pubbliche nel settore della sicurezza informativa, mentre la PTS può imporre agli operatori di attuare determinate misure di sicurezza tecnica o

organizzativa sulla base del diritto derivato.

Un altro esempio di paese con caratteristiche tipiche di questo profilo è l'Irlanda. L'Irlanda segue una "dottrina della sussidiarietà" in cui ogni ministero è responsabile dell'identificazione della CII e della valutazione del rischio nel proprio settore. Non è stata emanata alcuna regolamentazione specifica per la CIIP a livello nazionale. La normativa rimane settoriale ed esiste principalmente per il settore dell'energia e delle telecomunicazioni (2015). Altri esempi sono l'Austria, Cipro e la Finlandia.

Profilo 2 - Approccio centralizzato – con una sola autorità centrale competente di tutti i settori e i servizi di cui agli allegati II e III della direttiva

L'approccio centralizzato è caratterizzato da:

i) un'autorità centrale per i diversi settori
ii) una normativa di portata generale.

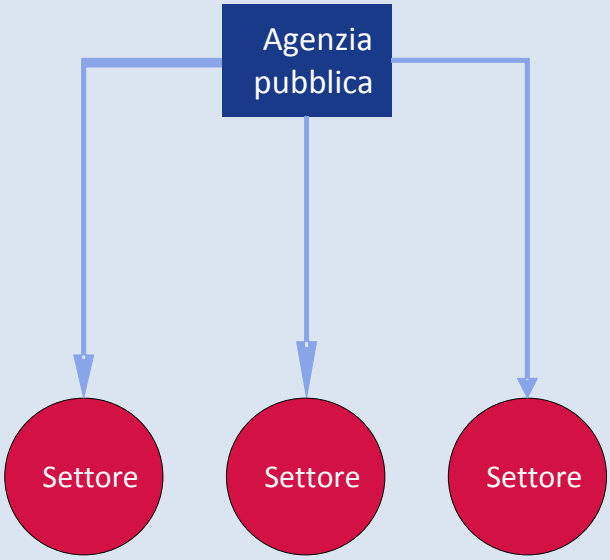
Autorità centrale per i diversi settori

Gli Stati membri che seguono un approccio centralizzato hanno creato autorità investite di responsabilità ed ampie competenze in diversi o in tutti i settori critici ovvero hanno esteso i poteri di autorità esistenti. Tali autorità principali per la CIIP combinano diversi compiti, come la pianificazione di emergenza, la gestione delle emergenze, i compiti di regolamentazione e il sostegno agli operatori privati. In molti casi il CSIRT nazionale o pubblico fa parte dell'autorità CIIP principale. Vista la carenza generale di competenze cibersicurezza, un'autorità centrale può probabilmente contare su una maggiore concentrazione di tali competenze rispetto a una pluralità di autorità settoriali

Normativa di portata generale.

Una normativa di portata generale crea obblighi e requisiti per tutti gli operatori di CII in tutti i settori tramite l'adozione di nuove leggi generali o tramite l'integrazione delle regolamentazioni settoriali vigenti. Questo approccio faciliterebbe un'applicazione coerente della direttiva NIS in tutti i settori e per i servizi contemplati. Eviterebbe il rischio di quelle lacune di attuazione che potrebbero verificarsi in caso di molteplici autorità con competenze specifiche.

Figura 3 – Approccio centralizzato



Esempi di approccio centralizzato

La Francia è un buon esempio di Stato membro dell'UE che segue un approccio centralizzato. Nel 2011 l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) francese è stata proclamata principale autorità nazionale per la difesa dei sistemi informativi. L'ANSSI ha un forte ruolo di vigilanza per gli "operatori di vitale importanza" (OIV); può imporre agli OIV di attenersi alle misure di sicurezza ed è autorizzata a sottoporli a controlli di sicurezza. Costituisce inoltre il principale punto di contatto unico per gli OIV, che sono tenuti a segnalarle gli incidenti di sicurezza.

In caso di incidente di sicurezza l'ANSSI agisce come agenzia di gestione delle emergenze per la CIIP e decide le misure che gli operatori sono tenuti ad adottare per rispondere alla crisi. Le azioni del governo sono coordinate all'interno del centro operativo dell'ANSSI. La rilevazione delle minacce e la risposta agli incidenti a livello operativo sono svolte da CERT-FR, che fa parte dell'ANSSI.

La Francia ha istituito un quadro giuridico generale per la CIIP. Nel 2006 il primo ministro ha ordinato l'elaborazione di un elenco di settori di infrastrutture critiche; sulla base dei dodici settori vitali così stabiliti, il governo ha individuato circa 250 OIV. Nel 2013 è stata promulgata la legge di programmazione militare (LPM)[13] che impone obblighi diversi agli OIV, come la segnalazione degli incidenti o l'attuazione di misure di sicurezza, che vincolano tutti gli OIV in tutti i settori (Senato francese 2013).

[13] Loi de programmation militaire.

3.3. Direttiva NIS, articolo 9 - Gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)

A norma dell'articolo 9 della direttiva NIS, ciascuno Stato membro è tenuto a designare uno o più CSIRT cui è attribuito il compito di trattare gli incidenti e i rischi per i settori elencati nell'allegato II e i servizi elencati nell'allegato III. Tenuto conto dell'obbligo di armonizzazione minima imposto dall'articolo 3 della direttiva, gli Stati membri hanno la facoltà di valersi dei CSIRT anche per settori non contemplati dalla direttiva, ad es. la pubblica amministrazione.

Gli Stati membri possono optare per la costituzione di un CSIRT all'interno dell'autorità nazionale competente[14].

3.4. Compiti e requisiti

I compiti dei CSIRT designati, elencati nell'allegato I della direttiva NIS, includono quanto segue:

- monitoraggio degli incidenti a livello nazionale;
- emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
- intervento in caso di incidente;
- analisi dinamica dei rischi e degli incidenti, nonché sensibilizzazione situazionale;
- partecipazione alla rete dei CSIRT nazionali (rete dei CSIRT) istituita a norma dell'articolo 12.

L'articolo 14, paragrafi 3, 5 e 6, e l'articolo 16, paragrafi 3, 6 e 7, prevedono taluni compiti supplementari collegati alle notifiche degli incidenti nei casi in cui lo Stato membro decide che i CSIRT possono intervenire in aggiunta o in vece delle autorità nazionali competenti.

In sede di recepimento della direttiva si aprono agli Stati membri diverse alternative riguardo al ruolo dei CSIRT in collegamento con gli obblighi di notifica degli incidenti: possono optare per la segnalazione diretta obbligatoria ai CSIRT, che presenta vantaggi di efficienza amministrativa, oppure per la segnalazione diretta alle autorità nazionali competenti con diritto dei CSIRT di accedere alle informazioni segnalate. In ultima analisi i CSIRT s'interessano della risoluzione dei problemi nei vari aspetti (dissuasione, rilevamento, risposta e attenuazione dell'impatto) collegati ai ciberincidenti, compresi quelli non critici ai fini della segnalazione obbligatoria, che si verificano con i rispettivi portatori d'interessi, mentre il rispetto della normativa è piuttosto materia trattata dalle autorità nazionali competenti.

[14] Cfr. articolo 9, paragrafo 1, ultima frase.

A norma dell'articolo 9, paragrafo 3, della direttiva, gli Stati membri devono garantire che i CSIRT abbiano accesso a un'infrastruttura di informazione e comunicazione sicura e resiliente.

A norma dell'articolo 9, paragrafo 4, della direttiva, gli Stati membri sono tenuti a comunicare alla Commissione il mandato dei CSIRT designati e gli elementi principali della procedura di trattamento degli incidenti loro affidata.

I requisiti applicabili ai CSIRT designati dagli Stati membri sono precisati nell'allegato I della direttiva NIS. Il CSIRT deve garantire un alto livello di disponibilità dei propri servizi di comunicazione. I suoi locali e sistemi informativi di supporto sono ubicati in siti sicuri e sono in grado di garantire la continuità operativa. I CSIRT dovrebbero inoltre poter partecipare a reti di cooperazione internazionale.

3.5. Assistenza per lo sviluppo dei CSIRT

Tramite il programma delle infrastrutture di servizi digitali (DSI) per la cibersicurezza del Meccanismo per collegare l'Europa (MCE) i CSIRT degli Stati membri possono ricevere dall'UE un consistente contributo finanziario da destinare al miglioramento delle proprie capacità e a una cooperazione reciproca che si concreta attraverso un meccanismo per lo scambio di informazioni. Il meccanismo di cooperazione in corso di sviluppo nell'ambito del progetto SMART 2015/1089 è inteso ad agevolare una cooperazione operativa rapida ed efficace cui partecipino, su base volontaria, i CSIRT degli Stati membri, in particolare a sostegno della rete dei CSIRT nei compiti affidatile ai sensi dell'articolo 12 della direttiva.

Per gli inviti a presentare proposte finalizzate allo sviluppo delle capacità dei CSIRT degli Stati membri si rimanda al sito internet dell'Agenzia esecutiva per l'innovazione e le reti (INEA) della Commissione europea[15].

I CSIRT degli Stati membri possono contare sul comitato direttivo del DSI per la cibersicurezza dell'MCE sia come struttura informale d'indirizzo e assistenza a livello di politiche ai fini dello sviluppo delle capacità, sia per l'attuazione del meccanismo di cooperazione volontaria.

