EUROPEAN UNION AGENCY
FOR CYBERSECURITY

QUADRO DI VALUTAZIONE DELLE CAPACITÀ A LIVELLO NAZIONALE

DICEMBRE 2020

INFORMAZIONI SULL'ENISA

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento dell'UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza contribuisce alla politica dell'UE in materia di sicurezza informatica, migliora l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche del futuro. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Per maggiori informazioni, visitare il sito www.enisa.europa.eu.

CONTATTI

Per contattare gli autori, inviare un messaggio di posta elettronica a team@enisa.europa.eu.
Per maggiori informazioni sul presente documento, si prega di scrivere a press@enisa.europa.eu.

AUTORI

Anna Sarri, Pinelopi Kyranoudi – Agenzia dell'Unione europea per la cibersicurezza (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique - Wavestone

RINGRAZIAMENTI

L'ENISA desidera ringraziare tutti gli esperti che hanno partecipato e hanno fornito un contributo prezioso a questa relazione e, in particolare, in ordine alfabetico:

Agenzia nazionale per la sicurezza informatica e delle informazioni (Repubblica ceca), Veronika Netolická

Agenzia per le tecnologie dell'informazione di Malta (Malta), Katia Bonello e Martin Camilleri

Amministrazione per la sicurezza delle informazioni (Repubblica di Slovenia), Marjan Kavčič

Autorità nazionale per la sicurezza (Slovacchia)

Centro europeo per la lotta alla criminalità informatica - EC3, Alzofra Martinez Alvaro

Centro europeo per la lotta alla criminalità informatica - EC3, Adrian-Ionut Bobeica

Centro nazionale portoghese per la cibersicurezza (Portogallo), Alexandre Leite e Pedro Matos

Centro per la cibersicurezza (Belgio)

CFCS – Center for Cybersikkerhed (Danimarca), Thomas Wulff

Dipartimento della sicurezza nazionale (Spagna), Maria Mar Lopez Gil

Divisione politica di cibersicurezza, Dipartimento dell'ambiente, del clima e delle comunicazioni (Irlanda), James Caffrey

Governo italiano (Italia)

Ministero degli affari economici e della comunicazione (Estonia), Anna-Liisa Pärnalaas

Ministero della giustizia e della pubblica sicurezza (Norvegia), Robin Bakke

Ministero della politica digitale (Grecia), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali e Sotiris Vasilos

Ministero federale dell'interno (Germania), Sascha-Alexander Lettgen

NCTV, Ministero della giustizia e della sicurezza (Paesi Bassi)
Ufficio centrale statale per lo sviluppo della società digitale (Croazia), Marin Ante Pivcevic
Università di Oxford - Global Cyber Security Capacity Centre, Carolin Weisser Harris

L'ENISA desidera ringraziare per il prezioso contributo a questo studio anche tutti gli esperti che hanno partecipato, ma preferiscono rimanere anonimi.

AVVERTENZA LEGALE

AVVISO SUI DIRITTI D'AUTORE

ISBN: 978-92-9204-482-4

DOI: 10.2824/144346

CATALOGO: TP-02-21-253-IT-N

1. INDICE

GLOSSARIO DEI TERMINI

ACRONIMO	DEFINIZIONE
ARR del SOG-IS	Gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione, accordo sul riconoscimento reciproco
C2M2	Cybersecurity Capability Maturity Model
CCRA	Accordo di riconoscimento dei criteri comuni
CCSMM	Community Cybersecurity Maturity Model
CII	Infrastrutture critiche informatizzate
CMM	Cybersecurity Capacity Maturity Model for Nations
CMMC	Certificazione del Cybersecurity Maturity Model
CPI	Cyber Power Index
CSIRT	Computer Security Incident Response Team
CVD	Divulgazione coordinata delle vulnerabilità
DPA	Data Protection Act (legge sulla protezione dei dati)
DSM	Mercato unico digitale
ECCG	Gruppo europeo per la certificazione della cibersicurezza
ECSM	Mese europeo della cibersicurezza
ECSO	Organizzazione europea per la cibersicurezza
EFTA	Associazione europea di libero scambio
EQF	Quadro europeo delle qualifiche
GCI	Global Cybersecurity Index
GDS	Government Digital Service
IA	Intelligenza artificiale
IA-CM	Modello di capacità di audit interno per il settore pubblico
ISMM	Information Security Maturity Model for NIST Cybersecurity Framework
LEA	Law Enforcement Agency (autorità di contrasto)
NCSS	Strategie nazionali per la cibersicurezza
NIS	Sicurezza delle reti e dell'informazione
NIST	Istituto nazionale per gli standard e la tecnologia
NLO	Funzionari nazionali di collegamento

OES	Operatori di servizi essenziali
OT	Tecnologia delle operazioni
PET	Tecnologie di rafforzamento della tutela della vita privata
PIMS	Sistema di gestione delle informazioni sulla privacy
PMI	Piccole e medie imprese
PPP	Partenariati pubblico-privato
Q-C2M2	Qatar Cybersecurity Capability Maturity Model
R&S	Ricerca e sviluppo
RGPD	Regolamento generale sulla protezione dei dati
SM	Stato membro
TIC	Tecnologie dell'informazione e della comunicazione
UE	Unione europea
UIT	Unione internazionale delle telecomunicazioni

SINTESI

Di fronte alla continua espansione del panorama delle minacce informatiche e al costante aumento dell'intensità e del numero degli attacchi informatici, gli Stati membri dell'UE devono reagire in modo efficace sviluppando e adattando ulteriormente le loro strategie nazionali in materia di cibersicurezza (NCSS). Dalla pubblicazione dei primi studi sulle NCSS a cura dell'ENISA nel 2012, gli Stati membri dell'UE e i paesi dell'EFTA hanno compiuto grandi progressi nello sviluppo e nell'attuazione delle rispettive strategie.

La presente relazione illustra il lavoro svolto dall'ENISA per la costruzione di un quadro di valutazione delle capacità a livello nazionale (NCAF).

Il quadro mira a fornire agli Stati membri un'autovalutazione del livello di maturità attraverso un esame dei loro obiettivi di NCSS, che li aiuterà a migliorare e a costruire capacità di cibersicurezza a livello sia strategico sia operativo.

Delinea una visione rappresentativa semplice del livello di maturità raggiunto dallo Stato membro nella cibersicurezza. Il quadro NCAF è uno strumento in grado di aiutare gli Stati membri a:

- fornire informazioni utili a sviluppare una strategia a lungo termine (ad es. buone pratiche, linee guida);
- contribuire a individuare gli elementi mancanti all'interno delle NCSS;
- contribuire all'ulteriore sviluppo di capacità di cibersicurezza;
- sostenere la responsabilità delle azioni politiche;
- aumentare la credibilità nei confronti del pubblico in generale e dei partner internazionali;
- sostenere la sensibilizzazione e rafforzare l'immagine pubblica di organizzazione trasparente;
- contribuire a prevedere i problemi del prossimo futuro;
- aiutare a individuare le lezioni apprese e le migliori pratiche;
- fornire una linea di riferimento sulla capacità di cibersicurezza a livello dell'UE per agevolare le discussioni;
- aiutare a valutare le capacità nazionali in materia di cibersicurezza.

Questo quadro è stato elaborato con il sostegno degli esperti del settore dell'ENISA e dei rappresentanti di 19 Stati membri e di paesi dell'EFTA ([1]). Destinatari di questa relazione sono i decisori politici, gli esperti e i funzionari governativi responsabili della progettazione,

([1]) Sono stati intervistati rappresentanti dei seguenti Stati membri e dei paesi dell'EFTA: Belgio, Croazia, Danimarca, Estonia, Germania, Grecia, Irlanda, Italia, Liechtenstein, Malta, Norvegia, Paesi Bassi, Portogallo, Repubblica ceca, Slovacchia, Slovenia, Spagna, Svezia, Ungheria.

dell'attuazione e della valutazione di una NCSS e, a livello più ampio, delle capacità di cibersicurezza, o coinvolti in tali attività.

Il quadro di valutazione delle capacità a livello nazionale tratta 17 obiettivi strategici ed è strutturato intorno a quattro poli tematici principali:

- Polo tematico n. 1: Governance e standard di cibersicurezza
  1. Elaborare un piano di emergenza informatica nazionale
  2. Stabilire misure di sicurezza di riferimento
  3. Proteggere l'identità digitale e generare fiducia nei servizi pubblici digitali

- Polo tematico n. 2: Sviluppo della capacità e sensibilizzazione
  4. Organizzare esercitazioni di cibersicurezza
  5. Istituire una capacità di risposta agli incidenti
  6. Sensibilizzare gli utenti
  7. Rafforzare i programmi formativi ed educativi
  8. Promuovere ricerca e sviluppo
  9. Fornire incentivi al settore privato per gli investimenti in misure di sicurezza
  10. Migliorare la cibersicurezza della catena di fornitura

- Polo tematico n. 3: Aspetti giuridici e normativi
  11. Proteggere infrastrutture critiche informatizzate, operatori di servizi essenziali (OES) e fornitori di servizi digitali (DSP)
  12. Affrontare la criminalità informatica
  13. Istituire meccanismi di segnalazione degli incidenti
  14. Rafforzare la privacy e la protezione dei dati

- Polo tematico n. 4: Cooperazione
  15. Istituire un partenariato pubblico-privato
  16. Istituzionalizzare la cooperazione tra agenzie pubbliche
  17. Impegnarsi nella cooperazione internazionale

1. INTRODUZIONE

La direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS), pubblicata nel luglio 2016, prevede che gli Stati membri dell'UE adottino una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi, denominata anche NCSS (*National Cyber Security Strategy*, strategia nazionale di cibersicurezza), come stabilito negli articoli 1 e 7. In questo contesto, una NCSS è definita come un quadro di riferimento che fissa principi strategici, linee guida, obiettivi strategici, priorità, politiche adeguate e misure di regolamentazione. L'obiettivo previsto di una NCSS è conseguire e mantenere un livello elevato di sicurezza della rete e dei sistemi, consentendo così agli Stati membri di attenuare le potenziali minacce. Essa può essere anche un catalizzatore per lo sviluppo industriale e il progresso economico e sociale.

Il regolamento UE sulla cibersicurezza stabilisce che l'ENISA debba promuovere la diffusione delle migliori pratiche nella definizione e nell'attuazione di una NCSS, sostenendo gli Stati membri nell'adozione della direttiva NIS e raccogliendo preziosi riscontri sulle loro esperienze. A tale scopo, l'ENISA ha messo a punto diversi strumenti per assistere gli Stati membri nello sviluppo, nell'attuazione e nella valutazione delle loro strategie nazionali per la cibersicurezza (NCSS).

Nell'ambito del suo mandato, l'ENISA intende sviluppare un quadro di autovalutazione delle capacità a livello nazionale per misurare il livello di maturità delle diverse NCSS. L'obiettivo della presente relazione è presentare lo studio condotto nella definizione del quadro di autovalutazione.

1.1 AMBITO E OBIETTIVI DELLO STUDIO

L'obiettivo principale del presente studio è creare un quadro di autovalutazione delle capacità a livello nazionale (in appresso NCAF) per misurare il livello di maturità delle capacità di cibersicurezza degli Stati membri. Nello specifico, il quadro dovrebbe sostenere gli Stati membri nelle seguenti attività:

- conduzione della valutazione delle rispettive capacità nazionali di cibersicurezza;
- miglioramento della consapevolezza del livello di maturità del paese;
- individuazione delle aree di miglioramento;
- creazione delle capacità di cibersicurezza.

Tale quadro dovrebbe aiutare gli Stati membri, e in particolare i decisori politici nazionali, a effettuare un esercizio di autovalutazione finalizzato migliorare le capacità nazionali di cibersicurezza.

1.2 APPROCCIO METODOLOGICO

L'approccio metodologico utilizzato per elaborare il quadro di autovalutazione delle capacità a livello nazionale si basa su quattro fasi principali.

1. **Ricerca a tavolino**: il primo passo ha previsto la conduzione di un'ampia revisione della letteratura per raccogliere le migliori pratiche relative allo sviluppo di un quadro di valutazione del grado di maturità delle strategie nazionali per la cibersicurezza. La ricerca a tavolino è incentrata su un'analisi sistematica dei documenti pertinenti in tema di creazione di capacità di cibersicurezza e di definizione delle strategie, sulle NCSS esistenti degli Stati membri e su un confronto dei modelli di maturità esistenti in materia di sicurezza informatica. Un esercizio di valutazione comparata sui modelli di

maturità esistenti è stato effettuato mediante l'adozione di un quadro di analisi sviluppato ai fini del presente studio. Il quadro di analisi si basa sulla metodologia di Becker ([2]) per lo sviluppo di modelli di maturità, che definisce un modello di procedura generico e consolidato per la progettazione di modelli di maturità e fornisce chiari requisiti per il loro sviluppo. Il quadro di analisi è stato ulteriormente personalizzato per soddisfare le esigenze di questo studio.