Se neocostituito o incaricato dei compiti previsti nell'allegato I della direttiva, il CSIRT può contare sulla consulenza e sulle competenze dell'ENISA per migliorare le proprie prestazioni e per ottenere i risultati voluti nelle proprie attività[16]. Si rilevi al riguardo che i CSIRT degli Stati membri potrebbero prendere a riferimento taluni aspetti dei lavori recenti dell'ENISA, in particolare - come indicato nella sezione 7 del presente allegato - i documenti e studi pubblicati in cui sono illustrate le buone pratiche e formulate raccomandazioni tecniche, comprensive di valutazioni sul grado di maturità dei CSIRT, riguardo a vari servizi e capacità

[15] Cfr. https://ec.europa.eu/inea/en/connecting-europe-facility.
[16] Cfr. articolo 9, paragrafo 5, della direttiva NIS.

di questi. Sono inoltre stati condivisi orientamenti e migliori pratiche attraversoi le reti dei CSIRT a livello sia mondiale (FIRST[17]) sia europeo (Trusted Introducer, TI[18]).

3.6. Ruolo del punto di contatto unico

A norma dell'articolo 8, paragrafo 3, della direttiva NIS, ciascuno Stato membro deve designare un punto di contatto unico nazionale, il quale svolge una funzione di collegamento per garantire la cooperazione transfrontaliera con le autorità competenti negli altri Stati membri e con il gruppo di cooperazione e la rete dei CSIRT[19] creati dalla direttiva stessa. Il considerando 31 e l'articolo 8, paragrafo 4, indicano il motivo per cui è imposto tale obbligo, vale a dire l'agevolazione della cooperazione e della comunicazione transfrontaliere. Si tratta di una necessità particolarmente acuta dato che gli Stati membri possono decidere di avere più di una autorità nazionale: un punto di contatto unico faciliterebbe quindi l'individuazione e la collaborazione tra le autorità di diversi Stati membri.

La funzione di collegamento del punto di contatto unico può comportare un'interazione con la segreteria del gruppo di cooperazione e con quella della rete dei CSIRT nei casi in cui il punto di contatto unico nazionale non è né un CSIRT né un membro del gruppo di cooperazione. Gli Stati membri devono garantire inoltre che il punto di contatto unico sia informato delle notifiche ricevute dagli operatori di servizi essenziali e dai fornitori di servizi digitali[20].

L'articolo 8, paragrafo 3, della direttiva precisa che, se lo Stato membro opta per la centralizzazione designando soltanto una autorità competente, questa svolge anche la funzione di punto di contatto unico. Lo Stato membro che opta invece per la decentralizzazione è libero di scegliere per la funzione di punto di contatto unico una delle varie autorità competenti . A prescindere dal modello istituzionale prescelto, se l'autorità competente, il CSIRT e il punto di contatto unico sono soggetti diversi, gli Stati membri hanno l'obbligo di garantire che essi collaborino in modo efficace ai fini dell'adempimento degli obblighi previsti dalla direttiva[21].

Entro il 9 agosto 2018 e in seguito ogni anno, una volta all'anno il punto di contatto unico è tenuto a trasmettere una relazione sintetica al gruppo di cooperazione in merito alle notifiche ricevute, compresi il numero di notifiche, la natura degli incidenti e le azioni intraprese dalle autorità, ad esempio l'informazione degli altri Stati membri coinvolti o la comunicazione all'impresa notificante di informazioni d'interesse ai fini del trattamento dell'incidente[22]. Su richiesta dell'autorità competente o del CSIRT, il punto di contatto unico trasmette le notifiche degli operatori di servizi essenziali ai punti di contatto unici degli altri Stati membri interessati dall'incidente[23].

Gli Stati membri devono informare la Commissione del punto di contatto unico designato e dei relativi compiti entro il termine fissato per il recepimento. La designazione del punto di

[17] Forum dei gruppi di sicurezza e d'intervento in caso di incidente (https://www.first.org/).
[18] https://www.trusted-introducer.org/
[19] Rete di CSIRT nazionali per la cooperazione operativa tra gli Stati membri a norma dell'articolo 12.
[20] Cfr. articolo 10, paragrafo 3.
[21] Cfr. articolo 10, paragrafo 1.
[22] Ibidem.
[23] Cfr. articolo 14, paragrafo 5.

contatto unico deve essere resa pubblica analogamente a quanto avviene per le autorità nazionali competenti. La Commissione pubblica l'elenco dei punti di contatto unici designati.

3.7. Sanzioni

L'articolo 21 lascia agli Stati membri un margine di discrezionalità nella decisione sul tipo e sulla natura delle sanzioni applicabili, a condizione che siano effettive, proporzionate e dissuasive. Detto in altri termini, gli Stati membri sono, in via di principio, liberi di stabilire l'importo massimo delle sanzioni previste nella normativa nazionale, ma l'importo o la percentuale fissati dovrebbero consentire alle autorità nazionali, in ciascun caso concreto, d'infliggere una sanzione effettiva, proporzionata e dissuasiva in considerazione di diversi fattori, quali la gravità o la frequenza della violazione.

4. Soggetti vincolati a obblighi in termini di requisiti di sicurezza e di notifiche di incidenti

I soggetti che svolgono un ruolo importante per la società e per l'economia, ai quali nell'articolo 4, punti 4 e 5, la direttiva si riferisce come operatori di servizi essenziali e fornitori di servizi digitali, sono tenuti ad adottare le misure di sicurezza adeguate e a notificare gli incidenti gravi alle autorità nazionali competenti. La disposizione si fonda sul principio che un incidente di sicurezza può produrre in questi servizi un effetto tale da rappresentare una grave minaccia per il loro funzionamento, con conseguenti pesanti perturbazioni delle attività economiche e della società in generale, potenzialmente in grado di minare la fiducia degli utenti e causare gravi danni all'economia dell'Unione[24].

Nella presente sezione si passano in rassegna i soggetti cui si applicano gli allegati II e III della direttiva NIS e se ne elencano gli obblighi. Grande spazio è dedicato all'identificazione degli operatori di servizi essenziali, data l'importanza che riveste ai fini di un'attuazione armonizzata della direttiva NIS in tutta l'UE. Sono inoltre spiegate diffusamente le definizioni di infrastrutture digitali e di fornitori di servizi digitali; è vagliata l'ipotesi di estendere l'applicabilità ad altri settori ed è illustrata in maggior dettaglio l'impostazione specifica seguita per i fornitori di servizi digitali.

4.1. Operatori di servizi essenziali

La direttiva NIS non indica esplicitamente quali soggetti specifici saranno considerati operatori di servizi essenziali nel suo ambito di applicazione. Stabilisce invece i criteri che gli Stati membri dovranno applicare per svolgere un processo di identificazione il cui esito porti a determinare quali imprese, dei tipi di soggetti previsti nell'allegato II, saranno considerate operatori di servizi essenziali e quindi sottoposte agli obblighi disposti dalla direttiva.

[24] Cfr. considerando 2.

4.1.1. Tipi di soggetti elencati nell'allegato II della direttiva NIS

L'articolo 4, punto 4, della direttiva definisce l'operatore di servizi essenziali come il soggetto pubblico o privato di un tipo di cui all'allegato II che soddisfa i criteri di cui all'articolo 5, paragrafo 2. Nell'allegato II sono elencati i settori, i sottosettori e i tipi di soggetti per i quali ciascuno Stato membro deve compiere il processo di identificazione ai sensi dell'articolo 5, paragrafo 2[25]. Tra i settori si annoverano energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua e infrastrutture digitali.

Per la maggior parte dei soggetti dei "settori tradizionali" la normativa dell'UE prevede definizioni articolate, cui peraltro rimanda l'allegato II, ma così non è per il settore delle infrastrutture digitali (punto 7 dell'allegato II), che comprende i punti di interscambio internet (IXP), i sistemi dei nomi di dominio (DNS) e i registri dei nomi di dominio di primo livello. Segue una spiegazione particolareggiata di queste ultime espressioni per chiarirne le definizioni.

1) Punto di interscambio internet (IXP)

Il punto di interscambio internet è definito all'articolo 4, punto 13, e precisato nel considerando 18; lo si può descrivere come un'infrastruttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti dal punto di vista tecnico, principalmente al fine di agevolare lo scambio del traffico internet. Può anche essere descritto come un luogo fisico in cui una serie di reti possono scambiarsi traffico internet attraverso un centro stella. Lo scopo principale di un IXP è permettere alle reti di interconnettersi direttamente, attraverso il punto di interscambio, piuttosto che mediante le reti di uno o più terzi. Di regola l'instradamento del traffico internet non compete al fornitore di IXP: se ne occupano i fornitori dei servizi di rete. I vantaggi dell'interconnessione diretta sono numerosi, ma i principali si ottengono in termini di costi, di tempi di latenza e di larghezza di banda. Solitamente nessuna parte fattura il traffico che transita da un punto di interscambio, mentre viene fatturato il traffico verso un fornitore di servizi internet upstream. Ubicata spesso nella stessa città delle due reti interessate, l'interconnessione diretta riduce i tempi di latenza perché evita ai dati di dover percorrere lunghe distanze per passare da una rete all'altra.

La definizione di IXP non comprende i punti fisici in cui si interconnettono soltanto due reti fisiche (ossia i fornitori di rete quali BASE e Proximus). In sede di recepimento della direttiva gli Stati membri devono operare pertanto una distinzione fra gli operatori che agevolano l'interscambio di traffico internet aggregato tra più operatori di rete e gli operatori di rete unica, i quali interconnettono fisicamente le rispettive reti in base a un accordo di interconnessione. In questo secondo caso i fornitori di servizi di rete non rientrano nella definizione dell'articolo 4, punto 13. Il concetto è precisato nel considerando 18, in cui si afferma che l'IXP non fornisce accesso alla rete né funziona da fornitore o carrier di transito. L'ultima categoria di fornitori sono le imprese che forniscono reti e/o servizi pubblici di

[25] Per maggiori particolari sul processo d'identificazione, cfr. punto 4.1.6.

comunicazione, le quali, essendo sottoposte agli obblighi di sicurezza e di notifica previsti agli articoli 13 bis e 13 ter della direttiva 2002/21/CE, esulano dall'ambito di applicazione della direttiva NIS[26].