2. **Raccolta del punto di vista degli esperti e dei portatori di interessi**: sulla base dei dati raccolti attraverso la ricerca a tavolino e dei risultati preliminari dell'analisi, questa fase ha previsto l'individuazione e l'invito di esperti, competenti nello sviluppo e nell'attuazione di una NCSS o di modelli di maturità, da intervistare. L'ENISA ha contattato il proprio gruppo di esperti sulle strategie nazionali per la cibersicurezza e i funzionari nazionali di collegamento (NLO) per trovare gli esperti pertinenti in ogni Stato membro. Sono stati intervistati inoltre alcuni esperti coinvolti nello sviluppo dei modelli di maturità. Nel complesso sono state condotte 22 interviste, 19 delle quali con rappresentanti di agenzie per la cibersicurezza di diversi Stati membri (e paesi dell'EFTA).
3. **Analisi del contributo alla valutazione:** i dati raccolti attraverso la ricerca a tavolino e le interviste sono stati poi analizzati per identificare le migliori pratiche nella progettazione di un quadro di autovalutazione volto a misurare il livello di maturità delle NCSS, per comprendere le esigenze degli Stati membri e per determinare quali dati sia possibile raccogliere nei diversi paesi europei ([3]). L'analisi ha permesso di mettere a punto il modello preliminare elaborato nelle fasi precedenti e di perfezionare l'insieme di indicatori inclusi nel modello, i livelli di maturità e le sue dimensioni.
4. **Finalizzazione del modello:** successivamente, una versione aggiornata del quadro di autovalutazione delle capacità a livello nazionale è stata esaminata dagli esperti in materia dell'ENISA e poi ulteriormente convalidata da esperti nel contesto di un workshop tenutosi nell'ottobre 2020, prima della pubblicazione.

1.3 DESTINATARI

Destinatari di questa relazione sono i decisori politici, gli esperti e i funzionari governativi responsabili della progettazione, dell'attuazione e della valutazione della NCSS e, a livello più ampio, delle capacità di cibersicurezza, o coinvolti in tali attività. Inoltre, i risultati formalizzati in questo documento possono essere utili agli esperti in materia di politica di cibersicurezza e ai ricercatori a livello nazionale o europeo.

([2]) J. Becker, R. Knackstedt, e J. Pöppelbuß, «Developing Maturity Models for IT Management: A Procedure Model and its Application», Business & Information Systems Engineering, vol. 1, n. 3, pp. 213–222, giugno 2009.
([3]) Ai fini della presente ricerca, i «paesi europei» citati nella relazione sono i 27 Stati membri dell'UE.

2. CONTESTO

2.1 PRECEDENTI LAVORI SUL CICLO DI VITA DELLA NCSS

Come indicato nel regolamento UE sulla cibersicurezza, uno degli obiettivi principali dell'ENISA è assistere gli Stati membri nello sviluppo delle strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi, promuovere la diffusione di tali strategie e monitorarne l'attuazione. Nell'ambito del suo mandato, l'ENISA ha prodotto diversi documenti su questo tema al fine di promuovere la condivisione delle buone pratiche e sostenere l'attuazione delle NCSS in tutta l'UE:

- «Practical guide on the development and execution phase of NCSS» ([4]), pubblicata nel 2012
- «Setting the course for national efforts to strengthen security in cyberspace» ([5]), pubblicato nel 2012
- Il primo quadro dell'ENISA per la valutazione della NCSS di uno Stato membro, pubblicato ([6]) nel 2014.
- «Online NCSS Interactive Map» ([7]), pubblicata nel 2014.
- «NCSS Good Practice Guide» ([8]) pubblicata nel 2016.
- «National Cybersecurity Strategies Evaluation Tool» ([9]), pubblicato nel 2018.
- «Good practices in innovation on Cybersecurity under the NCSS» ([10]), pubblicate nel 2019.

L'ALLEGATO A fornisce un breve riepilogo delle principali pubblicazioni dell'ENISA sull'argomento.

Le guide e i documenti sopra citati sono stati studiati nell'ambito della ricerca a tavolino. In particolare, il «National Cybersecurity Strategies Evaluation Tool» ([11]) è un elemento fondamentale dell'NCAF, che si basa sugli obiettivi trattati nello strumento online di valutazione della NCSS.

([4]) NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
([5]) NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
([6]) An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
([7]) National Cybersecurity Strategies - Interactive Map (ENISA, 2014, aggiornata nel 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
([8]) Si tratta dell'aggiornamento della guida del 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
([9]) National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
([10]) https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
([11]) National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

2.2 OBIETTIVI COMUNI INDIVIDUATI ALL'INTERNO DELLA NCSS EUROPEA

Data la disparità tra gli Stati membri è difficile individuare attività o piani d'azione comuni tra i diversi contesti, quadri giuridici e agende politiche nazionali. Tuttavia, le NCSS degli Stati membri hanno spesso obiettivi strategici che riguardano gli stessi temi. Pertanto, sulla base dei precedenti lavori dell'ENISA e dell'analisi delle NCSS degli Stati membri, sono stati identificati 22 obiettivi strategici, di cui 15 erano già stati individuati nei lavori precedenti dell'ENISA, 2 sono stati aggiunti in questo studio e 5 sono stati identificati per considerazioni future.

2.2.1 Obiettivi strategici comuni trattati dagli Stati membri

Sulla base del precedente lavoro dell'ENISA, ovvero lo strumento di valutazione delle strategie nazionali per la cibersicurezza ([12]), la seguente tabella riporta la succitata serie di 15 obiettivi strategici comunemente trattati nelle NCSS degli Stati membri. Gli obiettivi delineano l'essenza della «filosofia nazionale» generale sull'argomento. Per maggiori informazioni sugli obiettivi descritti di seguito, si rimanda alla relazione dell'ENISA «NCSS Good Practice Guide» ([13]).

Tabella 1. Obiettivi strategici comuni trattati dagli Stati membri nella rispettiva NCSS

N. rif.	Obiettivi strategici della NCSS	Obiettivi
1	**Elaborare piani di emergenza informatica nazionali**	▶ Presentare e spiegare i criteri da utilizzare per definire una situazione come crisi ▶ Definire i processi e le azioni chiave per gestire la crisi ▶ Delineare chiaramente i ruoli e le responsabilità dei diversi portatori di interessi durante una crisi cibernetica ▶ Presentare e spiegare i criteri per dichiarare il superamento di una crisi e/o chi ha l'autorità di dichiararlo
2	**Stabilire misure di sicurezza di riferimento**	▶ Armonizzare le diverse pratiche seguite dalle organizzazioni sia nel settore pubblico sia in quello privato ▶ Creare un linguaggio comune tra le autorità pubbliche competenti e le organizzazioni e aprire canali di comunicazione sicuri ▶ Consentire ai vari portatori di interessi di verificare e valutare in un'ottica di confronto le rispettive capacità di cibersicurezza ▶ Condividere informazioni sulle buone pratiche di cibersicurezza in ogni settore industriale ▶ Aiutare i portatori di interessi a definire le priorità dei loro investimenti in tema di sicurezza.
3	**Organizzare esercitazioni di cibersicurezza**	▶ Individuare gli elementi che devono essere testati (piani e processi, persone, infrastrutture, capacità di risposta, capacità di cooperazione, comunicazione, ecc.); ▶ Costituire un team nazionale per la pianificazione delle esercitazioni di cibersicurezza, con un chiaro mandato ▶ Integrare le esercitazioni di cibersicurezza nel ciclo di vita della strategia nazionale di cibersicurezza o del piano di emergenza informatica nazionale.
4	**Istituire una capacità di risposta agli incidenti**	▶ Mandato: si riferisce ai poteri, ai ruoli e alle responsabilità che devono essere assegnati al team dal rispettivo governo ▶ Portafoglio dei servizi: riguarda i servizi che un team fornisce alla sua comunità di riferimento o che utilizza per il proprio funzionamento interno

([12]) National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
([13]) Si tratta dell'aggiornamento della guida del 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

N. rif.	Obiettivi strategici della NCSS	Obiettivi
		▶ Capacità operative: si riferiscono ai requisiti tecnici e operativi che un team deve soddisfare ▶ Capacità di cooperazione: comprendono i requisiti relativi alla condivisione di informazioni con altri team non contemplati dalle tre categorie precedenti, ad esempio i decisori politici, le forze armate, le autorità di regolamentazione, gli operatori (infrastrutture critiche informatizzate), le autorità di contrasto
5	Sensibilizzare gli utenti	▶ Individuare le lacune nelle conoscenze riguardo a tematiche di cibersicurezza e sicurezza delle informazioni ▶ Colmare le lacune attraverso la sensibilizzazione o lo sviluppo e il rafforzamento delle basi della conoscenza
6	Rafforzare i programmi formativi ed educativi	▶ Potenziare le capacità operative del personale esistente nel campo della sicurezza delle informazioni ▶ Incoraggiare gli studenti a partecipare e prepararli ad entrare nel campo della cibersicurezza ▶ Promuovere e incoraggiare i rapporti tra gli ambienti accademici e l'industria nel campo della sicurezza delle informazioni ▶ Allineare la formazione sulla cibersicurezza alle esigenze delle imprese.
7	Promuovere ricerca e sviluppo	▶ Individuare le cause reali delle vulnerabilità anziché rimediare al loro impatto ▶ Riunire scienziati di diverse discipline per fornire soluzioni a problemi complessi e multidimensionali, come le minacce ciberfisiche ▶ Raccogliere le esigenze dell'industria e i risultati della ricerca, agevolando così il passaggio dalla teoria alla pratica ▶ Trovare modi non solo per mantenere, ma anche per aumentare il livello di cibersicurezza dei prodotti e dei servizi che sostengono le infrastrutture informatiche esistenti
8	Fornire incentivi al settore privato per gli investimenti in misure di sicurezza	▶ Individuare possibili incentivi affinché le imprese private investano in misure di sicurezza ▶ Fornire alle aziende incentivi per favorire gli investimenti nella sicurezza.
9	Proteggere infrastrutture critiche informatizzate (CII), OES e DSP	▶ Individuare le infrastrutture critiche informatizzate ▶ Identificare e mitigare i rischi pertinenti per le infrastrutture critiche informatizzate.
10	Affrontare la criminalità informatica	▶ Creare normative nel campo della criminalità informatica ▶ Aumentare l'efficacia delle autorità di contrasto.
11	Istituire meccanismi di segnalazione degli incidenti	▶ Acquisire conoscenze sull'ambiente generale delle minacce ▶ Valutare l'impatto degli incidenti (ad es. violazioni della sicurezza, guasti della rete, interruzioni del servizio) ▶ Acquisire conoscenze sulle vulnerabilità nuove ed esistenti e sui tipi di attacchi ▶ Aggiornare le misure di sicurezza di conseguenza ▶ Attuare le disposizioni della direttiva NIS sulla segnalazione degli incidenti
12	Rafforzare la privacy e la protezione dei dati	▶ Contribuire a rafforzare i diritti fondamentali in materia di privacy e protezione dei dati
13	Istituire un partenariato pubblico-privato (PPP)	▶ Dissuadere (costituire un deterrente per gli aggressori) ▶ Proteggere (utilizzare la ricerca sulle nuove minacce alla sicurezza) ▶ Rilevare (utilizzare la condivisione delle informazioni per affrontare le nuove minacce) ▶ Rispondere (fornire la capacità per fronte all'impatto iniziale di un incidente) ▶ Recuperare (fornire la capacità di riparare l'impatto finale di un incidente)
14	Istituzionalizzare la cooperazione tra agenzie pubbliche	▶ Aumentare la cooperazione tra le agenzie pubbliche con responsabilità e competenze legate alla cibersicurezza

N. rif.	Obiettivi strategici della NCSS	Obiettivi
		▶ Evitare una sovrapposizione di competenze e di risorse tra le agenzie pubbliche ▶ Migliorare e istituzionalizzare la cooperazione tra agenzie pubbliche in diverse aree della cibersicurezza
15	**Impegnarsi nella cooperazione internazionale (non solo con gli Stati membri dell'UE)**	▶ Beneficiare della creazione di una base di conoscenza comune tra gli Stati membri dell'UE ▶ Creare effetti sinergici tra le autorità nazionali che si occupano di cibersicurezza ▶ Consentire e incrementare la lotta contro la criminalità transnazionale

2.2.2 Obiettivi strategici supplementari

Sulla base della ricerca a tavolino effettuata e delle interviste condotte dall'ENISA sono stati individuati obiettivi strategici supplementari. Gli Stati membri si occupano sempre più spesso di questi temi nella loro NCSS o definiscono piani d'azione sullo stesso argomento. Vengono forniti anche esempi di attività svolte dagli Stati membri. Se un esempio proviene da una fonte pubblica, viene fornito un riferimento, mentre nei casi in cui gli esempi si basano su interviste riservate con funzionari degli Stati membri dell'UE, non vengono forniti riferimenti.

Sono stati individuati i seguenti obiettivi strategici supplementari:

- migliorare la cibersicurezza della catena di fornitura e
- proteggere l'identità digitale e generare fiducia nei servizi pubblici digitali.

Migliorare la cibersicurezza della catena di fornitura

Le piccole e medie imprese (PMI) costituiscono la spina dorsale dell'economia europea. Rappresentano infatti il 99 % di tutte le imprese dell'Unione ([14]) e si stima che nel 2015 le PMI abbiano creato circa l'85 % dei nuovi posti di lavoro e fornito due terzi dell'occupazione totale del settore privato nell'UE. Inoltre, dal momento che forniscono servizi alle grandi imprese e lavorano sempre più spesso con le amministrazioni pubbliche ([15]), occorre notare che nell'attuale contesto interconnesso le PMI costituiscono l'anello debole per gli attacchi informatici. Sono in effetti le più esposte agli attacchi, eppure spesso non possono permettersi investimenti adeguati nella sicurezza informatica ([16]). Il miglioramento della cibersicurezza della catena di fornitura dovrebbe perciò essere perseguito con una particolare attenzione alle PMI.