2) Sistema dei nomi di dominio (DNS)

L'articolo 4, punto 14, definisce il "sistema dei nomi di dominio" come "*un sistema distribuito e gerarchico di naming in una rete che inoltra le richieste dei nomi di dominio*". Più precisamente, il DNS può essere descritto come un sistema distribuito e gerarchico di naming per computer, servizi o qualsiasi altra risorsa collegata a internet che consente la codifica dei nomi di dominio in indirizzi IP (Internet Protocol). La funzione principale del sistema è convertire in indirizzi IP i nomi di dominio assegnati. Ai fini di questa "conversione" in indirizzi IP operativi il DNS necessita di un database, di server di naming e di un meccanismo di risoluzione. Pur non essendo l'unica funzione del DNS, la codifica dei nomi di dominio ne rappresenta il compito fondamentale. La definizione giuridica prevista all'articolo 4, punto 14, si concentra sulla funzione principale del sistema dal punto di vista dell'utente senza inoltrarsi in dettagli più tecnici, quali ad esempio la gestione dello spazio dei nomi di dominio, i server di naming, il meccanismo di risoluzione, ecc. L'articolo 4, punto 15, indica infine chi va considerato fornitore di servizi DNS.

3) Registro dei nomi di dominio di primo livello (registro dei nomi TLD)

Il registro dei nomi di dominio di primo livello è definito all'articolo 4, punto 16, come il soggetto che si occupa dell'amministrazione e della registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello. Tali funzioni di amministrazione e di registrazione dei nomi di dominio comprendono la codifica dei nomi TLD in indirizzi IP.

La IANA (Autorità per l'assegnazione dei numeri per internet) è responsabile del coordinamento globale per quanto riguarda la radice DNS, l'indirizzamento verso l'IP e altre risorse IP. Competono alla IANA, in particolare, l'assegnazione dei domini di primo livello generici (gTLD - ad esempio ".com") e dei domini di primo livello geografici (ccTLD - ad es. ".it") agli operatori (registri), così come il mantenimento dei relativi dati tecnici e amministrativi. La IANA tiene un registro mondiale dei TLD assegnati e interviene per divulgare l'elenco agli utenti internet di tutto il mondo e per inserirvi TLD nuovi.

I registri hanno l'importante funzione di assegnare, nell'ambito del rispettivo TLD, i nomi di secondo livello ai cosiddetti registranti, i quali possono, se lo desiderano, assegnare autonomamente i nomi di dominio di terzo livello. I ccTLD rappresentano un paese o un territorio con una targa conforme alla norma ISO 3166-1. I TLD "generici" sono di solito privi di qualsiasi indicazione geografica o legata a un paese.

La gestione del registro dei nomi TLD può comprendere la prestazione di servizi DNS. In base alle regole della IANA sulle deleghe, ad esempio, il soggetto cui è assegnata la gestione

[26] Per maggiori particolari sul rapporto tra la direttiva NIS e la direttiva 2002/21/CE, cfr. punto 5.2.

di un dato ccTLD deve anche occuparsi, nel paese in questione, della supervisione dei nomi di dominio e della gestione del DNS[27]. Gli Stati membri devono tener conto di queste circostanze quando effettuano il processo di identificazione degli operatori di servizi essenziali ai sensi dell'articolo 5, paragrafo 2.

4.1.2. Identificazione degli operatori di servizi essenziali

In applicazione dell'articolo 5 della direttiva ciascuno Stato membro è tenuto ad effettuare un processo di identificazione per tutti i soggetti dei tipi elencati nell'allegato II con sede nel suo territorio. In esito alla valutazione, tutti i soggetti rispondenti ai criteri dell'articolo 5, paragrafo 2, sono identificati come operatori di servizi essenziali e sottoposti agli obblighi di sicurezza e di notifica previsti all'articolo 14.

Gli Stati membri hanno tempo fino al 9 novembre 2018 per identificare gli operatori di ciascun settore e sottosettore. Per sostenere gli Stati membri in questo processo il gruppo di cooperazione sta redigendo un documento d'indirizzo contenente le informazioni d'interesse sulle diverse fasi necessarie e indicante le migliori pratiche relative all'identificazione degli operatori di servizi essenziali.

A norma dell'articolo 24, paragrafo 2, il gruppo di cooperazione è altresì tenuto ad esaminare la procedura, la sostanza e il tipo delle misure nazionali che consentono l'identificazione degli operatori di servizi essenziali in settori specifici. Uno Stato membro può chiedere al gruppo di cooperazione, entro il 9 novembre 2018, di esaminare i progetti di misure nazionali che consentono l'identificazione degli operatori di servizi essenziali.

4.1.3. Estensione ad altri settori

In considerazione dell'obbligo di armonizzazione minima imposto dall'articolo 3, gli Stati membri possono adottare o mantenere in vigore disposizioni normative atte a conseguire un livello di sicurezza più elevato delle reti e dei sistemi informativi. In questo senso sono in generale liberi di estendere gli obblighi di sicurezza e di notifica dell'articolo 14 a soggetti di settori e sottosettori diversi da quelli elencati nell'allegato II della direttiva NIS. Vari Stati membri hanno deciso di estendere gli obblighi ad alcuni dei settori elencati qui di seguito, o stanno vagliando l'ipotesi di procedere in tal senso.

i) Pubblica amministrazione

È possibile che la pubblica amministrazione offra servizi essenziali indicati nell'allegato II della direttiva che soddisfano le condizioni previste all'articolo 5, paragrafo 2, della stessa. In tal caso è sottoposta ai pertinenti obblighi di sicurezza e di notifica. Se non rientrano invece nell'ambito indicato, i servizi offerti dalla pubblica amministrazione non sono vincolati a tali obblighi.

La pubblica amministrazione è responsabile della regolare erogazione dei servizi pubblici prestati dagli enti statali, regionali e locali, dalle agenzie e dalle imprese consociate. Spesso questi servizi implicano la generazione e la gestione di dati personali e aziendali relativi a persone fisiche e a organizzazioni, dati che possono essere condivisi e messi a disposizione di

[27] Per ulteriori informazioni cfr. https://www.icann.org/resources/pages/delegation-2012-02-25-en.

vari soggetti del settore pubblico. In termini più generali, un livello elevato di sicurezza delle reti e dei sistemi informativi usati dalla pubblica amministrazione è un interesse rilevante della società e dell'economia nel loro complesso. La Commissione reputa pertanto opportuno che gli Stati membri valutino l'ipotesi d'includere la pubblica amministrazione nell'ambito di applicazione della normativa nazionale di attuazione della direttiva, al di là della prestazione di servizi essenziali di cui all'allegato II e all'articolo 5, paragrafo 2.

ii) Settore postale

Il settore postale ricomprende l'erogazione di servizi postali quali la raccolta, lo smistamento, il trasporto e la distribuzione degli invii postali.

iii) Settore alimentare

Il settore alimentare abbraccia la produzione dei prodotti agricoli e degli altri prodotti alimentari e potrebbe includere servizi essenziali come la sicurezza dell'approvvigionamento alimentare e la garanzia della sicurezza e della qualità degli alimenti.

iv) Industria chimica e nucleare

L'industria chimica e nucleare è dedita in particolare allo stoccaggio, alla produzione e alla trasformazione di prodotti chimici e petrolchimici o di materie nucleari.

v) Settore ambientale

Rientrano fra le attività ambientali la fornitura dei beni e la prestazione dei servizi necessari per tutelare l'ambiente e gestirne le risorse. Le attività sono mirate pertanto alla prevenzione, riduzione e eliminazione dell'inquinamento e alla preservazione del patrimonio di risorse naturali. In questo settore potrebbero costituire servizi essenziali il monitoraggio e il controllo dell'inquinamento (ad esempio, atmosferico o delle acque) e dei fenomeni meteorologici.

vi) Protezione civile

Nel settore della protezione civile l'obiettivo è la prevenzione delle calamità naturali e antropiche, la preparazione a farvi fronte e la capacità di rispondervi. I servizi prestati a tal fine possono comprendere l'attivazione di numeri di emergenza e le azioni per informare sulle emergenze, contenerle e rispondervi.

4.1.4. Giurisdizione

A norma dell'articolo 5, paragrafo 1, ciascuno Stato membro è tenuto a identificare gli operatori di servizi essenziali con una sede nel suo territorio. La disposizione non precisa che cosa s'intenda giuridicamente per "sede", ma il considerando 21 chiarisce che lo stabilimento in uno Stato membro implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile, senza che sia determinante la forma giuridica assunta. Questo significa che può ricadere nella giurisdizione dello Stato membro non soltanto l'operatore di servizi essenziali che ha la sede sociale sul suo territorio, ma anche l'operatore che vi ha, ad esempio, una succursale o altro tipo di stabilimento legale.

Può di conseguenza verificarsi che lo stesso soggetto ricada contemporaneamente nella giurisdizione di diversi Stati membri.

4.1.5. Informazioni da presentare alla Commissione

Ai fini del riesame che la Commissione deve effettuare a norma dell'articolo 23, paragrafo 1, della direttiva NIS, gli Stati membri sono tenuti a presentarle, entro il 9 novembre 2018 e successivamente ogni due anni, le informazioni seguenti:

- le misure nazionali che consentono l'identificazione degli operatori di servizi essenziali;
- l'elenco dei servizi essenziali;
- il numero degli operatori di servizi essenziali identificati per ciascun settore di cui all'allegato II e la loro rilevanza nel settore;
- le soglie, ove esistono, usate per determinare il livello di fornitura con riferimento al numero di utenti che dipendono da tale servizio di cui all'articolo 6, paragrafo 1, lettera a), o all'importanza del soggetto a norma dell'articolo 6, paragrafo 1, lettera f).

Il riesame previsto all'articolo 23, paragrafo 1, che precede la revisione completa della direttiva, dà riscontro all'importanza che i colegislatori annettono a una corretta attuazione della direttiva sotto il profilo dell'identificazione degli operatori di servizi essenziali al fine di evitare la frammentazione del mercato.