Oltre a questo approccio sistemico, gli Stati membri possono anche mettere in rilievo gli sforzi sulla cibersicurezza di specifici servizi e i prodotti TIC considerati essenziali: tecnologie TIC utilizzate nelle infrastrutture critiche informatizzate, meccanismi di sicurezza applicati nel settore delle telecomunicazioni (controlli a livello di ISP, ecc.), servizi fiduciari come da definizione nel regolamento eIDAS e fornitori di servizi cloud. Ad esempio, nella sua strategia nazionale di cibersicurezza per il periodo 2019-2024 ([17]), la Polonia si è impegnata a sviluppare un sistema di valutazione e certificazione della sicurezza dello spazio cibernetico nazionale come meccanismo di garanzia della qualità nella catena di fornitura. Questo sistema di certificazione

([14]) https://ec.europa.eu/growth/smes/
([15]) https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
([16]) https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
([17]) http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

sarà allineato al quadro di certificazione dell'UE per i prodotti, i servizi e i processi digitali TIC, stabilito dal regolamento UE 2019/881 sulla cibersicurezza.

Migliorare la cibersicurezza della catena di fornitura è quindi di capitale importanza. Tale obiettivo può essere realizzato, tra l'altro, stabilendo politiche forti per la promozione delle PMI, fornendo linee guida per i requisiti di cibersicurezza nelle procedure di gara nella pubblica amministrazione, favorendo la cooperazione all'interno del settore privato, costruendo PPP, promuovendo meccanismi di divulgazione coordinata delle vulnerabilità (CVD) ([18]), creando un sistema di certificazione dei prodotti, comprendendo componenti di cibersicurezza nelle iniziative digitali per le PMI e finanziando lo sviluppo delle competenze.

Proteggere l'identità digitale e generare fiducia nei servizi pubblici digitali

Nel febbraio 2020, la Commissione ha delineato la sua visione della trasformazione digitale dell'UE nella comunicazione «Plasmare il futuro digitale dell'Europa» ([19]), con l'obiettivo di fornire tecnologie inclusive al servizio delle persone e nel rispetto dei valori fondamentali dell'UE. La comunicazione afferma, in particolare, che è essenziale promuovere la trasformazione digitale delle pubbliche amministrazioni in tutta Europa. A tal fine, è di fondamentale importanza creare fiducia nei servizi pubblici e nelle amministrazioni per quanto riguarda l'identità digitale. Ciò è ancora più cruciale considerando che le operazioni e gli scambi di dati nel settore pubblico sono spesso di natura sensibile.

Molti paesi hanno espresso l'intenzione di trattare questo argomento nelle loro NCSS, tra questi: Danimarca, Estonia, Francia, Lussemburgo, Malta, Paesi Bassi, Regno Unito e Spagna. Tra questi paesi, alcuni hanno anche indicato la possibilità di affrontare tale obiettivo strategico nell'ambito di un piano più ampio:

- L'Estonia collega il suo piano d'azione associato in tema di «sicurezza della capacità di identificazione e autenticazione elettronica» alla più ampia Agenda digitale 2020 per l'Estonia.
- La NCSS della Francia stabilisce che il Segretario di Stato responsabile della tecnologia digitale sovrintende alla definizione di una tabella di marcia «per proteggere la vita digitale, la privacy e i dati personali del popolo francese».
- La NCSS dei Paesi Bassi afferma che la cibersicurezza nelle pubbliche amministrazioni, così come i servizi pubblici forniti ai cittadini e alle imprese, sono trattati in modo più dettagliato nell'Ampio programma per il governo digitale.
- Poiché il governo del Regno Unito continua a spostare sempre più servizi online, ha affidato al *Government Digital Service* (GDS) il compito di garantire che tutti i nuovi servizi digitali creati o acquisiti dal governo siano anche «sicuri per impostazione predefinita», con l'appoggio del centro nazionale per la cibersicurezza (*National Cybersecurity Centre*, NCSC) britannico.

2.2.3 Altri obiettivi strategici considerati

Durante la fase di ricerca a tavolino e nell'ambito delle interviste condotte dall'ENISA sono stati studiati altri obiettivi strategici. Si è deciso tuttavia che tali obiettivi non avrebbero fatto parte del quadro di autovalutazione. L'ALLEGATO C - Altri obiettivi studiati

fornisce le definizioni di ciascun obiettivo, che possono fungere da base per promuovere discussioni future su eventuali miglioramenti della NCSS.

([18]) https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
([19]) Plasmare il futuro digitale dell'Europa, COM(2020) 67 final: https://ec.europa.eu/transparency/regdoc/rep/1/2020/IT/COM-2020-67-F1-IT-MAIN-PART-1.PDF

I seguenti obiettivi strategici sono stati esaminati per considerazione futura.

- Sviluppare strategie di cibersicurezza specifiche per i settori
- Lottare contro le campagne di disinformazione
- Proteggere le tecnologie di punta (5G, IA, informatica quantistica, ecc.)
- Garantire la sovranità dei dati
- Fornire incentivi per lo sviluppo del settore delle assicurazioni informatiche

2.3 INSEGNAMENTI ESSENZIALI TRATTI DALL'ESERCIZIO DI VALUTAZIONE COMPARATA

Lo scopo della ricerca a tavolino sui modelli di maturità esistenti relativi alla cibersicurezza era di raccogliere informazioni e prove a sostegno della progettazione del quadro di autovalutazione delle capacità a livello nazionale nell'area della NCSS. In questo contesto è stata condotta un'ampia revisione della letteratura inerente ai modelli esistenti, a integrazione dei risultati della ricerca esplorativa iniziale sui modelli di maturità della cibersicurezza e sulle NCSS esistenti, illustrata nelle sezioni 2.1 e 2.2. Questa revisione sistematica corrobora la selezione e la giustificazione dei livelli di maturità del quadro di valutazione e la definizione delle diverse dimensioni e dei diversi indicatori.

Nell'ambito della revisione sistematica dei modelli di maturità sono stati considerati e analizzati 10 modelli, sulla base delle loro caratteristiche principali. La panoramica globale delle caratteristiche principali di ogni modello esaminato nell'ambito di questo studio è riportata nella Tabella 2. Panoramica dei modelli di maturità analizzati, mentre per un'analisi dettagliata si rimanda all'ALLEGATO A.

Tabella 2. Panoramica dei modelli di maturità analizzati

Nome del modello	N. di livelli di maturità	N. di attributi	Metodo di valutazione	Rappresentazione dei risultati
Cybersecurity Capacity Maturity Model for Nations (CMM)	5	5 dimensioni principali	Collaborazione con un'organizzazione locale per mettere a punto il modello prima di applicarlo al contesto nazionale	Grafico radar a 5 sezioni
Cybersecurity Capability Maturity Model (C2M2)	4	10 domini principali	Metodologia e kit di strumenti di autovalutazione	Scheda di valutazione bilanciata con grafici a torta
Framework for Improving Critical Infrastructure Cybersecurity	n.d. (4 livelli)	5 funzioni essenziali	Autovalutazione	n.d.
Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	5	5 domini principali	n.d.	n.d.
Cybersecurity Maturity Model Certification (CMMC)	5	17 domini principali	Valutazione da parte di revisori terzi	n.d.
Community Cybersecurity Maturity Model (CCSMM)	5	6 dimensioni principali	Valutazione all'interno delle comunità con il contributo delle agenzie di contrasto statali e federali	n.d.
Information Security Maturity Model for NIST Cybersecurity Framework (ISMM)	5	23 aree valutate	n.d.	n.d.

Internal Audit Capability Model (IA-CM) per il settore pubblico	5	6 elementi	Autovalutazione	n.d.
Global Cybersecurity Index (GCI)	n.d.	5 pilastri	Autovalutazione	Graduatoria
Cyber Power Index (CPI)	n.d.	4 categorie	Analisi comparativa a cura dell'Economist Intelligence Unit	Graduatoria

Questa revisione sistematica ha permesso di trarre conclusioni sulle migliori pratiche adottate nei modelli esistenti, al fine di sostenere lo sviluppo del modello concettuale per il modello di maturità attuale. In particolare, l'esercizio di analisi comparativa ha corroborato la definizione dei livelli di maturità, la creazione di poli tematici dimensionali e la selezione degli indicatori, nonché una metodologia di visualizzazione adeguata dei risultati del modello. I risultati più pertinenti per ciascuno di questi elementi sono riportati in dettaglio nella Tabella 3

Tabella 3. Insegnamenti essenziali tratti dall'esercizio di valutazione comparata

Caratteristica	Insegnamento chiave
Livelli di maturità	▶ Una scala di maturità a cinque livelli per i quadri di valutazione delle capacità di cibersicurezza è comunemente accettata e in grado di fornire risultati di valutazione granulari (vedere la Tabella 6. Confronto dei livelli di maturità per una visione esaustiva della definizione dei livelli di maturità per ciascun modello). ▶ Tutti i modelli forniscono una definizione generale di ogni livello di maturità, che viene poi adattata alle diverse dimensioni o ai diversi poli tematici dimensionali. ▶ Nel misurare la maturità delle capacità di cibersicurezza vengono generalmente valutati due aspetti principali: la maturità delle strategie e la maturità dei processi per attuarle.
Attributi	▶ L'analisi comparativa degli attributi dei modelli di maturità esistenti mostra risultati eterogenei, con un numero medio di attributi per modello compreso tra quattro e cinque. ▶ Un modello basato su circa quattro o cinque attributi fornisce ai paesi il giusto livello di granularità dei dati, raggruppando tra loro le dimensioni pertinenti e garantendo la leggibilità dei risultati (vedere la Tabella 7. Confronto degli attributi o delle **dimensioni** per una descrizione degli attributi di ciascun modello). ▶ Il principio chiave adottato da tutti i modelli nella definizione dei poli tematici si basa sulla coerenza degli elementi raggruppati all'interno di ciascun cluster.
Metodo di valutazione	▶ I metodi di valutazione utilizzati nei diversi modelli analizzati variano tra loro. ▶ Il metodo più comune è basato sull'autovalutazione.
Rappresentazione dei risultati	▶ È importante presentare i risultati a diversi livelli di granularità. ▶ La metodologia di visualizzazione deve essere autoesplicativa e di facile lettura.

Il modello concettuale è stato creato sulla base dell'esercizio di analisi comparativa dei diversi modelli di maturità e sulla base dei precedenti lavori dell'ENISA. Si è deciso inoltre di avvalersi dello *strumento interattivo online dell'ENISA* per elaborare gli indicatori di maturità utilizzati per ciascun attributo.

2.4 SFIDE DELLA VALUTAZIONE DELLA NCSS

Gli Stati membri si trovano ad affrontare molte sfide nella creazione delle capacità di cibersicurezza e, nello specifico, nell'assicurare che tali capacità siano al passo con gli ultimi sviluppi. Di seguito è riportata una sintesi delle sfide individuate dagli Stati membri e discusse con essi nell'ambito di questo studio.

- **Difficoltà di coordinamento e cooperazione:** coordinare gli sforzi a livello nazionale per disporre di una risposta efficiente ai problemi di cibersicurezza può rivelarsi una sfida a causa dell'elevato numero di portatori di interessi coinvolti.
- **Mancanza di risorse per eseguire la valutazione:** a seconda del contesto locale e della struttura nazionale di governance della cibersicurezza informatica, valutare la NCSS e i suoi obiettivi può richiedere anche più di 15 persone/giorni.
- **Mancanza di sostegno per lo sviluppo di capacità di cibersicurezza:** alcuni Stati membri hanno dichiarato che, per difendere un bilancio e ottenere sostegno per lo sviluppo di capacità di cibersicurezza, devono prima percorrere una fase di valutazione per identificare lacune e limiti.
- **Difficoltà nell'attribuzione di successi o cambiamenti alla strategia:** a fronte dell'evoluzione quotidiana delle minacce e del miglioramento della tecnologia è necessario adattare costantemente i piani d'azione in risposta. Tuttavia, la valutazione di una NCSS e l'attribuzione dei cambiamenti alla strategia stessa si confermano un compito arduo. Ciò a sua volta rende difficile identificare i limiti e i difetti della NCSS.
- **Difficoltà di misurare l'efficacia della NCSS:** è possibile raccogliere metriche per misurare diverse aree, quali il progresso, l'attuazione, la maturità e l'efficacia. Se da un lato misurare i progressi e l'attuazione è relativamente facile rispetto alla misurazione dell'efficacia, dall'altro quest'ultima rimane più significativa per valutare gli esiti e gli impatti di una NCSS. Sulla base delle interviste condotte dall'ENISA, un ampio numero di Stati membri ha confermato l'importanza di misurare quantitativamente l'efficacia di una NCSS, sottolineando altresì che si tratta di un compito molto impegnativo, se non impossibile in alcuni casi.
- **Difficoltà di adottare un quadro comune:** gli Stati membri dell'UE operano in contesti diversi in termini di politica, organizzazione, cultura, struttura della società e maturità della NCSS. Alcuni degli Stati membri intervistati nell'ambito di questo studio hanno affermato che potrebbe rivelarsi difficile difendere e utilizzare un quadro di autovalutazione «unico».

2.5 VANTAGGI DI UNA VALUTAZIONE DELLE CAPACITÀ A LIVELLO NAZIONALE

Dal 2017 tutti gli Stati membri dell'UE dispongono di una NCSS ([20]). Pur trattandosi di uno sviluppo positivo, è altresì importante che gli Stati membri siano in grado di valutare adeguatamente queste NCSS, apportando così un valore aggiunto alle relative pianificazione e attuazione strategiche.

Uno degli obiettivi del quadro di valutazione delle capacità a livello nazionale è esaminare le capacità di cibersicurezza sulla base delle priorità stabilite nelle varie NCSS. Fondamentalmente, il quadro valuta il livello di maturità delle capacità di sicurezza informatica degli Stati membri nei campi definiti dagli obiettivi della NCSS. I risultati del quadro assistono perciò i responsabili delle politiche degli Stati membri nella definizione della strategia nazionale in materia di cibersicurezza, fornendo loro informazioni sulla situazione a livello nazionale ([21]).

([20]) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
([21]) Weiss, C.H. (1999), The interface between evaluation and public policy, Evaluation, 5(4), 468-486.