Affinché questo processo possa compiersi nel miglior modo possibile, la Commissione esorta gli Stati membri a discutere la questione nel gruppo di cooperazione e a condividervi le esperienze maturate al riguardo. La Commissione incoraggia inoltre gli Stati membri a trasmetterle - in aggiunta alle informazioni da comunicarle ai sensi della direttiva e se del caso in via riservata - l'elenco degli operatori di servizi essenziali identificati (e quindi selezionati). La disponibilità di tali elenchi agevolerebbe la Commissione nella valutazione dell'uniformità del processo di identificazione e ne migliorerebbe la qualità, consentendole peraltro di raffrontare le impostazioni seguite dai diversi Stati membri; il risultato sarebbe un miglioramento nella realizzazione degli obiettivi della direttiva.

4.1.6. Svolgimento del processo di identificazione

Nel processo di identificazione di un dato soggetto l'autorità nazionale dovrebbe valutare sei aspetti fondamentali, sintetizzati nelle domande riportate nella figura 4. Nei capoversi che seguono ogni domanda corrisponde a una fase dell'iter a norma dell'articolo 5 in combinato disposto con l'articolo 6 e in considerazione dell'applicabilità dell'articolo 1, paragrafo 7.

Fase 1 – **Il soggetto rientra in uno dei (sotto)settori e corrisponde a uno dei tipi contemplati nell'allegato II della direttiva?**

L'autorità nazionale dovrebbe valutare se il soggetto stabilito nel territorio del suo paese rientra in uno dei settori o sottosettori elencati nell'allegato II della direttiva. L'allegato II contempla vari settori economici che sono considerati funzionali al regolare funzionamento del mercato interno, in particolare i settori e sottosettori seguenti:

- energia: energia elettrica, petrolio e gas;

- trasporti: trasporto aereo, ferroviario, per via navigabile e su strada;
- settore bancario: enti creditizi;
- infrastrutture dei mercati finanziari: sedi di negoziazione, controparti centrali;
- sanità: presidi sanitari (compresi ospedali e cliniche private);
- acqua: fornitura e distribuzione di acqua potabile;
- infrastrutture digitali: punti di interscambio internet, fornitori di servizi di sistema dei nomi di dominio, registri dei nomi di dominio di primo livello[28].

Fase 2 – **Si applica una lex specialis?**

L'autorità nazionale deve valutare se si applichi la disposizione sulla lex specialis prevista dall'articolo 1, paragrafo 7, ai cui sensi, qualora un atto giuridico dell'Unione imponga ai fornitori di servizi digitali o agli operatori di servizi essenziali obblighi di sicurezza e/o di notifica almeno equivalenti a quelli della direttiva NIS, si applicano gli obblighi imposti da detto atto giuridico speciale. Il considerando 9 precisa che, in presenza delle condizioni previste all'articolo 1, paragrafo 7, gli Stati membri dovrebbero applicare le disposizioni dell'atto giuridico settoriale dell'Unione, comprese quelle in materia di giurisdizione, mentre non sarebbero d'applicazione le disposizioni della direttiva NIS. In tal caso l'autorità competente dovrebbe interrompere il processo di identificazione previsto all'articolo 5, paragrafo 2[29].

Fase 3 – **L'operatore fornisce un servizio essenziale ai sensi della direttiva?**

A norma dell'articolo 5, paragrafo 2, lettera a), il soggetto sottoposto a identificazione deve fornire un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali. Nella valutazione gli Stati membri dovrebbero tener conto del fatto che uno stesso soggetto può fornire sia servizi essenziali che servizi non essenziali; di conseguenza, gli obblighi di sicurezza e di notifica della direttiva NIS gli si applicheranno soltanto per le attività di fornitura di servizi essenziali.

Ai sensi dell'articolo 5, paragrafo 3, lo Stato membro dovrebbe stendere un elenco di tutti i servizi essenziali prestati nel suo territorio da operatori di servizi essenziali. L'elenco dovrà essere trasmesso alla Commissione entro il 9 novembre 2018 e, in seguito, ogni due anni[30].

Fase 4 – **Il servizio dipende da una rete e un sistema informativo?**

Occorre indicare se il servizio soddisfa il secondo criterio dell'articolo 5, paragrafo 2, lettera b), in particolare se la fornitura del servizio essenziale dipende da una rete e un sistema informativo quale definiti all'articolo 4, punto 1.

Fase 5 – **Un incidente di sicurezza produrrebbe effetti negativi rilevanti?**

L'articolo 5, paragrafo 2, lettera c), impone all'autorità nazionale di valutare se un incidente possa avere effetti negativi rilevanti sulla fornitura del servizio. A tal fine l'articolo 6,

[28]Per un approfondimento su questi soggetti cfr. sezione 4.1.1.
[29] Per un approfondimento sull'applicabilità della lex specialis cfr. sezione 5.1.
[30] Cfr. articolo 5, paragrafo 7, lettera b).

paragrafo 1, elenca i fattori intersettoriali di cui occorre tenere conto nella valutazione, mentre l'articolo 6, paragrafo 2, stabilisce che, ove opportuno, la valutazione tenga conto anche di fattori settoriali.

I **fattori intersettoriali** elencati all'articolo 6, paragrafo 1, sono i seguenti:

- il numero di utenti che dipendono dal servizio fornito dal soggetto;
- la dipendenza di altri settori di cui all'allegato II dal servizio fornito dal soggetto;
- l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;
- la quota di mercato del soggetto;
- la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;
- l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

Quanto ai **fattori settoriali**, il considerando 28 presenta alcuni esempi (cfr. tabella 4) che potrebbero orientare utilmente le autorità nazionali.

Tabella 4: Esempi di fattori settoriali di cui tenere conto per stabilire se un incidente possa produrre effetti negativi rilevanti

Settore	Esempi di fattori settoriali
fornitori di energia	volume o quota di energia nazionale prodotta
fornitori di petrolio	volume di petrolio fornito su base giornaliera
trasporto aereo (inclusi aeroporti e vettori aerei) **trasporto ferroviario** **porti marittimi**	quota di volume di traffico nazionale; numero di passeggeri o di operazioni di trasporto merci su base annua
settore bancario e infrastrutture dei mercati finanziari	importanza sistemica in base alle attività totali; rapporto tra attività totali e PIL
settore sanitario	numero di pazienti assistiti dal fornitore su base annua
produzione, trattamento e fornitura di acqua	volume e numero e tipi di utenti riforniti (inclusi, ad esempio, ospedali, servizi pubblici, organizzazioni o persone fisiche); esistenza di fonti idriche alternative per servire la stessa area geografica

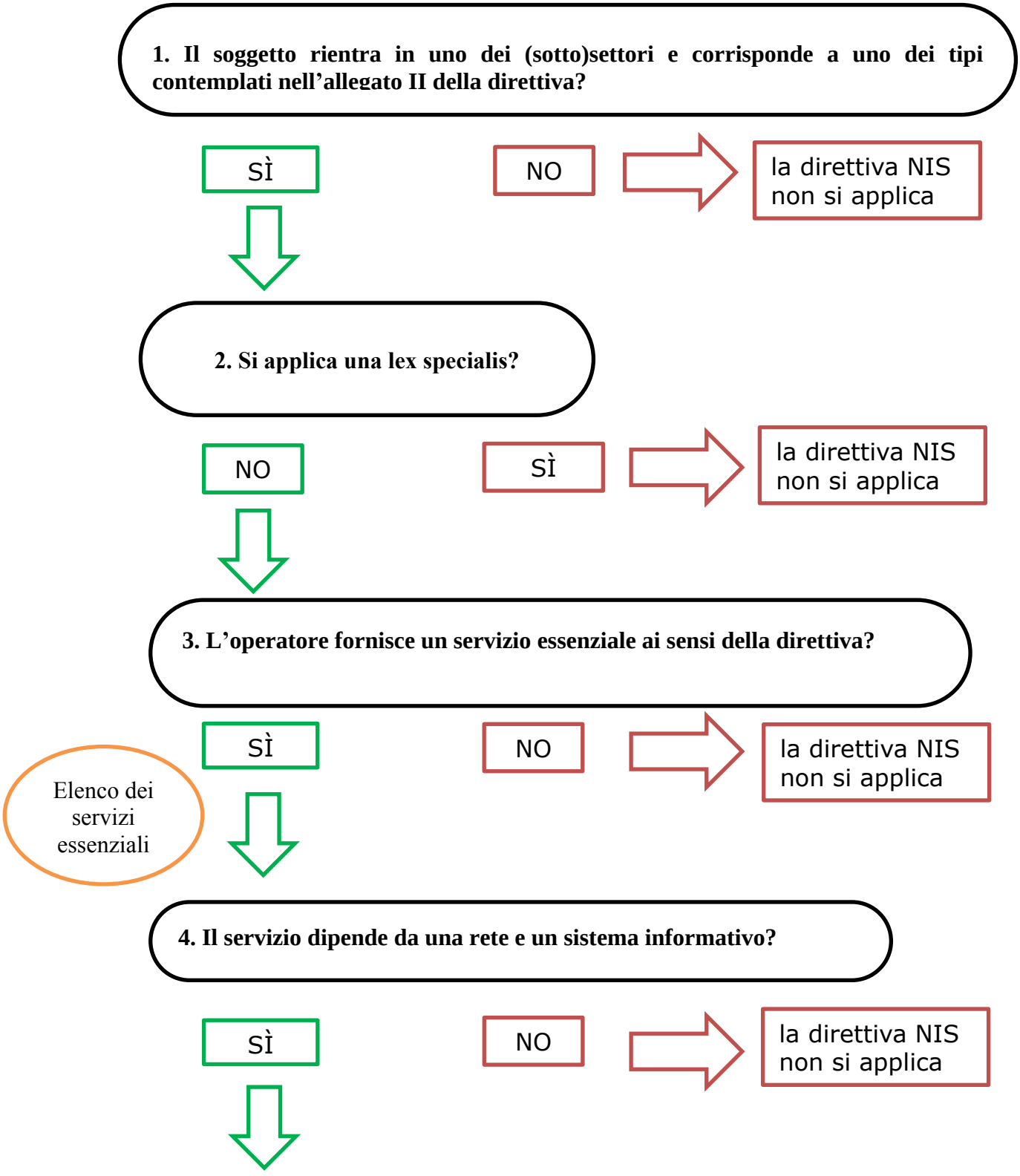
Per effettuare la valutazione ai sensi dell'articolo 5, paragrafo 2, gli Stati membri non dovrebbero aggiungere altri criteri rispetto a quelli elencati in tale disposizione, perché una tale aggiunta potrebbe ridurre il numero degli operatori di servizi essenziali identificati e metterne a repentaglio l'armonizzazione minima disposta dall'articolo 3 della direttiva.

Fase 6 **– L’operatore presta servizi essenziali in altri Stati membri?**

Sono contemplati i casi in cui l’operatore fornisce servizi essenziali in due o più Stati membri. L’articolo 5, paragrafo 4, impone agli Stati membri interessati di consultarsi prima che sia concluso il processo d’identificazione[31].

[31] Per un approfondimento sul processo di consultazione cfr. sezione 4.1.7.

Figura 4. Processo di identificazione in 6 fasi



5. Un incidente di sicurezza produrrebbe effetti negativi rilevanti?

Fattori intersettoriali (articolo 6, paragrafo 1)

- **Numero di utenti** che dipendono dal servizio
- **Dipendenza** di altri settori essenziali dal servizio
- Impatto che gli incidenti potrebbero avere sulle **attività economiche e sociali** o sulla **pubblica sicurezza**
- Possibile **diffusione geografica**
- Importanza del soggetto per il mantenimento di un **livello** sufficiente **del servizio**

Fattori settoriali (esempi indicati al considerando 28)

- **Energia**: volume o quota di energia nazionale prodotta
- **Trasporti**: quota di volume di traffico nazionale e numero di operazioni su base annua
- **Sanità**: numero di pazienti assistiti dal fornitore su base annua

SÌ

NO → la direttiva NIS non si applica

6. L'operatore presta servizi essenziali in altri Stati membri?

SÌ

NO → la direttiva NIS non si applica

Consultazione obbligatoria con gli Stati membri interessati

Adozione di misure nazionali (ad esempio, elenco degli operatori di servizi essenziali, misure giuridiche e interventi politici).

4.1.7. Processo di consultazione transfrontaliera

Quando un operatore presta servizi essenziali in due o più Stati membri, l'articolo 5, paragrafo 4, impone agli Stati membri interessati di consultarsi prima che sia concluso il processo d'identificazione. Lo scopo della consultazione è agevolare la valutazione della criticità dell'operatore in termini di impatto transfrontaliero.

L'esito ricercato con la consultazione è permettere alle autorità nazionali di confrontarsi sulle rispettive posizioni e argomentazioni per, idealmente, convergere nelle conclusioni sull'identificazione dell'operatore. La direttiva NIS non osta tuttavia a che gli Stati membri giungano a conclusioni diverse sull'opportunità di identificare il soggetto come operatore di servizi essenziali. Il considerando 24 menziona la possibilità, per gli Stati membri, di chiedere l'assistenza del gruppo di cooperazione al riguardo.

A parere della Commissione, gli Stati membri dovrebbero adoperarsi per giungere ad una conclusione consensuale su questi aspetti, in modo da evitare che la stessa impresa si ritrovi inquadrata in un diverso status giuridico nei diversi Stati membri. La divergenza delle conclusioni dovrebbe costituire l'eccezione, ad esempio quando il soggetto identificato come operatore di servizi essenziali in uno Stato membro ha un'attività marginale e irrilevante in un altro.

4.2. Obblighi di sicurezza

A norma dell'articolo 14, paragrafo 1, gli Stati membri devono provvedere a che, tenuto conto delle conoscenze più aggiornate, gli operatori di servizi essenziali adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni. L'articolo 14, paragrafo 2, dispone l'adozione di misure adeguate per prevenire e minimizzare l'impatto degli incidenti.

Il gruppo di cooperazione sta lavorando, in un filone di attività specifico, alla stesura di orientamenti non vincolanti sulle misure di sicurezza per gli operatori di servizi essenziali[32]. Il gruppo perfezionerà il documento d'indirizzo entro il quarto trimestre 2017. La Commissione esorta gli Stati membri ad attenersi rigorosamente a tale documento, in modo da riuscire ad allineare il più possibile le disposizioni nazionali sugli obblighi di sicurezza. L'armonizzazione di tali obblighi faciliterebbe notevolmente sia la messa in conformità degli operatori di servizi essenziali, che spesso forniscono servizi essenziali in più di uno Stato membro, sia le funzioni di vigilanza delle autorità nazionali competenti e dei CSIRT.

4.3 Obblighi di notifica

A norma dell'articolo 14, paragrafo 3, gli Stati membri sono tenuti a provvedere a che gli operatori di servizi essenziali notifichino "*gli incidenti aventi un impatto rilevante sulla*

[32] Nel citato filone di attività sono stati distribuiti elenchi delle norme, buone pratiche e metodologie di valutazione/gestione del rischio seguite a livello internazionale in tutti i settori contemplati dalla direttiva NIS, che sono andati ad alimentare la riflessione sui domini di protezione e le misure di sicurezza proposti.

continuità dei servizi essenziali prestati". Detti operatori, quindi, non dovrebbero notificare gli incidenti di lieve entità, ma soltanto gli incidenti gravi che compromettono la continuità del servizio essenziale. Nella definizione dell'articolo 4, punto 7, l'incidente è "*ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi*". L'articolo 4, punto 2, definisce a sua volta l'espressione "sicurezza della rete e dei sistemi informativi" come la capacità della rete "*di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi*". In potenza, quindi, l'obbligo di notifica potrebbe scattare al verificarsi di qualsiasi evento che produca effetti negativi non soltanto sulla disponibilità, ma anche sull'autenticità, l'integrità o la riservatezza dei dati o dei servizi collegati. La continuità del servizio di cui all'articolo 14, paragrafo 3, può infatti risultare compromessa non soltanto nei casi che implicano la disponibilità fisica, ma anche al verificarsi di qualsiasi altro incidente di sicurezza che vada a intaccare la regolare prestazione del servizio[33].

Il gruppo di cooperazione sta elaborando, in un filone di attività specifico, orientamenti non vincolanti sulla notifica, per i casi in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti a norma dell'articolo 14, paragrafo 7, e sul formato e la procedura applicabili alle notifiche nazionali. Gli orientamenti dovrebbero essere completati entro il quarto trimestre 2017.

L'esistenza di obblighi nazionali di notifica divergenti può dar luogo a incertezza giuridica, a procedure più complesse e gravose e a costi amministrativi considerevoli per i fornitori che operano a livello transfrontaliero. La Commissione accoglie quindi con favore il lavoro del gruppo di cooperazione. Come per gli obblighi di sicurezza, la Commissione esorta gli Stati membri ad attenersi rigorosamente al documento d'indirizzo che sarà elaborato dal gruppo di cooperazione, in modo da riuscire ad allineare il più possibile le disposizioni nazionali sulla notifica degli incidenti.

4.4. Direttiva NIS, allegato III - Fornitori di servizi digitali

I fornitori di servizi digitali costituiscono la seconda categoria di soggetti cui si applica la direttiva NIS. Sono considerati protagonisti importanti dell'economia, perché molte imprese si rivolgono a loro per i servizi che prestano e perché una perturbazione del servizio digitale fornito potrebbe avere un impatto su attività economiche e sociali fondamentali.

4.4.1. Categorie di fornitori di servizi digitali

Per definire il "servizio digitale" l'articolo 4, punto 5, rimanda alla definizione giuridica contenuta nell'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535, limitandone l'ambito di applicazione ai tipi di servizi elencati nell'allegato III. L'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 definisce tale servizio come "qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi" e l'allegato III della direttiva elenca tre tipi specifici

[33] Lo stesso vale per i fornitori di servizi digitali.

di servizio: mercato online, motore di ricerca online e servizio nella nuvola (cloud computing). Diversamente dagli operatori di servizi essenziali, la direttiva non impone agli Stati membri di identificare i fornitori di servizi digitali, che sono quindi sottoposti comunque ai pertinenti obblighi. Gli obblighi della direttiva, vale a dire gli obblighi di sicurezza e di notifica previsti all'articolo 16, valgono pertanto per tutti i fornitori di servizi digitali ai quali essa si applica.

Nelle sezioni che seguono sono illustrati in maggior dettaglio i tre tipi di servizi digitali ricompresi nell'ambito di applicazione della direttiva.

1. Fornitore di servizi del mercato online

Il mercato online permette a numerose imprese di vario genere d'interagire commercialmente con i consumatori e di allacciare rapporti con altre imprese. Mette a disposizione delle imprese l'infrastruttura di base per operare in rete e attraverso le frontiere. Svolge una funzione importante nell'economia, in particolare offrendo alle PMI accesso al grande mercato unico digitale dell'UE. Possono rientrare fra le attività del fornitore di servizi del mercato digitale anche la prestazione di servizi di informatica in remoto atti ad facilitare l'attività economica del cliente, come l'elaborazione di operazioni e l'aggregazione di informazioni sugli acquirenti, i fornitori e i prodotti, così come i servizi di agevolazione della ricerca di prodotti adeguati, la fornitura di prodotti, la messa a disposizione di conoscenze sulle operazioni e l'abbinamento tra compratori e venditori.