L'NCAF è sostanzialmente destinato ad aiutare gli Stati membri a individuare le aree di miglioramento e a rafforzare le capacità.

Il quadro mira a fornire agli Stati membri un'autovalutazione del livello di maturità attraverso un esame dei loro obiettivi di NCSS che li aiuterà a migliorare e costruire capacità di sicurezza informatica a livello sia strategico sia operativo.

Con un approccio più pratico, basato sulle interviste condotte dall'ENISA con diverse agenzie responsabili del settore della cibersicurezza in diversi Stati membri, sono stati identificati e messi in rilievo i seguenti vantaggi del quadro di valutazione delle capacità a livello nazionale:

- fornire informazioni utili a sviluppare una strategia a lungo termine (ad es. buone pratiche, linee guida);
- contribuire a individuare gli elementi mancanti all'interno delle NCSS;
- contribuire all'ulteriore sviluppo di capacità di cibersicurezza;
- sostenere la responsabilità delle azioni politiche;
- aumentare la credibilità nei confronti del pubblico in generale e dei partner internazionali;
- sostenere la sensibilizzazione e rafforzare l'immagine pubblica di organizzazione trasparente;
- contribuire a prevedere i problemi del prossimo futuro;
- aiutare a individuare le lezioni apprese e le migliori pratiche;
- fornire una linea di riferimento sulla capacità di cibersicurezza a livello dell'UE per agevolare le discussioni;
- aiutare a valutare le capacità nazionali in materia di cibersicurezza.

3. METODOLOGIA DEL QUADRO DI VALUTAZIONE DELLE CAPACITÀ A LIVELLO NAZIONALE

3.1 FINALITÀ GENERALE

L'**obiettivo principale** dell'NCAF è misurare il livello di maturità delle capacità di cibersicurezza degli **Stati membri** allo scopo di sostenerli nella conduzione della valutazione di tali capacità a livello nazionale, aumentando la consapevolezza del livello di maturità raggiunto dal paese, individuando le aree di miglioramento e rafforzando le capacità di sicurezza informatica.

3.2 LIVELLI DI MATURITÀ

Il quadro si basa su **cinque livelli di maturità** che definiscono le fasi attraversate dagli Stati membri nella creazione delle capacità di cibersicurezza, nell'ambito corrispondente di ciascun obiettivo della NCSS. I livelli rappresentano gradi crescenti di maturità, a partire dal **livello 1**, dove gli Stati membri non hanno un approccio chiaramente definito per lo sviluppo di capacità di cibersicurezza nelle aree oggetto degli obiettivi della NCSS, per terminare con il **livello 5**, caratterizzato da una strategia di sviluppo delle capacità di cibersicurezza dinamica e in grado di adattarsi agli sviluppi ambientali. La Tabella 4 mostra la scala dei livelli di maturità, con una descrizione di ciascuno di essi.

Tabella 4. Scala di maturità a cinque livelli del quadro di valutazione delle capacità a livello nazionale dell'ENISA

LIVELLO 1 - INIZIALE/AD HOC	LIVELLO 2 - PRIMA DEFINIZIONE	LIVELLO 3 - COSTITUZIONE	LIVELLO 4 - OTTIMIZZAZIONE	LIVELLO 5 - ADATTABILITÀ
Lo Stato membro non ha un approccio chiaramente definito per lo sviluppo delle capacità di cibersicurezza negli ambiti trattati dagli obiettivi della NCSS. È possibile tuttavia che tale paese abbia fissato alcuni obiettivi generici ed eseguito alcuni studi (tecnici, politici, programmatici) per migliorare le capacità a livello nazionale.	È stato definito l'approccio nazionale per lo sviluppo delle capacità nell'ambito trattato dagli obiettivi della NCSS. Esistono piani d'azione o attività per raggiungere i risultati, ma si trovano in una fase iniziale. Inoltre, potrebbero essere stati identificati e/o coinvolti i portatori di interessi attivi.	Il piano d'azione per lo sviluppo delle capacità nell'ambito trattato dagli obiettivi della NCSS è chiaramente definito e sostenuto dai portatori di interessi correlati. Le pratiche e le attività sono applicate e implementate in modo uniforme a livello nazionale. Le attività sono definite e documentate con un'allocazione e una governance chiare delle risorse e una serie di scadenze.	Il piano d'azione è valutato regolarmente: vengono assegnate priorità, è ottimizzato e sostenibile. I risultati delle attività di sviluppo delle capacità di cibersicurezza sono misurati regolarmente. Vengono identificati i fattori di successo, le sfide e le lacune nell'attuazione delle attività.	La strategia di sviluppo delle capacità di cibersicurezza è dinamica e in grado di adattarsi. L'attenzione costante agli sviluppi ambientali (progressi tecnologici, conflitti globali, nuove minacce, ecc.) favorisce la capacità di decisione rapida e di intervento immediato in un'ottica di miglioramento.

3.3 POLI TEMATICI E STRUTTURA GENERALE DEL QUADRO DI AUTOVALUTAZIONE

Il quadro di autovalutazione è caratterizzato da **quattro poli tematici**: (I) Governance e standard di cibersicurezza, (II) Sviluppo delle capacità e sensibilizzazione, (III) Aspetti giuridici e normativi e (IV) Cooperazione. Ognuno di questi poli tematici tratta un'area tematica essenziale per costruire capacità di cibersicurezza in un paese e contiene un insieme di obiettivi diversi, che gli Stati membri potrebbero includere nelle loro NCSS. In particolare:

- **(I) Governance e standard di cibersicurezza**: questo polo tematico misura la capacità degli Stati membri di stabilire una governance adeguata, norme e buone pratiche nel campo della sicurezza informatica. Questa dimensione considera diversi aspetti della ciberdifesa e della resilienza, sostenendo al contempo lo sviluppo dell'industria della cibersicurezza nazionale e generando fiducia verso le amministrazioni pubbliche.
- **(II) Sviluppo della capacità e sensibilizzazione**: questo polo tematico valuta la capacità degli Stati membri di sensibilizzare in merito ai rischi e alle minacce della sicurezza informatica e a come affrontarli. Questa dimensione misura inoltre l'abilità del paese a sviluppare costantemente capacità di cibersicurezza e aumentare il livello generale di conoscenze e competenze in questo campo. Affronta lo sviluppo del mercato della cibersicurezza e i progressi nella ricerca e sviluppo in materia. Il polo tematico raggruppa tutti gli obiettivi che gettano le basi per promuovere lo sviluppo delle capacità.
- **(III) Aspetti giuridici e normativi**: questo polo tematico misura la capacità degli Stati membri di mettere in atto gli strumenti giuridici e normativi necessari per affrontare e contrastare l'aumento della cibercriminalità e gli incidenti ad essa correlati, nonché per proteggere le infrastrutture critiche informatizzate. Questa dimensione valuta anche la capacità degli Stati membri di creare un quadro giuridico per proteggere i cittadini e le imprese, come ad esempio nell'equilibrare tra sicurezza e privacy;
- **(IV) Cooperazione**: questo polo tematico valuta la cooperazione e la condivisione delle informazioni tra diversi gruppi di portatori di interessi a livello nazionale e internazionale come strumenti importanti per comprendere meglio e rispondere a un contesto di minacce in costante evoluzione.

Gli obiettivi inseriti nel modello sono quelli comunemente adottati dagli Stati membri e sono stati selezionati tra gli obiettivi elencati nella sezione 2.2. In particolare, il modello valuta i seguenti obiettivi:

- 1. Elaborare piani di emergenza informatica nazionali (I)
- 2. Stabilire misure di sicurezza di riferimento (I)
- 3. Proteggere l'identità digitale e generare fiducia nei servizi pubblici digitali (I)
- 4. Istituire una capacità di risposta agli incidenti (II)
- 5. Sensibilizzare gli utenti (II)
- 6. Organizzare esercitazioni di cibersicurezza (II)
- 7. Rafforzare i programmi di formazione e istruzione (II)
- 8. Promuovere la ricerca e lo sviluppo (II)
- 9. Fornire incentivi al settore privato per investire in misure di sicurezza (II)
- 10. Migliorare la cibersicurezza della catena di fornitura (II)
- 11. Proteggere le infrastrutture critiche informatizzate, OES e DSP (III)
- 12. Affrontare la criminalità informatica (III)
- 13. Istituire meccanismi di segnalazione degli incidenti (III)
- 14. Rafforzare la privacy e la protezione dei dati (III)
- 15. Istituzionalizzare la cooperazione tra agenzie pubbliche (IV)
- 16. Impegnarsi nella cooperazione internazionale (IV)
- 17. Istituire un partenariato pubblico-privato (IV)

I quattro poli tematici e gli obiettivi sottostanti sono combinati nel modello per avere una visione olistica del grado di maturità delle capacità di cibersicurezza degli Stati membri. La Figura 1

presenta la struttura generale del quadro di autovalutazione e mostra come questi elementi, vale a dire obiettivi, poli tematici e quadro di autovalutazione, siano collegati per valutare le prestazioni di un paese.

Figura 1. Struttura del quadro di autovalutazione

Per ogni obiettivo incluso nel quadro di autovalutazione, vi è una serie di indicatori distribuiti tra i cinque livelli di maturità. Ogni indicatore è basato su una domanda dicotomica (sì/no) e può costituire un requisito o un elemento facoltativo.

3.4 MECCANISMO DI ASSEGNAZIONE DEL PUNTEGGIO

Il **meccanismo di assegnazione del punteggio** del quadro di autovalutazione tiene conto degli elementi sopra citati e dei principi elencati nella sezione 3.5. Il modello fornisce in realtà un punteggio basato sul valore di due parametri: il **livello di maturità** e il **tasso di copertura**. Ciascuno di questi parametri può essere calcolato a diversi livelli: (i) per obiettivo, (ii) per poli tematici di obiettivi o (iii) complessivamente.

Punteggi a livello di obiettivo

Il **punteggio del livello di maturità** fornisce una panoramica del livello di maturità mostrando quali capacità e pratiche sono state messe in atto. Il punteggio del livello di maturità è calcolato come il livello più alto per il quale l'intervistato ha soddisfatto tutti i requisiti (cioè ha risposto «SÌ» a tutte le domande che costituivano un requisito), oltre ad avere soddisfatto tutti i requisiti dei livelli di maturità precedenti.

Il **tasso di copertura** mostra il grado di copertura di tutti gli indicatori per i quali la risposta è affermativa, indipendentemente dal livello. È un valore complementare che tiene conto di tutti gli indicatori che misurano un obiettivo. Il tasso di copertura è calcolato come il rapporto tra il numero totale di domande relative all'obiettivo e il numero di domande per le quali la risposta è affermativa.

È importante specificare che, nel prosieguo del documento, il termine ***punteggio*** è usato in riferimento sia ai valori del livello di maturità sia al tasso di copertura.

La figura 2 - Meccanismo di assegnazione del punteggio per obiettivo fornisce una rappresentazione del meccanismo di valutazione descritto nella sezione 3.1, che sarà approfondito di seguito.

Figura 2. Meccanismo di assegnazione del punteggio per obiettivo

La *Figura 2 mostra un esempio di come viene calcolato il livello di maturità per obiettivo. È opportuno notare che l'intervistato ha soddisfatto tutti i requisiti dei primi tre livelli di maturità e solo parzialmente quelli del livello 4. Quindi, il punteggio indica che il* ***livello di maturità dell'intervistato è il livello 3 per l'obiettivo «Organizzare l'esercitazione di cibersicurezza»***.

Tuttavia, nell'esempio rappresentato nella Figura 2, il livello di maturità dell'obiettivo non coglie le informazioni fornite dagli indicatori che hanno un punteggio positivo e che sono al di sopra del livello 3 di maturità. In tale caso, il tasso di copertura può offrire una panoramica di tutti gli elementi che l'intervistato ha attuato per raggiungere l'obiettivo in questione, indipendentemente dal suo livello di maturità effettivo. In questo caso, il rapporto tra il numero totale di domande relative all'obiettivo e il numero di domande per le quali la risposta è affermativa è pari a 19/27, vale a dire che ***il valore del tasso di copertura è 70 %.***

Inoltre, per adattarsi alle specificità degli Stati membri permettendo comunque una panoramica coerente, il punteggio è calcolato da due diversi campioni a livello di poli tematici e a livello complessivo:

- **Punteggi generali:** un campione completo che copre tutti gli obiettivi inclusi nel polo tematico o nel quadro complessivo (da uno a 17);
- **Punteggi specifici:** un campione specifico che copre solo gli obiettivi selezionati dallo Stato membro (di solito corrispondenti agli obiettivi presenti nella NCSS del paese specifico) all'interno del polo tematico o nel quadro complessivo.

Punteggi a livello di polo tematico

Il **livello di maturità generale di ogni polo tematico** è calcolato come la media aritmetica del livello di maturità di tutti gli obiettivi all'interno di tale polo.

Il **livello di maturità specifico per ciascun polo tematico** è calcolato come la media aritmetica del livello di maturità degli obiettivi all'interno di tale polo che lo Stato membro ha scelto di valutare (di solito corrispondenti agli obiettivi presenti nella NCSS del paese specifico).

Ad esempio, la Figura 1 mostra che il polo tematico (I) Governance e standard di cibersicurezza è costituito da tre obiettivi. Ipotizzando che l'intervistato abbia scelto di valutare solo i primi due obiettivi, ma non il terzo, e ipotizzando che i primi due obiettivi presentino un livello di maturità rispettivamente di 2 e 4, allora il livello di maturità del cluster considerando tutti gli obiettivi è il 2 (polo tematico (I) livello di maturità generico = (2+4)/3), mentre il livello di maturità del polo tematico considerando solo gli obiettivi specifici selezionati dal valutatore è il 3 (livello di maturità specifico per il polo tematico (I) = (2+4)/2).