L'espressione "mercato online", che è definita all'articolo 4, punto 17, e precisata nel considerando 15, indica un servizio che consente ai consumatori e ai professionisti di concludere contratti di vendita o di servizi online con i professionisti, e costituisce la destinazione finale per la conclusione di tali contratti. *E-bay*, ad esempio, è un fornitore che può essere considerato un mercato online, perché permette ad altri di aprire sulla sua piattaforma un negozio in cui mettere i loro prodotti e servizi a disposizione dei consumatori e delle imprese nell'ambiente online. Anche i negozi online di applicazioni attivi nella distribuzione di applicazioni e programmi informatici sono considerati corrispondere alla definizione di mercato online, perché permettono agli sviluppatori di applicazioni di vendere o distribuire i loro servizi ai consumatori o ad altre imprese. Esulano invece dalla definizione dell'articolo 4, punto 17, gli intermediari di servizi prestati da terzi, quali ad esempio *Skyscanner* e i servizi di confronto dei prezzi, che per l'effettiva conclusione del contratto di acquisto del prodotto o del servizio reinstradano l'utente verso il sito internet del professionista.

2. Fornitore di servizi di motore di ricerca online

L'espressione "motore di ricerca online", che è definita all'articolo 4, punto 18, e precisata nel considerando 16, indica un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o sui siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema. Non sono contemplate le funzioni di ricerca limitate alla ricerca interna a un sito e ai siti internet di confronto dei prezzi. I motori di ricerca del tipo di

quello contenuto in Eur-Lex[34], ad esempio, non possono essere considerati motori di ricerca ai sensi della direttiva perché la loro funzione di ricerca è limitata al contenuto del concreto sito web che la mette a disposizione.

3. Fornitore di servizi nella nuvola (cloud computing)

L'articolo 4, punto 19, definisce il servizio nella nuvola (cloud computing) come "un servizio digitale che consente l'accesso a un insieme scalabile e elastico di risorse informatiche condivisibili"; il considerando 17 chiarisce i concetti di "risorse informatiche" e di "insieme scalabile e elastico".

In sintesi, il cloud computing può essere descritto come un tipo particolare di servizio informatico che usa risorse condivise per elaborare dati su richiesta, dove le "risorse condivise" possono essere qualsiasi tipo di componenti di hardware o di software (ad es., reti, server o altre infrastrutture, servizi di archiviazione, applicazioni e servizi) erogate su richiesta agli utenti per l'elaborazione di dati. In relazione alle risorse informatiche l'aggettivo "condivisibili" indica che una molteplicità di utenti condivide la stessa infrastruttura fisica per l'elaborazione dei dati. Le risorse informatiche possono essere qualificate di "condivisibili" se l'insieme delle risorse usate dal prestatore del servizio può essere esteso o ridotto in qualsiasi momento a seconda delle esigenze dell'utente. Questo implica che, quando occorre aggiornare il volume totale della capacità di calcolo o di archiviazione, sarà possibile aggiungere o sopprimere centri di dati o singoli componenti all'interno di un centro di dati. Con l'espressione "insieme elastico" ci si riferisce alla variazione del carico di lavoro tramite l'attivazione e la disattivazione automatica delle risorse, in modo che in ogni dato momento le risorse disponibili corrispondano il più possibile alla domanda[35].

Attualmente i fornitori di cloud computing propongono principalmente tre modelli di servizio:

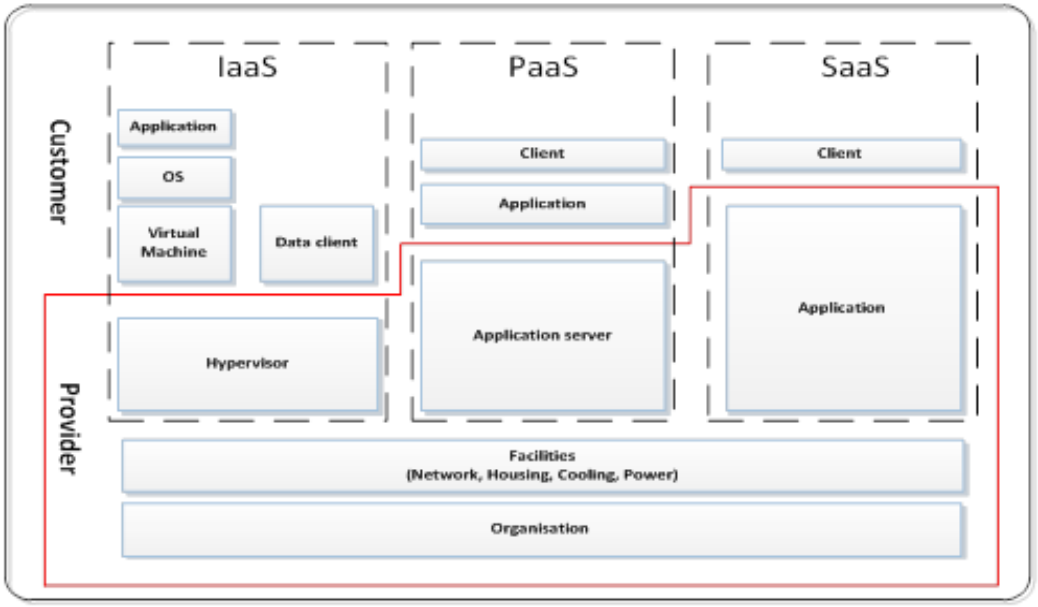
- a livello di infrastruttura (IaaS): categoria di servizio di nuvola in cui la capacità messa a disposizione del cliente è un'infrastruttura. Comprende l'erogazione virtuale di risorse informatiche sotto forma di hardware, capacità di rete e servizi di archivio. Il modello IaaS alimenta server, sistemi di archiviazione, reti e sistemi operativi. Mette a disposizione delle imprese un'infrastruttura aziendale in cui archiviare i dati e far girare le applicazioni necessarie per il funzionamento quotidiano;

- a livello di piattaforma (PaaS): categoria di servizio di nuvola in cui la capacità messa a disposizione del cliente è una piattaforma. Comprende le piattaforme informatiche online tramite cui le imprese possono far girare le applicazioni esistenti o svilupparne e testarne di nuove;

[34] Cfr. http://eur-lex.europa.eu/homepage.html.
[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, "Elasticity in Cloud Computing: What It Is, and What It Is Not" - cfr. https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Cfr. anche pagine 2-6 del COM(2012) 529.

- a livello di software (SaaS): categoria di servizio di nuvola in cui la capacità messa a disposizione del cliente è un'applicazione o un software utilizzabili in remoto attraverso internet. Questo tipo di servizi di nuvola libera l'utente finale dalla necessità di acquistare, installare e gestire il software e presenta il vantaggio di rendere il software accessibile da qualsiasi luogo in cui vi sia un collegamento internet.

Figura 5. Modelli di servizio e risorse nella nuvola informatica



L'ENISA ha emanato linee guida complete su aspetti specifici del cloud[36] e un documento d'indirizzo sui fondamenti della nuvola informatica[37].

4.4.2. Obblighi di sicurezza

A norma dell'articolo 16, paragrafo 1, gli Stati membri devono provvedere a che i fornitori di servizi digitali adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dell'offerta di servizi. Tali misure dovrebbero tener conto delle conoscenze più aggiornate e dei cinque elementi seguenti: i) sicurezza dei sistemi e degli impianti; ii) trattamento degli incidenti; iii) gestione della continuità operativa; iv) monitoraggio, audit e test; v) conformità con le norme internazionali.

In questo contesto l'articolo 16, paragrafo 8, conferisce alla Commissione il potere di adottare atti di esecuzione che specifichino ulteriormente tali elementi e assicurino un livello elevato di armonizzazione per i fornitori di questi servizi. La Commissione prevede di adottare l'atto di

[36] Cfr. https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security.
[37] ENISA, *Cloud Security Guide for SMEs* (2015). Cfr. https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

esecuzione in materia nell'autunno 2017. Gli Stati membri devono altresì provvedere a che i fornitori di servizi digitali adottino le misure necessarie per prevenire e minimizzare l'impatto degli incidenti al fine di assicurare la continuità dei servizi che prestano.

4.4.3. Obblighi di notifica

I fornitori di servizi digitali dovrebbero essere tenuti a notificare gli incidenti gravi alle autorità competenti o ai CSIRT. A norma dell'articolo 16, paragrafo 3, della direttiva NIS, quest'obbligo di notifica scatta quando l'incidente di sicurezza ha un impatto rilevante sulla fornitura del servizio. L'articolo 16, paragrafo 4, elenca cinque parametri di cui fornitori di servizi digitali devono tenere conto per determinare se l'impatto dell'incidente sia rilevante. In questo contesto l'articolo 16, paragrafo 8, conferisce alla Commissione il potere di adottare atti di esecuzione che specifichino ulteriormente tali parametri. Quest'ulteriore specificazione dei parametri costituirà uno degli elementi dell'atto di esecuzione in cui saranno specificati gli elementi di sicurezza di cui al punto 4.4.2, che la Commissione intende adottare in autunno.

4.4.4. Approccio normativo basato sul rischio

L'articolo 17 dispone che i fornitori di servizi digitali siano sottoposti al controllo di vigilanza ex post delle autorità nazionali competenti. Gli Stati membri devono provvedere a che le autorità competenti adottino provvedimenti quando ottengono la prova che un fornitore di servizi digitali non rispetta gli obblighi di cui all'articolo 16 della direttiva.

A norma dell'articolo 16, paragrafi 8 e 9, alla Commissione è conferito il potere di adottare atti di esecuzione sugli obblighi di notifica e di sicurezza che innalzeranno il livello di armonizzazione fra i fornitori di servizi digitali. A norma dell'articolo 16, paragrafo 10, gli Stati membri non possono imporre ai fornitori di servizi digitali ulteriori obblighi in materia di sicurezza o di notifica oltre a quelli previsti dalla direttiva, tranne quando il provvedimento è necessario per salvaguardare le funzioni essenziali dello Stato, in particolare quelle di tutela della sicurezza nazionale, e per consentire le attività di indagine, accertamento e perseguimento dei reati.

In considerazione della transnazionalità dei fornitori di servizi digitali, la direttiva non applica il modello basato su una pluralità di giurisdizioni parallele, bensì un approccio fondato sul criterio dello stabilimento principale della società nell'UE[38]. In questo modo è possibile applicare ai fornitori di servizi digitali uno stesso complesso di norme, con una sola autorità competente della vigilanza; si tratta di un aspetto particolarmente importante perché numerosi fornitori di servizi digitali offrono simultaneamente servizi in molti Stati membri. Quest'approccio allevia il più possibile l'onere di conformità ai fornitori di servizi digitali e assicura il regolare funzionamento del mercato unico digitale.

4.4.5. Giurisdizione

Come già accennato, l'articolo 18, paragrafo 1, della direttiva NIS sottopone il fornitore di servizi digitali alla giurisdizione dello Stato membro in cui ha lo stabilimento principale. A norma dell'articolo 18, paragrafo 2, il fornitore di servizi digitali che non è stabilito nel

[38] Cfr., in particolare, articolo 18 della direttiva.

territorio dell'UE ma vi offre servizi deve designare un rappresentate nell'Unione. In tal caso, il fornitore di servizi digitali è soggetto alla giurisdizione dello Stato membro in cui è stabilito il suo rappresentante. Se il fornitore di servizi digitali presta servizi in uno Stato membro senza aver designato un rappresentante nell'UE, lo Stato membro può, in via di principio, adottare provvedimenti nei suoi confronti, in quando il fornitore è in violazione degli obblighi derivanti dalla direttiva.

4.4.6. Esenzione dei fornitori di servizi digitali di dimensioni limitate dagli obblighi di sicurezza e di notifica

A norma dell'articolo 16, paragrafo 11, gli obblighi di sicurezza e di notifica imposti da questo stesso articolo non si applicano ai fornitori di servizi digitali che sono microimprese o piccole imprese ai sensi della raccomandazione 2003/361/CE della Commissione[39]. Questo significa che tali obblighi non vincolano le imprese con meno di 50 dipendenti e con un fatturato annuo e/o un totale di bilancio annuo non superiore a 10 milioni di euro. Per stabilire le dimensioni dell'impresa è irrilevante che questa presti esclusivamente servizi digitali ai sensi della direttiva NIS o anche altri servizi.

5. Rapporto tra la direttiva NIS e altri atti legislativi

La presente sezione tratta delle disposizioni sulla lex specialis previste dall'articolo 1, paragrafo 7, della direttiva NIS illustrando i tre esempi di lex specialis valutati finora dalla Commissione e precisando gli obblighi di sicurezza e di notifica applicabili al settore delle telecomunicazioni e ai prestatori di servizi fiduciari.

5.1. Direttiva NIS, articolo 1, paragrafo 7 - Disposizione sulla lex specialis

A norma dell'articolo 1, paragrafo 7, della direttiva NIS, le disposizioni sugli obblighi di sicurezza e/o di notifica che la direttiva impone ai fornitori di servizi digitali o agli operatori di servizi essenziali non sono applicabili quando una normativa settoriale dell'UE prevede obblighi di sicurezza e/o di notifica che hanno effetti almeno equivalenti a quelli della direttiva. Gli Stati membri devono tenere conto dell'articolo 1, paragrafo 7, nel recepimento generale della direttiva e informare la Commissione in merito all'applicazione delle disposizioni sulla lex specialis.

Metodologia

Per valutare l'equivalenza di un atto giuridico settoriale dell'UE con le pertinenti disposizioni della direttiva NIS, è particolarmente importante stabilire se gli obblighi di sicurezza imposti dalla normativa settoriale comprendano misure atte a garantire la sicurezza della rete e dei sistemi informativi quale definita all'articolo 4, punto 2, della direttiva.

Quanto agli obblighi di notifica, l'articolo 14, paragrafo 3, e l'articolo 16, paragrafo 3, della direttiva NIS prevedono che gli operatori di servizi essenziali e i fornitori di servizi digitali

[39] GU L 24 del 20.5.2003, pag. 36.

notifichino senza indebito ritardo all'autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla fornitura del servizio. In questo contesto occorre prestare particolare attenzione agli obblighi dell'operatore/del fornitore di servizi digitali d'includere nella notifica le informazioni che consentono all'autorità competente o al CSIRT di determinare se l'incidente di sicurezza produca un impatto transfrontaliero.

Ai fini dell'applicazione dell'articolo 1, paragrafo 7, della direttiva NIS, attualmente non vige per la categoria dei fornitori di servizi digitali alcuna normativa settoriale che preveda obblighi di sicurezza e di notifica comparabili a quelli previsti all'articolo 16 della direttiva[40].

Per quanto riguarda gli operatori di servizi essenziali, si applicano attualmente nel settore finanziario, in particolare per i comparti delle banche e delle infrastrutture dei mercati finanziari di cui al punto 3 e al punto 4 dell'allegato II, obblighi di sicurezza e/o di notifica previsti da norme settoriali dell'UE, e questo perché la sicurezza e la solidità dell'infrastruttura informatica e delle reti e dei sistemi informativi usati dagli enti finanziari costituiscono uno degli elementi essenziali dell'assolvimento degli obblighi inerenti al rischio operativo cui tali enti sono sottoposti in virtù della normativa dell'UE.

Esempi

i) Seconda direttiva sui servizi di pagamento

Nel settore bancario, in particolare per quanto riguarda la prestazione di servizi di pagamento da parte degli enti creditizi quali definiti all'articolo 4, paragrafo 1, punto 1), del regolamento (UE) n. 575/2013, la cosiddetta seconda direttiva sui servizi di pagamento (PSD2)[41] prevede obblighi di sicurezza e di notifica agli articoli 95 e 96.

Più precisamente, a norma dell'articolo 95, paragrafo 1, i prestatori di servizi di pagamento sono tenuti a adottare misure di mitigazione e meccanismi di controllo adeguati per gestire i rischi operativi e di sicurezza relativi ai servizi di pagamento che prestano. Con tali misure i prestatori dovrebbero stabilire e gestire procedure efficaci di gestione degli incidenti, anche per quanto concerne l'individuazione e la classificazione degli incidenti operativi e di sicurezza gravi. I considerando 95 e 96 della PSD2 precisano la natura di queste misure di sicurezza. Dalle disposizioni citate emerge chiaramente che le misure previste intendono gestire i rischi di sicurezza che interessano la rete e i sistemi informativi usati per la prestazione di servizi di pagamento. Si può considerare pertanto che questi obblighi di sicurezza abbiano effetti almeno equivalenti alle corrispondenti disposizioni dell'articolo 14, paragrafi 1 e 2, della direttiva NIS.

Per quanto riguarda gli obblighi di notifica, l'articolo 96, paragrafo 1, della PSD2 impone al prestatore di servizi di pagamento di notificare senza indugio all'autorità competente qualsiasi incidente grave relativo alla sicurezza. Analogamente all'articolo 14, paragrafo 5, della

[40] Fatta salva la notifica di una violazione dei dati personali all'autorità di controllo di cui all'articolo 33 del regolamento generale sulla protezione dei dati.
[41] Direttiva (UE) 2015/2366, GU L 337 del 23.12.2015, pag. 35.

direttiva NIS, l'articolo 96, paragrafo 2, della PSD2 chiede all'autorità competente d'informare le omologhe degli altri Stati membri per i quali l'incidente ha rilevanza. Quest'obbligo implica la necessità d'includere nella segnalazione degli incidenti di sicurezza le informazioni che consentono alle autorità di valutare l'impatto transfrontaliero dell'incidente. L'articolo 96, paragrafo 3, lettera a), della PSD2 conferisce all'Autorità bancaria europea il potere di elaborare, in cooperazione con la Banca centrale europea, orientamenti sull'esatto contenuto e formato della notifica.

Per quanto riguarda la prestazione di servizi di pagamento da parte degli enti creditizi è pertanto legittimo concludere che, in applicazione dell'articolo 1, paragrafo 7, della direttiva NIS, si dovrebbero applicare gli articoli 95 e 96 della PSD2 anziché le corrispondenti disposizioni dell'articolo 14 della direttiva NIS.

ii) Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni

Per quanto riguarda le infrastrutture del mercato finanziario, il regolamento (UE) n. 648/2012 prevede, in combinato disposto con il regolamento delegato (UE) n. 153/2013 della Commissione, disposizioni sugli obblighi di sicurezza in capo alle controparti centrali (CCP) che possono essere considerate lex specialis. Detti atti giuridici prevedono in particolare misure tecniche e organizzative relative alla sicurezza della rete e dei sistemi informativi che, quanto a livello di dettaglio, vanno persino oltre gli obblighi dell'articolo 14, paragrafi 1 e 2, della direttiva NIS e che, in termini di obblighi di sicurezza, possono quindi essere considerate soddisfare le condizioni stabilite all'articolo 1, paragrafo 7, della stessa direttiva.

Nello specifico, l'articolo 26, paragrafo 1, del regolamento (UE) n. 648/2012 prevede che il soggetto debba essere dotato di "*solidi dispositivi di governo societario, ivi compresa una chiara struttura organizzativa con linee di responsabilità ben definite, trasparenti e coerenti, procedure efficaci per l'individuazione, la gestione, la sorveglianza e la segnalazione dei rischi ai quali sono o potrebbero essere esposte e adeguati meccanismi di controllo interno, tra cui valide procedure amministrative e contabili*". A norma dell'articolo 26, paragrafo 3, la struttura organizzativa deve assicurare la continuità e il regolare funzionamento dei servizi e delle attività mediante sistemi, risorse e procedure adeguati e proporzionati.