Il **tasso di copertura generale per ciascun polo tematico** è calcolato come il rapporto tra il numero totale di domande all'interno del polo tematico e il numero di domande per le quali la risposta è affermativa.

Il **tasso di copertura specifico per ciascun cluster** è calcolato come il rapporto tra il numero totale di domande all'interno del polo tematico attinenti agli obiettivi che lo Stato membro ha scelto di valutare (di solito corrispondenti agli obiettivi presenti nella NCSS del paese specifico) e il numero di domande per le quali la risposta è affermativa.

Punteggi a livello complessivo

Il **livello di maturità generale complessivo di un paese** è calcolato come la media aritmetica del livello di maturità di tutti gli obiettivi all'interno del quadro, da uno a 17.

Il **livello di maturità specifico complessivo di un paese** è calcolato come la media aritmetica del livello di maturità degli obiettivi all'interno del quadro che lo Stato membro ha scelto di valutare (di solito corrispondenti agli obiettivi presenti nella NCSS del paese specifico).

Il **tasso di copertura generale complessivo di un paese** è calcolato come il rapporto tra il numero totale di domande all'interno di tutti gli obiettivi inclusi nel quadro (da uno a 17) e il numero di domande per le quali la risposta è affermativa.

Il **tasso di copertura specifico complessivo di un paese** è calcolato come il rapporto tra il numero totale di domande relative all'obiettivo nell'ambito del quadro che lo Stato membro ha scelto di valutare (di solito corrispondenti agli obiettivi presenti nella NCSS del paese specifico) e il numero di domande per le quali la risposta è affermativa.

Per ciascun indicatore, gli intervistati possono selezionare come risposta una terza opzione: «non so/non pertinente». In questo caso, l'indicatore è escluso dal calcolo totale dei risultati.

I livelli di maturità a livello di polo tematico e complessivi sono calcolati con una media aritmetica al fine di mostrare i progressi tra due valutazioni. Infatti, l'alternativa, che consiste nel considerare il livello di maturità dell'obiettivo meno maturo quale livello di maturità complessivo e del polo tematico, sebbene pertinente dal punto di vista della maturità, non tiene in considerazione i progressi compiuti in aree coperte da altri obiettivi.

Poiché il livello del polo tematico e quello complessivo sono consolidati ai fini della relazione, si è scelto di utilizzare la media aritmetica. Per una maggiore accuratezza, si invita a utilizzare i punteggi a livello di obiettivo per finalità di relazione.

La figura 3 in appresso riepiloga i meccanismi di assegnazione del punteggio per tutti i diversi livelli del modello (obiettivo, polo tematico e complessivo).

Figura 3. Meccanismo di assegnazione del punteggio complessivo

3.5 REQUISITI PER IL QUADRO DI AUTOVALUTAZIONE

Il quadro di valutazione delle capacità a livello nazionale (NCAF) presentato in questa sezione si basa sulle esigenze evidenziate dagli Stati membri ed è incentrato su una serie di requisiti elencati di seguito.

- L'NCAF è utilizzato su base volontaria dagli Stati membri come quadro di autovalutazione.
- L'NCAF intende misurare le capacità di cibersicurezza degli Stati membri relativamente ai 17 obiettivi. Tuttavia lo Stato membro può scegliere gli obiettivi rispetto ai quali eseguire la valutazione e valutare solo un sottoinsieme dei 17 obiettivi.
- Il quadro di autovalutazione intende misurare il livello di maturità delle capacità di cibersicurezza degli Stati membri.
- I risultati della valutazione non vengono pubblicati, a meno che lo Stato membro non decida di farlo di sua iniziativa.
- Lo Stato membro può esporre i risultati della valutazione presentando il livello di maturità delle capacità di cibersicurezza del paese, di un polo tematico di obiettivi o anche di un singolo obiettivo.
- Tutti gli obiettivi valutati sono ugualmente pertinenti all'interno del quadro di valutazione e hanno perciò la medesima importanza. Lo stesso vale per gli indicatori impiegati al suo interno.
- Lo Stato membro è in grado di tenere traccia dei progressi compiuti nel corso del tempo.

Il quadro di autovalutazione mira a sostenere gli Stati membri nello sviluppo delle capacità di cibersicurezza e include quindi anche una serie di raccomandazioni o linee guida per orientare gli Stati membri nel migliorare il proprio livello di maturità.

Nota: tali raccomandazioni o linee guida sono generiche e basate sulle pubblicazioni dell'ENISA e sulle lezioni apprese da altri paesi e dipenderanno dal risultato dell'autovalutazione.

4. INDICATORI DELL'NCAF

4.1 INDICATORI DEL QUADRO

La sezione presenta il quadro di valutazione delle capacità a livello nazionale dell'ENISA. Le seguenti sezioni sono organizzate per poli tematici.

Per ciascun polo tematico, una tabella riporta la serie completa di indicatori sotto forma di domande rappresentative di un determinato livello di maturità. Il questionario è lo strumento principale per l'autovalutazione. Per ciascun obiettivo sono presenti due serie di indicatori:

- una serie di domande generiche sulla maturità della strategia (9 domande generiche), contrassegnate con le lettere da «a» a «c» per ciascun livello di maturità, ripetute per ogni obiettivo e
- una serie di domande sulle capacità di cibersicurezza (319 domande sulle capacità di cibersicurezza), numerate da «1» a «10» per ciascun livello di maturità, specifiche per l'area interessata dall'obiettivo.

Ogni domanda viene presentata con un tag (0-1) che denota se la domanda è un indicatore che costituisce un requisito (1) oppure un elemento facoltativo (0) per il livello di maturità.

Ogni domanda può essere riconosciuta da un numero di identificazione composto da:

- numero dell'obiettivo
- livello di maturità
- numero della domanda.

Per esempio, la domanda ID 1.2.4 è la quarta domanda nel livello di maturità 2 dell'obiettivo strategico (I) «Elaborare piani di emergenza informatica nazionali».

Si precisa che, in tutto il questionario, l'ambito delle domande è a livello nazionale, se non diversamente indicato. In tutte le domande, il soggetto (pronome impersonale) si riferisce allo Stato membro in modo generico e non all'individuo o all'ente pubblico che effettua la valutazione.

Per la definizione di ciascun obiettivo, si rimanda al capitolo 2.2 - Obiettivi comuni individuati all'interno della NCSS europea.

4.1.1 Polo tematico n. 1: Governance e standard di cibersicurezza

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
1 – Elaborare piani di emergenza informatica nazionali	a	L'obiettivo è trattato nella strategia nazionale in materia di cibersicurezza (NCSS) attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	Si è iniziato a lavorare alla creazione di piani di emergenza informatica nazionali? Ad esempio, stabilendo gli obiettivi generali, l'ambito di applicazione e/o i principi dei piani di emergenza.	1	Si dispone di una dottrina/strategia nazionale che include la cibersicurezza come fattore di crisi (ossia un programma generale, una politica, ecc.)?	1	Si dispone di un piano di gestione delle crisi cibernetiche a livello nazionale?	1	Si è soddisfatti del numero o della percentuale di settori critici inclusi nel piano di emergenza informatica nazionale?	1	Esiste un processo a livello nazionale di apprendimento delle lezioni a seguito delle esercitazioni di cibersicurezza o delle crisi reali?	1
	2	È generalmente compreso che gli incidenti informatici costituiscono un fattore di crisi che potrebbe minacciare la sicurezza nazionale?	0	Si dispone di un hub per acquisire informazioni e informare i decisori? Ossia, metodi, piattaforme o sedi per garantire che tutti gli attori coinvolti nella risposta possano accedere alle stesse informazioni in tempo reale sulla crisi cibernetica.	1	Si dispone di procedure specifiche per le crisi cibernetiche a livello nazionale?	1	Vengono organizzate con sufficiente frequenza attività (ossia esercitazioni) in relazione alla pianificazione dell'emergenza informatica nazionale?	1	Si dispone di un processo per testare regolarmente il piano nazionale?	1
	3	Sono stati eseguiti studi (tecnici, operativi, politici) nel campo della pianificazione dell'emergenza informatica?	0	Vengono impegnate le risorse pertinenti per supervisionare lo sviluppo e l'esecuzione dei piani di emergenza informatica nazionali?	1	Si dispone di un team di comunicazione con una formazione specifica per rispondere alle crisi cibernetiche e informare il pubblico?	1	Si dispone di un numero sufficiente di persone dedicate alla pianificazione delle crisi, ad analizzare le lezioni apprese e ad attuare eventuali cambiamenti?	1	Si dispone di strumenti e piattaforme adeguati per creare una consapevolezza situazionale?	1
	4	-		Si dispone di una metodologia di valutazione delle minacce informatiche a livello nazionale che contempla procedure per la valutazione dell'impatto?	0	Vengono coinvolti tutti i portatori di interessi a livello nazionale (sicurezza nazionale, difesa, protezione civile, forze dell'ordine, ministeri, autorità, ecc.)?	1	Si dispone di un numero sufficiente di persone formate a rispondere alle crisi cibernetiche a livello nazionale?	1	Viene seguito un modello di maturità specifico per monitorare e migliorare il piano di emergenza informatica?	0
	5	-		-		Si dispone di strutture e sale situazioni adeguate per la gestione delle crisi?	1	-		Si dispone di risorse specializzate nella previsione delle minacce o che lavorano sulla cibersicurezza potenziale per affrontare le crisi o sfide future?	0

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
	6	-		-		Vi è un'interazione con i portatori di interessi internazionali nell'UE, se necessario?	0	-		-	
	7	-		-		Vi è un'interazione con i portatori di interessi internazionali nei paesi terzi, se necessario?	0	-		-	
2 – Stabilire misure di sicurezza di riferimento	a	L'obiettivo è trattato nella strategia nazionale in materia di cibersicurezza (NCSS) attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	È stato eseguito uno studio per individuare i requisiti e le lacune per le organizzazioni **pubbliche** sulla base di standard riconosciuti a livello internazionale? Ad esempio ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, UIT, ISA, IEC, CIS, ecc.	1	Le misure di sicurezza sono elaborate in conformità con le norme internazionali/nazionali?	1	Le misure di sicurezza di riferimento sono obbligatorie?	1	Esiste un processo per aggiornare frequentemente le misure di sicurezza di riferimento?	1	Esiste un processo per irrobustire le TIC quando le misure non riescono ad affrontare gli incidenti?	1
	2	È stato eseguito uno studio per individuare i requisiti e le lacune per le organizzazioni **private** sulla base di standard riconosciuti a livello internazionale? Ad esempio ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, UIT, ISA, IEC, CIS, ecc.	1	Il settore privato e altri portatori di interessi vengono consultati nella definizione delle misure di sicurezza di riferimento?	1	Vengono attuate misure di sicurezza orizzontali in tutti i settori critici?	1	È in atto un meccanismo di monitoraggio per esaminare l'adozione delle misure di sicurezza di riferimento?	1	Viene valutata la pertinenza delle nuove norme sviluppate in risposta agli ultimi sviluppi nel panorama delle minacce?	1
	3	-		-		Vengono attuate misure di sicurezza specifiche per il settore in tutti i settori critici?	1	Esiste un'autorità nazionale preposta a controllare l'effettiva applicazione delle misure di sicurezza di riferimento?	1	È in essere o viene promosso un processo nazionale di divulgazione coordinata delle vulnerabilità (CVD)?	1

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
	4	-				Le misure di sicurezza di riferimento sono in linea con i sistemi di certificazione pertinenti?	1	Si dispone di un processo per identificare le organizzazioni non conformi entro un determinato termine?	1	-	
	5	-		-		È previsto un processo di autovalutazione del rischio per le misure di sicurezza di riferimento?	1	Esiste un processo di verifica per assicurare che le misure di sicurezza siano applicate correttamente?	1	-	
2 – Stabilire misure di sicurezza di riferimento	6	-		-		È prevista la revisione delle misure di sicurezza di riferimento obbligatorie nel processo di approvvigionamento degli enti pubblici?	0	Viene definita o incoraggiata attivamente l'adozione di standard sicuri per lo sviluppo dei prodotti IT/OT critici (attrezzature mediche, veicoli connessi e autonomi, apparecchiature radio professionali, attrezzature per l'industria pesante, ecc.)?	0	-	
3 – Proteggere l'identità digitale e generare fiducia nei servizi pubblici digitali	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	Sono stati eseguiti studi o analisi delle lacune per individuare le esigenze di fornire servizi pubblici digitali ai cittadini e alle imprese?	1	Si eseguono analisi dei rischi per determinare il profilo di rischio delle risorse o dei servizi prima di trasferirli sul cloud o di intraprendere progetti di trasformazione digitale?	1	Vengono promosse metodologie di tutela della vita privata fin dalla progettazione in tutti i progetti di e-government?	1	Vengono raccolti indicatori sugli incidenti di sicurezza informatica che riguardano la violazione dei servizi pubblici digitali?	1	È prevista la partecipazione a gruppi di lavoro europei per mantenere gli standard e/o progettare nuovi requisiti per i servizi fiduciari elettronici (firme elettroniche, sigilli elettronici, servizi elettronici di recapito certificato, marcatura temporale, autenticazione di siti web)? Ad esempio ETSI/CEN/CENELEC, ISO, IETF, NIST, UIT, ecc.	1
	2	-		Si dispone di una strategia per creare o promuovere regimi di identificazione elettronica (e-ID) nazionali sicuri per i cittadini e le imprese?	1	I portatori di interessi privati vengono coinvolti nella progettazione e nella fornitura di servizi pubblici digitali sicuri?	1	È stato attuato il riconoscimento reciproco dei mezzi di identificazione elettronica con altri Stati membri?	1	Si partecipa attivamente alle revisioni tra pari nell'ambito della notifica dei regimi e-ID alla Commissione europea?	1