L'articolo 26, paragrafo 6, precisa che le CCP devono mantenere "*sistemi informatici adeguati per gestire la complessità, la diversità e il tipo dei servizi forniti e delle attività esercitate, in modo da assicurare norme di sicurezza elevate e l'integrità e la riservatezza delle informazioni detenute*". L'articolo 34, paragrafo 1, impone ai soggetti di adottare, attuare e mantenere una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, in grado di assicurare la ripresa tempestiva delle attività.

Detti obblighi sono precisati nel regolamento delegato (UE) n. 153/2013 della Commissione, del 19 dicembre 2012, che integra il regolamento (UE) n. 648/2012 del Parlamento europeo e

del Consiglio, per quanto riguarda le norme tecniche di regolamentazione relative ai requisiti per le controparti centrali[42]. In particolare, l'articolo 4 impone alle CCP l'obbligo di sviluppare idonei strumenti di gestione dei rischi così da essere in grado di gestire e riferire su tutti i rischi rilevanti; è altresì indicato il tipo di misure (ad es., impiego di solidi sistemi di informazione e di controllo del rischio, disponibilità di risorse, competenze e accesso a tutte le informazioni pertinenti per la funzione di gestione del rischio, disponibilità di adeguati meccanismi di controllo interno, quali procedure amministrative e contabili solide, per assistere il consiglio della CCP nel controllo e nella valutazione dell'adeguatezza e dell'efficacia delle sue politiche, procedure e sistemi di gestione dei rischi).

L'articolo 9 fa esplicito riferimento alla sicurezza dei sistemi informatici e impone una serie di misure tecniche e organizzative concrete finalizzate al mantenimento di un solido quadro di sicurezza informatica che permetta la gestione dei rischi in materia di sicurezza informatica. Tali misure dovrebbero comprendere i meccanismi e le procedure atti a garantire la disponibilità dei servizi e la salvaguardia dell'autenticità, dell'integrità e della riservatezza dei dati.

iii) Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE[43]

Con riguardo alle sedi di negoziazione l'articolo 48, paragrafo 1, della direttiva 2014/65/UE impone agli operatori di garantire la continuità dei servizi della sede in caso di malfunzionamento del sistema di negoziazione. Quest'obbligo generale è stato precisato e integrato di recente dal regolamento delegato (UE) 2017/584 della Commissione, del 14 luglio 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per specificare i requisiti organizzativi delle sedi di negoziazione[4445], il cui articolo 23, paragrafo 1, prevede in particolare che le sedi di negoziazione dispongano di procedure e disposizioni per la sicurezza fisica ed elettronica intese a proteggere i loro sistemi da abusi o accesso non autorizzato e a garantire l'integrità dei dati. Queste misure dovrebbero consentire la prevenzione o la minimizzazione dei rischi di attacchi contro i sistemi di informazione.

A norma dell'articolo 23, paragrafo 2, le misure e disposizioni adottate dagli operatori dovrebbero permettere di individuare prontamente e di gestire il rischio legato all'accesso non autorizzato, alle interferenze nel sistema che ostacolano gravemente o interrompono il funzionamento dei sistemi d'informazione e alle interferenze nei dati che ne compromettono la disponibilità, l'integrità o l'autenticità. L'articolo 15 del regolamento obbliga le sedi di negoziazione a dotarsi di efficaci disposizioni in materia di continuità operativa per garantire una sufficiente stabilità del sistema e far fronte a eventi perturbatori. Le misure dovrebbero in

[42] GU L 52 del 23.2.2013, pag. 41.
[43] GU L 173 del 12.6.2014, pag. 349.
[44] GU L 87 del 31.3.2017, pag. 350.
[45] http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017R0584&rid=1

particolare consentire all'operatore di riprendere le negoziazioni entro approssimativamente due ore e di assicurare che la quantità massima di dati perduti sia prossima allo zero.

A norma dell'articolo 16 il piano di continuità operativa delle sedi di negoziazione deve prevedere misure specifiche per far fronte agli eventi perturbatori e gestirli; sono quindi indicati determinati elementi che l'operatore deve tener presenti quando adotta il piano di continuità operativa (ad es., costituzione di uno specifico gruppo addetto alle operazioni di sicurezza, esecuzione di una valutazione di impatto che individui i rischi e che venga riesaminata periodicamente).

Visto il loro contenuto, le misure di sicurezza risultano essere volte a gestire e affrontare il rischio collegato alla disponibilità, autenticità, integrità e riservatezza dei dati o dei servizi forniti; è pertanto legittimo concludere che questa normativa settoriale dell'UE impone obblighi di sicurezza che producono effetti almeno equivalenti ai corrispondenti obblighi dell'articolo 14, paragrafi 1 e 2, della direttiva NIS.

5.2. Direttiva NIS, articolo 1, paragrafo 3 - Prestatori di servizi di telecomunicazione e di servizi fiduciari

A norma dell'articolo 1, paragrafo 3, della direttiva NIS, gli obblighi di sicurezza e di notifica da essa previsti non si applicano ai prestatori che sono soggetti agli obblighi di cui agli articoli 13 bis e 13 ter della direttiva 2002/21/CE. Gli articoli 13 bis e 13 ter della direttiva 2002/21/CE si applicano alle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, le quali devono quindi, nell'ambito di tali prestazioni, rispettare gli obblighi di sicurezza e di notifica stabiliti dalla stessa direttiva 2002/21/CE.

Se l'impresa presta anche altri servizi, quali servizi digitali (ad es., servizi di cloud computing o di mercato online) elencati nell'allegato III della direttiva NIS o servizi quali il DNS o l'IXP in conformità dell'allegato II, punto 7, della stessa direttiva, alla fornitura di questi particolari servizi si applicano tuttavia gli obblighi di sicurezza e di notifica della direttiva NIS. Poiché i prestatori dei servizi elencati nell'allegato II, punto 7, rientrano nella categoria degli operatori di servizi essenziali, gli Stati membri sono tenuti a effettuare nei loro confronti un processo di identificazione ai sensi dell'articolo 5, paragrafo 2, per stabilire concretamente quali prestatori di servizi DNS, IXP o TLD debbano rispettare gli obblighi della direttiva NIS. In esito a questa valutazione, quindi, saranno vincolati agli obblighi della direttiva NIS soltanto i fornitori di servizi di DNS, IXP o TLD che soddisfano i criteri previsti all'articolo 5, paragrafo 2, della stessa direttiva.

L'articolo 1, paragrafo 3, indica che gli obblighi di sicurezza e di notifica della direttiva non si applicano neppure ai prestatori di servizi fiduciari, che l'articolo 19 del regolamento (UE) n. 910/2014 assoggetta ad obblighi analoghi.

6. Documenti di strategia nazionale per la sicurezza cibernetica pubblicati

	Stato membro	Titolo della strategia e collegamenti ipertestuali disponibili
1	Austria	*Austrian Cybersecurity Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgio	*Securing Cyberspace* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgaria	*Cyber Resilient Bulgaria 2020* (2016) http://www.cyberbg.eu/ (BG)
4	Croazia	*The national cyber security strategy of the republic of Croatia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Repubblica ceca	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Cipro	*Cybersecurity Strategy of the Republic of Cyprus* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Danimarca	*The Danish Cyber and Information Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estonia	*Cyber Security Strategy* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Finlandia	*Finland´s Cyber security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Francia	*French national digital security strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Irlanda	*National Cyber Security Strategy 2015-2017* (2015)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Italia	*National Strategic Framework for Cyberspace Security (Quadro strategico nazionale per la sicurezza dello spazio cibernetico)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Germania	*Cyber-security Strategy for Germany* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Ungheria	*National Cyber Security Strategy of Hungary* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Lettonia	*Cyber Security Strategy of Latvia 2014–2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Lituania	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Lussemburgo	*National Cybersecurity Strategy II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*National Cyber Security Strategy Green Paper* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Paesi Bassi	*National Cyber Security Strategy 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Polonia	*Cyberspace Protection Policy of the Republic of Poland* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Romania	*Cybersecurity Strategy of Romania* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portogallo	*National Cyberspace Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-

		strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23	Slovacchia	*Cyber Security Concept of the Slovak Republic for 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slovenia	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Spagna	*National Cyber Security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Svezia	*The Swedish National Cybersecurity Strategy* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Regno Unito	*National Cyber Security Strategy (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Elenco di buone pratiche e raccomandazioni emanate dall'ENISA

Risposta agli incidenti

- ✓ Strategie di risposta agli incidenti e cooperazione nelle crisi cibernetiche[46]

Trattamento degli incidenti

- ✓ Progetto di automazione per il trattamento degli incidenti[47]
- ✓ Guida di buone pratiche per la gestione degli incidenti[48]

Classificazione e tassonomia degli incidenti

- ✓ Panoramica delle tassonomie esistenti[49]
- ✓ Guida alle buone pratiche per l'impiego delle tassonomie nella prevenzione e individuazione degli incidenti[50]

Grado di maturità dei CSIRT

- ✓ Sfide per i CSIRT nazionali in Europa nel 2016 - Studio sul grado di maturità dei CSIRT[51]
- ✓ Studio sul grado di maturità dei CSIRT - Processo di valutazione[52]
- ✓ Orientamenti per i CSIRT nazionali e pubblici sulla valutazione del grado di maturità[53]

Sviluppo delle capacità dei CSIRT e formazione

- ✓ Guida alle buone pratiche sulle metodologie di formazione[54]

Per informazioni sui CSIRT esistenti in Europa - Rassegna dei CSIRT per paese[55]

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). Cfr.https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation.
[47] Per ulteriori informazioni: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation.
[48] ENISA, *Good Practice Guide for Incident Management* (2010). Cfr.https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.
[49] Per ulteriori informazioni: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies.
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Cfr.https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection.
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Cfr.https://www.enisa.europa.eu/publications/study-on-csirt-maturity.
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). Cfr.https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process.
[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Cfr. https://www.enisa.europa.eu/publications/csirt-capabilities.
[54] ENISA, *Good Practice Guide on Training Methodologies* (2014). Cfr.https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies.
[55] Per ulteriori informazioni: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.