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
3 – Proteggere l'identità digitale e generare fiducia nei servizi pubblici digitali	3	-		Si dispone di una strategia per creare o promuovere servizi fiduciari elettronici nazionali sicuri (firme elettroniche, sigilli elettronici, servizi elettronici di recapito certificato, marcatura temporale, autenticazione di siti web) per i cittadini e le imprese?	1	Viene implementata una linea di riferimento di sicurezza minima per tutti i servizi pubblici digitali?	1	-		-	
	4	-		Si dispone di una strategia in tema di *governmental cloud* (una strategia di cloud computing rivolta a organismi pubblici come ministeri, agenzie governative e amministrazioni pubbliche, ecc.) che tenga conto delle implicazioni per la sicurezza?	0	Sono disponibili regimi di identificazione elettronica per i cittadini e le imprese con un livello di garanzia significativo o elevato, come definito nell'allegato del regolamento eIDAS (UE) n. 910/2014?	1	-		-	
	5	-		-		Si dispone di servizi pubblici digitali che richiedono regimi di identificazione elettronica con un livello di garanzia significativo o elevato, come definito nell'allegato del regolamento eIDAS (UE) n. 910/2014?	1	-		-	
	6	-		-		Si dispone di fornitori di servizi fiduciari per i cittadini e le imprese (firme elettroniche, sigilli elettronici, servizi elettronici di recapito certificato, marcatura temporale, autenticazione di siti web)?	1	-		-	
	7	-		-		Viene promossa l'adozione di misure di sicurezza di riferimento per tutti i modelli di implementazione del cloud (ad es. privato, pubblico, ibrido, IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Polo tematico n. 2: Sviluppo della capacità e sensibilizzazione

Obiettivo della NCSS	N.	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
4 – Istituire una capacità di risposta agli incidenti	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	Si dispone di capacità informali di risposta agli incidenti gestite all'interno o tra i settori pubblico e privato?	1	Si dispone di almeno un CSIRT nazionale ufficiale?	1	Si dispone di capacità di risposta agli incidenti per i settori citati nell'allegato II della direttiva NIS?	1	Sono state definite e promosse pratiche standardizzate per le procedure di risposta agli incidenti e gli schemi di classificazione degli incidenti?	1	Sono previsti meccanismi per il rilevamento precoce, l'identificazione, la prevenzione, la risposta e la mitigazione delle vulnerabilità zero-day?	1
	2	-		I CSIRT nazionali hanno un ambito di intervento chiaramente definito? Ad esempio a seconda del settore interessato, dei tipi di incidenti, degli impatti.	1	Esiste nel paese un meccanismo di cooperazione tra CSIRT per rispondere agli incidenti?	1	La capacità di risposta agli incidenti viene valutata al fine di assicurare la disponibilità di risorse e competenze adeguate a svolgere i compiti definiti al punto (2) dell'allegato I della direttiva NIS?	1	-	
	3	-		I CSIRT nazionali hanno relazioni chiaramente definite con altri portatori di interessi nazionali per quanto concerne il panorama nazionale della cibersicurezza e le pratiche di risposta agli incidenti (ad es. autorità di contrasto, militari, ISP, NCSC)?	0	I CSIRT nazionali hanno una capacità di risposta agli incidenti in conformità con l'allegato I della direttiva NIS? Ad esempio, disponibilità, sicurezza fisica, continuità operativa, cooperazione internazionale, monitoraggio degli incidenti, capacità di preallarme e annuncio, risposta agli incidenti, analisi dei rischi e sensibilizzazione situazionale, cooperazione con il settore privato, pratiche standard, ecc.	1	-		-	
	4	-				Esiste un meccanismo di cooperazione con altri paesi confinanti riguardo agli incidenti?	1	-		-	

Obiettivo della NCSS	N.	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
4 – Istituire una capacità di risposta agli incidenti	5	-		-		Sono state definite formalmente politiche e procedure chiare di gestione degli incidenti?	1	-		-	
	6	-		-		I CSIRT nazionali partecipano a esercitazioni di cibersicurezza a livello nazionale e internazionale?	1	-		-	
	7	-		-		I CSIRT nazionali sono affiliati al FIRST (Forum of Incident Response and Security Teams)?	0	-		-	
5 – Sensibilizzare gli utenti	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	Esiste un minimo riconoscimento da parte della pubblica amministrazione, del settore privato o degli utenti in generale della necessità di sensibilizzare sui temi della cibersicurezza e della privacy?	1	È stato identificato un pubblico specifico di destinatari per la sensibilizzazione degli utenti? Ad esempio, utenti in generale, giovani, utenti aziendali (che possono essere ulteriormente suddivisi in PMI, OES, DSP, ecc.).	1	Sono stati sviluppati piani/strategie di comunicazione per le campagne?	1	Vengono elaborate metriche per valutare la campagna durante la fase di pianificazione?	1	Sono in atto meccanismi per assicurare che le campagne di sensibilizzazione siano costantemente pertinenti per quanto concerne il progresso tecnologico, i cambiamenti nel panorama delle minacce, le normative e le direttive di sicurezza nazionali?	1
	2	Le agenzie pubbliche conducono campagne di sensibilizzazione in materia di cibersicurezza nell'ambito della loro organizzazione su una base ad-hoc? Ad esempio in seguito a un incidente di sicurezza informatica.	0	Viene elaborato un piano di progetto per sensibilizzare sui temi della sicurezza delle informazioni e della privacy?	1	Si dispone di un processo per creare contenuti a livello di pubblica amministrazione?	1	Le campagne vengono valutate dopo l'esecuzione?	1	Si esegue una valutazione periodica o uno studio per misurare i cambiamenti di atteggiamento o di comportamento in materia di cibersicurezza e privacy nei settori pubblico e privato?	1

Obiettivo della NCSS	N.	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
5 – Sesibilizzare gli utenti	3	Le agenzie pubbliche conducono campagne di sensibilizzazione sulla cibersicurezza rivolte al pubblico generale su una base ad-hoc? Ad esempio in seguito a un incidente di sicurezza informatica.	0	Vi sono risorse disponibili e facilmente identificabili (ad es. un unico portale online, kit di sensibilizzazione) per gli utenti che vogliano informarsi sulle questioni relative alla cibersicurezza e alla privacy?	1	Si dispone di meccanismi per individuare le aree target per la sensibilizzazione (ad es. panorama delle minacce dell'ENISA, panorami nazionali, panorami internazionali, feedback dei centri nazionali per la lotta alla criminalità informatica, ecc.)?	1	Sono in atto meccanismi per identificare i mezzi o i canali di comunicazione più pertinenti a seconda del pubblico target al fine di massimizzare l'estensione e il coinvolgimento? Ad esempio, diversi tipi di media digitali, opuscoli, e-mail, materiale didattico, manifesti in aree frequentate, TV, radio, ecc.	1	È prevista la consultazione con esperti del comportamento per adattare la campagna al pubblico target?	1
	4	-		-		I portatori di interessi si riuniscono con esperti e team di comunicazione per creare contenuti?	1			-	
	5	-		-		Il settore privato viene coinvolto negli sforzi di sensibilizzazione compiuti per promuovere e diffondere i messaggi a un pubblico più vasto?	1	-		-	
	6	-		-		Vengono predisposte iniziative di sensibilizzazione specifiche per i dirigenti del settore pubblico, privato, del mondo accademico o della società civile?	1	-		-	
	7	-		-		È prevista la partecipazione alle campagne del Mese europeo della sicurezza informatica dell'ENISA (ECSM)?	0	-		-	
6 – Organizzare esercitazioni di cibersicurezza	a	L'obiettivo è trattato nella strategia nazionale in materia di cibersicurezza (NCSS) attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						

Obiettivo della NCSS	N.	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
6 – Organizzare esercitazioni di cibersicurezza	1	Vengono condotte esercitazioni di crisi in altri settori (diversi dalla cibersicurezza) a livello nazionale o paneuropeo?	1	Si dispone di un programma di esercitazione di cibersicurezza a livello nazionale?	1	Vengono coinvolte tutte le autorità della pubblica amministrazione correlate (anche se lo scenario è specifico per il settore)?	1	Vengono redatti rapporti delle azioni compiute/di valutazione?	1	Si dispone di una capacità di analisi delle lezioni apprese per la cibersicurezza (processi di reporting, analisi, mitigazione)?	1
	2	Vi sono risorse assegnate alla progettazione e alla pianificazione delle esercitazioni di gestione delle crisi?	1	Vengono eseguite o si assegna priorità alle esercitazioni di gestione delle crisi cibernetiche su funzioni vitali della società e infrastrutture critiche?	1	Viene coinvolto il settore privato nella pianificazione e nell'esecuzione delle esercitazioni?	1	Vengono testati piani e procedure a livello nazionale?	1	Esiste un processo consolidato per le lezioni apprese?	1
	3	-		È stato individuato un organismo di coordinamento per supervisionare la progettazione e la pianificazione delle esercitazioni di cibersicurezza (agenzia pubblica, società di consulenza, ecc.)?	0	Vengono organizzate esercitazioni specifiche di settore a livello nazionale e/o internazionale?	1	È prevista la partecipazione a esercitazioni di cibersicurezza a livello paneuropeo?	1	Gli scenari delle esercitazioni vengono adattati in funzione degli ultimi sviluppi (progressi tecnologici, conflitti globali, panorama delle minacce, ecc.)?	1
	4	-		-		Vengono organizzate esercitazioni in tutti i settori critici menzionati nell'allegato II della direttiva sulla cibersicurezza?	1	-		Le procedure di gestione delle crisi vengono allineate con quelle degli altri Stati membri per garantire un'efficace gestione paneuropea delle crisi?	1
	5	-		-		Vengono organizzate esercitazioni di cibersicurezza intersettoriali?	1	-		Si dispone di un meccanismo per adattare rapidamente la strategia, i piani e le procedure in base alle lezioni apprese durante le esercitazioni?	0
	6	-		-		Vengono organizzate esercitazioni di cibersicurezza specifiche a vari livelli (livello tecnico e operativo, livello procedurale, livello decisionale, livello politico, ecc.)	0	-		-	
7 – Rafforzare i programmi formativi ed educativi	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		

Obiettivo della NCSS	N.	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	È considerato lo sviluppo di programmi educativi e di formazione sulla cibersicurezza?	1	Vengono istituiti corsi dedicati alla cibersicurezza?	1	Il paese include la cultura della cibersicurezza nelle prime fasi del percorso educativo degli studenti? Ad esempio, si sostiene la cibersicurezza nelle scuole medie e superiori?	1	Il personale del settore pubblico e privato viene esortato a essere accreditato o certificato?	1	Sono in atto meccanismi per assicurare che i programmi educativi e di formazione siano costantemente pertinenti per quanto concerne gli sviluppi tecnologici attuali ed emergenti, i cambiamenti nel panorama delle minacce, le normative e le direttive di sicurezza nazionali?	1
	2	-		Le università del paese offrono dottorati di ricerca in cibersicurezza come disciplina indipendente e non come materia informatica?	1	Esistono laboratori di ricerca e istituti di istruzione nazionali specializzati in cibersicurezza?	1	Il paese ha sviluppato programmi di formazione o mentoring sulla cibersicurezza per sostenere le start-up e le PMI nazionali?	1	Vengono istituiti centri di eccellenza accademici nella cibersicurezza che fungano da poli per la ricerca e l'istruzione?	1
	3	-		È prevista la formazione degli educatori, indipendentemente dal loro campo, sui temi della sicurezza delle informazioni e della privacy? Ad esempio sicurezza online, protezione dei dati personali, bullismo online.	1	Vengono incoraggiati/finanziati corsi dedicati alla cibersicurezza e piani di formazione per i dipendenti delle agenzie di collocamento degli Stati membri?	1	Viene promosso attivamente l'inserimento di corsi sulla sicurezza delle informazioni nell'istruzione superiore, non solo per gli studenti di informatica ma anche per altre specialità professionale? Ad esempio corsi su misura per le esigenze di tale professione.	1	Le istituzioni accademiche partecipano a discussioni di primo piano nell'area dell'educazione e della ricerca sulla cibersicurezza a livello internazionale?	0
	4	-		-		Si dispone di corsi sulla cibersicurezza e/o di programmi scolastici specializzati per i livelli da 5 a 8 dell'EQF (quadro europeo delle qualifiche)?	1	Viene valutata regolarmente la carenza di competenze (mancanza di personale di cibersicurezza) nell'area della sicurezza delle informazioni?	1	-	
	5	-		-		Vengono incoraggiate e/o sostenute iniziative per includere corsi sulla sicurezza di internet nell'istruzione primaria e secondaria?	1	Vengono promossi il networking e la condivisione di informazioni tra gli istituti universitari, a livello sia nazionale sia internazionale?	1		

Obiettivo della NCSS	N.	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
7 - Rafforzare i programmi formativi ed educativi	6	-		-		Vengono finanziati o offerti gratuitamente ai cittadini corsi di formazione di base sulla cibersicurezza?	0	Viene coinvolto in qualche forma il settore privato nelle iniziative di formazione sulla cibersicurezza? Ad esempio progettazione ed erogazione di corsi, stage, tirocini, ecc.	1	-	
	7	-		-		Vengono organizzati eventi annuali sulla sicurezza delle informazioni (ad es. gare tra hacker o hackathon)?	0	Vengono implementati meccanismi di finanziamento per promuovere la diffusione di lauree in cibersicurezza? Ad esempio borse di studio, apprendistato/stage garantito, posti di lavoro garantiti in settori specifici o ruoli nel settore pubblico.	0	-	
8 – Promuovere ricerca e sviluppo	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	Sono stati eseguiti studi o analisi per identificare le priorità di R&S in materia di cibersicurezza?	1	Si dispone di un processo per definire le priorità di R&S (ad es. argomenti emergenti per la dissuasione, la protezione, il rilevamento e l'adattamento a nuovi tipi di attacchi informatici)?	1	Esiste un piano per collegare le iniziative di R&S all'economia reale?	1	Le iniziative di R&S sulla cibersicurezza sono in linea con gli obiettivi strategici pertinenti, ad es. mercato unico digitale, Orizzonte 2020, programma Europa digitale, strategia di cibersicurezza dell'UE?	1	Si persegue a livello nazionale la cooperazione con le iniziative internazionale di R&S correlate alla cibersicurezza?	1
	2	-		Il settore privato è coinvolto nella definizione delle priorità di R&S?	1	Esistono progetti nazionali relativi alla cibersicurezza?	1	Esiste uno schema di valutazione per le iniziative di R&S?	1	Le priorità di R&S sono allineate alla regolamentazione attuale o imminente (a livello nazionale)?	1

Obiettivo della NCSS	N.	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
8 – Promuovere ricerca e sviluppo	3	-		Il mondo accademico è coinvolto nella definizione delle priorità di R&S?	1	Si dispone di ecosistemi di startup e di altri canali di networking locali/regionali (ad es. parchi tecnologici, poli di innovazione, eventi/piattaforme di networking) per promuovere l'innovazione (anche per le start-up della cibersicurezza)?	1	Esistono accordi di cooperazione con università e altre strutture di ricerca?	1	È prevista la partecipazione a discussioni di primo piano in uno o più temi di R&S all'avanguardia a livello internazionale?	0
	4	-		Esistono iniziative nazionali di R&S legate alla cibersicurezza?	0	Esistono investimenti in programmi di R&S sulla cibersicurezza nel mondo accademico e nel settore privato?	1	Esiste un organismo istituzionale riconosciuto che supervisiona le attività di R&S sulla cibersicurezza?	0	-	
	5	-		-		Esistono cattedre di ricerca industriale nelle università per collegare gli argomenti della ricerca alle esigenze del mercato?	1	-		-	
	6	-		-		Si dispone di programmi di finanziamento di R&S per la cibersicurezza?	0	-		-	
9 – Fornire incentivi al settore privato per gli investimenti in misure di sicurezza	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	Esiste una politica industriale o una volontà politica di incoraggiare lo sviluppo dell'industria della cibersicurezza?	1	Il settore privato è coinvolto nella progettazione degli incentivi?	1	Esistono incentivi economici/normativi o di altro tipo per promuovere gli investimenti nella cibersicurezza?	1	Esistono attori privati che rispondono agli incentivi investendo in misure di sicurezza? Ad esempio investitori specializzati in cibersicurezza e investitori non specializzati.	1	Gli incentivi sui temi della cibersicurezza vengono orientati in base agli sviluppi delle minacce più recenti?	1

Obiettivo della NCSS	N.	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
9 – Fornire incentivi al settore privato per gli investimenti in misure di sicurezza	2	-		Sono stati identificati argomenti di cibersicurezza specifici da sviluppare? Ad esempio crittografia, privacy, nuove forme di autenticazione, IA per la cibersicurezza, ecc.	0	Viene fornito sostegno supporto (ad es. incentivi fiscali) per le start-up e le PMI della cibersicurezza?	1	Vengono forniti incentivi al settore privato affinché si concentri sulla sicurezza delle tecnologie d'avanguardia? Ad esempio 5G, intelligenza artificiale, IoT, informatica quantistica, ecc.	1	-	
	3	-		-		Vengono forniti incentivi fiscali o altre incentivazioni finanziarie per investimenti del settore privato nelle start-up di cibersicurezza?	1	-		-	
	4	-		-		Viene facilitato l'accesso al processo degli appalti pubblici per le start-up e le PMI della cibersicurezza?	0	-		-	
	5	-		-		È disponibile un budget per fornire incentivi al settore privato?	0	-		-	
10 – Migliorare la cibersicurezza della catena di fornitura	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	È stato condotto uno studio sulle buone pratiche di sicurezza per la gestione della catena di fornitura utilizzate dagli appalti in vari segmenti industriali e/o nel settore pubblico?	1	Vengono eseguite valutazioni di cibersicurezza lungo tutta la catena di fornitura di servizi e prodotti TIC in settori critici [identificati nell'allegato II della direttiva NIS (2016/1148)]?	1	Viene utilizzato un sistema di certificazione della sicurezza per prodotti e servizi basati sulle TIC? Ad es. l'accordo sul reciproco riconoscimento (ARR) del gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione (SOG-IS) in Europa, l'accordo di riconoscimento dei criteri comuni (CCRA), iniziative nazionali, iniziative settoriali, ecc.	1	Si dispone di un processo per aggiornare le valutazioni di cibersicurezza della catena di fornitura di servizi e prodotti TIC in settori critici [identificati nell'allegato II della direttiva NIS (2016/1148)]?	1	Si dispone di sonde di rilevamento negli elementi chiave della catena di fornitura per rilevare i primi segni di compromissione? Ad es. controlli di sicurezza a livello di ISP, sonde di sicurezza nei componenti delle infrastrutture principali, ecc.	1

Obiettivo della NCSS	N.	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
10 – Migliorare la cibersicurezza della catena di fornitura	2	-		Vengono applicati standard nelle politiche di approvvigionamento delle pubbliche amministrazioni per garantire che i fornitori di prodotti o servizi TIC rispondano ai requisiti di riferimento per la sicurezza delle informazioni? Ad esempio ISO/IEC 27001 e 27002, ISO/IEC 27036, ecc.	1	Vengono promosse attivamente le migliori prassi di sicurezza e di tutela della vita privata fin dalla progettazione nello sviluppo di prodotti e servizi TIC? Ad esempio ciclo di vita di sviluppo software sicuro, ciclo di vita IoT.	1	Si dispone di un processo per individuare gli anelli deboli della cibersicurezza nella catena di fornitura di servizi e prodotti TIC in settori critici [identificati nell'allegato II della direttiva NIS (2016/1148)]?	1	-	
	3	-		-		Vengono elaborati e forniti cataloghi centralizzati con informazioni estese degli standard esistenti in materia di sicurezza delle informazioni e della privacy che siano modulati per le PMI e applicabili dalle stesse?	1	Sono in atto meccanismi per assicurare che i prodotti e i servizi TIC che sono critici per gli OES siano ciber-resilienti, abbiano cioè la capacità di mantenere la disponibilità e la sicurezza di fronte a un incidente informatico? Ad esempio attraverso test, valutazioni regolari, rilevamento di elementi compromessi, ecc.	1	-	
	4	-				Vi è una partecipazione attiva alla progettazione di un quadro di certificazione a livello dell'UE per prodotti digitali, servizi e processi TIC, come stabilito nel regolamento UE sulla cibersicurezza [Regolamento (UE) 2019/881]? Ad es. partecipazione al Gruppo europeo per la certificazione della cibersicurezza (ECCG), promozione di standard e procedure di natura tecnica per la sicurezza dei prodotti/servizi TIC.	0	Viene promosso lo sviluppo di sistemi di certificazione rivolti alle PMI per incentivare l'adozione di standard di sicurezza delle informazioni e privacy?	0	-	
	5	-		-		Viene fornito qualche tipo di incentivo alle PMI per l'adozione di standard di sicurezza e privacy?	0	Sono in atto disposizioni per incoraggiare le grandi aziende ad aumentare la cibersicurezza delle piccole imprese nelle loro catene di fornitura? Ad esempio hub di cibersicurezza, formazione, campagne di sensibilizzazione, ecc.	0	-	

Obiettivo della NCSS	N.	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
	6	-		-		I fornitori di software vengono incoraggiati a sostenere le PMI garantendo configurazioni predefinite sicure nei prodotti destinati alle organizzazioni di piccole dimensioni?	0	-		-	

4.1.3 Polo tematico n. 3: Aspetti giuridici e normativi

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
11 – Proteggere infrastrutture critiche informatizzate, operatori di servizi essenziali (OES) e fornitori di servizi digitali (DSP)	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	È riconosciuto a livello generale che i gestori di infrastrutture critiche informatizzate contribuiscono alla sicurezza nazionale?	1	Si dispone di una metodologia per identificare i servizi essenziali?	1	È stata attuata la direttiva NIS (2016/1148)?	1	Esiste una procedura per aggiornare il registro dei rischi?	1	Vengono create e aggiornate le relazioni sul panorama delle minacce?	1
	2	-		Si dispone di una metodologia per identificare le infrastrutture critiche informatizzate?	1	È stata attuata la direttiva ECI (2008/114) relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione?	1	Sono in atto altri meccanismi per valutare che le misure tecniche e organizzative adottate dagli OES siano appropriate per gestire i rischi posti alla sicurezza delle reti e dei sistemi informativi? Ad esempio, audit regolari sulla cibersicurezza, quadro nazionale per l'attuazione di misure standard, strumenti tecnici forniti dalla pubblica amministrazione, come sonde di rilevamento o revisione della configurazione specifica del sistema.	1	A seconda degli ultimi sviluppi nel panorama delle minacce, si è in grado di inserire un nuovo settore nel piano d'azione per la protezione delle infrastrutture critiche informatizzate (CIIP)?	1
	3	-		Si dispone di una metodologia per identificare gli OES?	1	Si dispone di un registro nazionale degli OES identificati per ogni settore critico?	1	Viene rivisto e aggiornato di conseguenza l'elenco degli OES identificati almeno ogni due anni?	1	A seconda degli ultimi sviluppi nel panorama delle minacce, si è in grado di adattare nuovi requisiti nel piano d'azione CIIP?	1

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
11 – Proteggere infrastrutture critiche informatizzate, operatori di servizi essenziali (OES) e fornitori di servizi digitali (DSP)	4	-		Si dispone di una metodologia per identificare i fornitori di servizi digitali?	1	Si dispone di un registro nazionale per i fornitori di servizi digitali identificati?	1	Sono in atto altri meccanismi per valutare che le misure tecniche e organizzative adottate dai fornitori di servizi digitali siano appropriate per gestire i rischi posti alla sicurezza delle reti e dei sistemi informativi? Ad esempio, audit regolari sulla cibersicurezza, quadro nazionale per l'attuazione di misure standard, strumenti tecnici forniti dalla pubblica amministrazione, come sonde di rilevamento o revisione della configurazione specifica del sistema.	1	-	
	5	-		Si dispone di una o più autorità nazionali che effettuano la supervisione sulla protezione delle infrastrutture critiche informatizzate e sulla sicurezza delle reti e dei sistemi informativi? Ad esempio come previsto dalla direttiva NIS (2016/1148).	1	Si dispone di un registro dei rischi nazionale per i rischi noti o identificati?	1	Viene rivisto e aggiornato di conseguenza l'elenco dei fornitori di servizi digitali identificati almeno ogni due anni?	1	-	
	6	-		Vengono sviluppati piani di protezione specifici per il settore? Ad esempio, includendo misure di cibersicurezza di riferimento (obbligatorie o linee guida).	0	Si dispone di una metodologia per mappare le dipendenze delle infrastrutture critiche informatizzate?	1	Viene utilizzato un sistema di certificazione della sicurezza (nazionale o internazionale) per aiutare gli OES e i fornitori di servizi digitali a identificare prodotti TIC sicuri? Ad esempio l'ARR del SOG-IS in Europa, iniziative nazionali, ecc.	1	-	
	7	-		-		Si attuano pratiche di gestione del rischio per identificare, quantificare e gestire i rischi relativi alle infrastrutture critiche informatizzate a livello nazionale?	1	Si utilizza un sistema di certificazione della sicurezza o una procedura di qualificazione per valutare i fornitori di servizi che lavorano con gli OES? Ad es. fornitori di servizi nel campo del rilevamento degli incidenti, della risposta agli incidenti, dell'audit della cibersicurezza, dei servizi cloud, delle smart card.	1	-	

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
11 – Proteggere infrastrutture critiche informatizzate, operatori di servizi essenziali (OES) e fornitori di servizi digitali (DSP)	8	-		-		È previsto il coinvolgimento in un processo di consultazione per identificare le dipendenze transfrontaliere?	1	Sono in atto meccanismi per misurare il livello di conformità degli OES e dei fornitori di servizi digitali per quanto riguarda le misure di cibersicurezza di riferimento?	0	-	
	9					Si dispone di un unico punto di contatto responsabile del coordinamento delle questioni relative alla sicurezza delle reti e dei sistemi informativi a livello nazionale e della cooperazione transfrontaliera a livello dell'Unione?	1	Sono in vigore disposizioni per garantire la continuità dei servizi forniti dalle infrastrutture critiche informatizzate? Ad esempio previsione delle crisi, procedure per la ricostruzione dei sistemi critici informatizzati, continuità aziendale senza IT, procedure di backup in isolamento (air gap), ecc.	0		
	10					Vengono definite misure di cibersicurezza di riferimento (obbligatorie o come linee guida) per i fornitori di servizi digitali e per tutti i settori identificati nell'allegato II della direttiva NIS (2016/1148)?	1				
	11	-		-		Vengono forniti strumenti o metodologie per rilevare gli incidenti informatici?	1	-		-	
12 – Affrontare la criminalità informatica	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
12 – Affrontare la criminalità informatica	1	È stato eseguito uno studio per identificare i requisiti di applicazione della legge (base giuridica, risorse, competenze, ecc.) per affrontare efficacemente la criminalità informatica?	1	Il quadro giuridico nazionale è pienamente conforme al quadro giuridico pertinente dell'UE, inclusa la direttiva (UE) 2013/40 relativa agli attacchi contro i sistemi di informazione? Ad esempio accesso illecito a sistemi di informazione, interferenza illecita relativamente ai sistemi, interferenza illecita relativamente ai dati, intercettazione illecita, strumenti utilizzati per commettere i reati, ecc.	1	Si dispone di unità dedicate al trattamento della criminalità informatica nelle procure?	1	Si raccolgono statistiche secondo le disposizioni dell'articolo 14, paragrafo 1, della direttiva (UE) 2013/40 relativa agli attacchi contro i sistemi di informazione?	1	Si dispone di formazione interistituzionale o workshop formativi per autorità di contrasto, giudici, procuratori e CSIRT nazionali/pubblici a livello nazionale e/o multilaterale?	1
	2	È stato eseguito uno studio per identificare i requisiti per procuratori e giudici (base giuridica, risorse, competenze, ecc.) per affrontare efficacemente la criminalità informatica?	1	Esistono disposizioni giuridiche in materia di furto d'identità online e furto di dati personali online?	1	Si dispone di un budget dedicato alle unità di criminalità informatica?	1	Vengono raccolte statistiche separate sulla criminalità informatica? Ad esempio statistiche operative, statistiche sulle tendenze della criminalità informatica, statistiche sui proventi della criminalità informatica e sui danni provati, ecc.	1	È prevista la partecipazione ad azioni coordinate a livello internazionale per contrastare le attività criminali? Ad esempio, infiltrazione di forum di hacking criminale, gruppi di criminalità informatica organizzata, mercati del dark web e smantellamento di botnet, ecc.	1
	3	Il paese ha firmato la Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica?	1	Esistono disposizioni giuridiche in materia di furto di proprietà intellettuale e violazioni del diritto d'autore online?	1	È stato istituito un organismo/un'entità centrale per coordinare le attività nel campo della lotta alla criminalità informatica?	1	Viene valutata l'adeguatezza della formazione fornita al personale delle autorità di contrasto, della magistratura e dei CSIRT nazionali per affrontare la criminalità informatica?	1	Esiste una chiara separazione delle funzioni tra CSIRT, autorità di contrasto e magistratura (procuratori e giudici) quando cooperano per affrontare i crimini informatici?	1
	4			Esistono disposizioni giuridiche in materia di molestie o bullismo online?	1	Sono stati istituiti meccanismi di cooperazione tra le istituzioni nazionali pertinenti coinvolte nella lotta alla criminalità informatica, compresi autorità di contrasto e CSIRT nazionali?	1	Vengono eseguite valutazioni regolari per garantire la disponibilità di risorse sufficienti (umane, di bilancio e di strumenti) dedicate alle unità di criminalità informatica all'interno delle autorità di contrasto?	1	Il quadro normativo facilita la cooperazione tra CSIRT/autorità di contrasto e magistratura (procuratori e giudici)?	1
	5			Esistono disposizioni giuridiche in materia di frode informatica? Ad esempio conformità alle disposizioni della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica.	1	È prevista la cooperazione e la condivisione di informazioni con altri Stati membri nell'ambito della lotta alla criminalità informatica?	1	Vengono eseguite valutazioni regolari per garantire la disponibilità di risorse sufficienti (umane, di bilancio e di strumenti) dedicate alle unità di criminalità informatica all'interno delle autorità responsabili dell'azione penale?	1	È prevista la partecipazione alla costruzione e al mantenimento di strumenti e metodologie, moduli e procedure standardizzati da condividere con i portatori di interessi dell'UE (autorità di contrasto, CSIRT, ENISA, EC3 di Europol, ecc.)?	1

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
12 – Affrontare la criminalità informatica	6	-		Esistono disposizioni giuridiche in materia di tutela dei minori online? Ad esempio conformità alle disposizioni della direttiva (UE) 2011/93 e della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica.	1	È prevista la cooperazione e la condivisione di informazioni con le agenzie dell'UE (ad es. EC3 di Europol, Eurojust, ENISA) nell'ambito della lotta alla criminalità informatica?	1	Si dispone di unità, tribunali dedicati o giudici specializzati per gestire i casi di criminalità informatica?	1	Sono in atto meccanismi avanzati per dissuadere gli individui dall'essere attirati o coinvolti nella criminalità informatica?	0
	7	-		È stato individuato un punto di contatto nazionale operativo per lo scambio di informazioni e la risposta a richieste di informazioni urgenti di altri Stati membri, relativamente ai reati di cui alla direttiva (UE) 2013/40 relativa agli attacchi contro i sistemi di informazione?	1	Si dispone di strumenti adeguati per affrontare la criminalità informatica? Ad es. tassonomia e classificazione dei crimini informatici, strumenti per la raccolta di prove elettroniche, strumenti di informatica forense, piattaforme di condivisione affidabili, ecc.	1	Esistono disposizioni dedicate a fornire supporto e assistenza alle vittime di crimini informatici (utenti generici, PMI, grandi aziende)?	1	Il paese utilizza il programma UE e/o il protocollo di risposta alle emergenze delle autorità di contrasto (EU LE ERP) per rispondere efficacemente agli incidenti informatici su larga scala?	0
	8			La propria autorità di contrasto prevede un'unità di criminalità informatica dedicata?	1	Si dispone di procedure operative standard per gestire gli incidenti informatici?	1	È stato istituito un quadro interistituzionale e meccanismi di cooperazione tra tutti portatori di interessi pertinenti (ad es. autorità di contrasto, CSIRT nazionale, comunità giudiziaria), compreso il settore privato (ad es. operatori di servizi essenziali, fornitori di servizi), ove opportuno, per rispondere agli attacchi informatici?	1	-	
	9			È stato designato un punto di contatto attivo 24 ore su 24, 7 giorni su 7 in conformità con l'art. 35 della Convenzione di Budapest?	1	Il paese partecipa alle opportunità di formazione offerte e/o sostenute dalle agenzie dell'UE (ad es. Europol, Eurojust, OLAF, Cepol, ENISA)?	0	Il quadro normativo facilita la cooperazione tra CSIRT e autorità di contrasto?	1	-	
	10	-		È stato designato un punto di contatto operativo nazionale, attivo 24 ore su 24, 7 giorni su 7, per il protocollo di risposta alle emergenze delle autorità di contrasto (EU LE ERP) al fine di rispondere agli incidenti informatici di maggior rilievo?	1	Il paese sta considerando l'adozione del secondo protocollo addizionale alla Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica?	0	Sono in atto meccanismi (ad es. strumenti, procedure) per facilitare lo scambio di informazioni e la cooperazione tra CSIRT/autorità di contrasto ed eventualmente la magistratura (procuratori e giudici) nell'ambito della lotta alla criminalità informatica?	1	-	

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
	11			Viene fornita regolarmente una formazione specialistica ai portatori di interessi coinvolti nella lotta alla criminalità informatica (autorità di contrasto, magistratura, CSIRT)? Ad esempio, sessioni di formazione sul perseguimento dei reati favoriti dall'informatica, formazione sulla raccolta di prove elettroniche e sulla garanzia di integrità lungo la catena di custodia digitale e sull'informatica forense, ecc.	1						
	12			Il paese ha ratificato/aderito alla Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica?	1			-	-	-	
	13	-		Il paese ha firmato e ratificato il protocollo addizionale (relativo all'incriminazione di atti di natura razzista e xenofoba commessi a mezzo di sistemi informatici) alla Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica?	0	-	-	-		-	
13 – Istituire meccanismi di segnalazione degli incidenti	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	Esistono meccanismi informali di condivisione delle informazioni sugli incidenti di cibersicurezza tra organizzazioni private e autorità nazionali?	1	Si dispone di un sistema di segnalazione degli incidenti per tutti i settori contemplati dall'allegato II della direttiva NIS?	1	Si dispone di un sistema di segnalazione obbligatoria degli incidenti che funziona nella pratica?	1	Si dispone di una procedura armonizzata per i sistemi di segnalazione degli incidenti settoriali?	1	Viene creato un rapporto annuale sugli incidenti?	1

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
13 – Istituire meccanismi di segnalazione degli incidenti	2	-		Sono stati attuati i requisiti di comunicazione per i fornitori di servizi di telecomunicazione in conformità con l'articolo 40 della direttiva (UE) 2018/1972? La direttiva prevede che gli Stati membri garantiscano che i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico comunichino senza indebito ritardo all'autorità competente ogni incidente di sicurezza che abbia avuto conseguenze significative sul funzionamento delle reti o dei servizi.	1	Esiste un meccanismo di coordinamento/cooperazione per gli obblighi di segnalazione degli incidenti relativi a RGPD, articolo 40 (precedentemente articolo 13 *bis*) della direttiva NIS e eIDAS?	1	Si dispone di un sistema di segnalazione degli incidenti per settori diversi da quelli contemplati dalla direttiva NIS?	1	Esistono relazioni sul panorama della cibersicurezza o altri tipi di analisi preparati dall'entità che riceve le relazioni sugli incidenti?	1
	3	-		Sono stati attuati i requisiti di notificazione per i prestatori di servizi fiduciari in conformità con l'articolo 19 del regolamento eIDAS [regolamento (UE) 910/2014]? L'articolo 19 prevede, tra gli altri obblighi, che i prestatori di servizi fiduciari notifichino all'organismo di vigilanza gli incidenti/le violazioni importanti.	1	Si dispone di strumenti adeguati per garantire la riservatezza e l'integrità delle informazioni condivise attraverso i vari canali di segnalazione?	1	Viene misurata l'efficacia delle procedure di segnalazione degli incidenti? Ad esempio indicatori sugli incidenti segnalati attraverso i canali appropriati, tempistica di segnalazione degli incidenti, ecc.	1	-	
	4	-		Sono stati attuati gli obblighi di notifica per i fornitori di servizi digitali in conformità con l'articolo 16 della direttiva NIS? L'articolo 16 prevede che i fornitori di servizi digitali notifichino senza indebito ritardo all'autorità competente o al CSIRT qualsiasi incidente avente un impatto rilevante sulla fornitura di un servizio di cui all'allegato III che essi offrono all'interno dell'Unione.	1	Esiste una piattaforma/uno strumento per facilitare il processo di segnalazione?	0	Si dispone di una tassonomia comune a livello nazionale per la classificazione degli incidenti e le categorie di cause profonde?	0	-	

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
14 – Rafforzare la privacy e la protezione dei dati	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	Vengono eseguiti studi o analisi per identificare aree di miglioramento per proteggere più efficacemente i diritti alla vita privata dei cittadini?	1	L'autorità nazionale per la protezione dei dati è coinvolta in aree problematiche legate alla cibersicurezza (ad es. preparazione di nuove leggi e regolamenti sulla cibersicurezza, misure minime di sicurezza definite)?	1	Vengono promosse migliori pratiche sulle misure di sicurezza e la protezione dei dati fin dalla progettazione per il settore pubblico e/o privato?	1	Vengono eseguite valutazioni regolari per garantire la disponibilità di risorse sufficienti (umane, di bilancio e di strumenti) dedicate alle autorità competenti per la protezione dei dati personali?	1	Sono in atto meccanismi per monitorare gli ultimi sviluppi tecnologici al fine di adattare le linee guida pertinenti e le disposizioni/obblighi giuridici?	1
	2	È stata sviluppata una base giuridica a livello nazionale per applicare il regolamento generale sulla protezione dei dati (regolamento UE n. 2016/679)? Ad esempio, mantenere o introdurre disposizioni più specifiche o limitazioni alle norme del regolamento.	0	-		Vengono avviati programmi di sensibilizzazione e formazione su questo argomento?	1	Vengono incoraggiate le organizzazioni e le imprese a ottenere la certificazione ISO/IEC 27701:2019 sul sistema di gestione delle informazioni personali (PIMS)?	1	È prevista la partecipazione attiva alle iniziative di R&S riguardanti le tecnologie di rafforzamento della tutela della vita privata (PET) o la promozione di tali iniziative?	0
	3	-		-		Le procedure di segnalazione degli incidenti vengono coordinate con le autorità competenti per la protezione dei dati personali?	1	-		-	
	4	-		-		Viene promosso e sostenuto lo sviluppo di standard tecnici sulla sicurezza delle informazioni e sulla privacy? Sono specificamente adattati alle piccole e medie imprese (PMI)?	0	-		-	

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
	5	-		-		Vengono fornite linee guida pratiche e modulabili per sostenere diversi tipi di titolari del trattamento dei dati nel soddisfare i requisiti e gli obblighi giuridici in materia di privacy e protezione dei dati?	0	-		-	

4.1.4 Polo tematico n. 4: Cooperazione

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
15 – Istituire un partenariato pubblico-privato (PPP)	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						
	1	È generalmente riconosciuto che i PPP contribuiscono a incrementare il livello di cibersicurezza nel paese con diversi mezzi? Ad esempio, la condivisione degli interessi verso la crescita del settore del cibersicurezza, la cooperazione nella costruzione di un quadro normativo pertinente per la cibersicurezza, la promozione di R&S, ecc.	1	Si dispone di un piano d'azione nazionale per istituire PPP?	1	Sono stati istituiti partenariati pubblico-privato nazionali?	1	Sono stati istituiti PPP intersettoriali?	1	In funzione degli ultimi sviluppi tecnologici e normativi, si è in grado di adattare o creare PPP?	1
	2	-		Viene stabilita una base legale o contrattuale (leggi specifiche, accordi di non divulgazione, proprietà intellettuale) per esaminare i PPP?	1	Sono stati istituiti PPP specifici per settore?	1	Nei PPP istituiti, ci si concentra anche sulla cooperazione pubblico-pubblico e privato-privato?	1		
	3	-		-		Vengono forniti finanziamenti per la creazione di PPP?	1	Vengono promossi PPP tra le piccole e medie imprese (PMI)?	1	-	

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
15 – Istituire un partenariato pubblico-privato (PPP)	4	-		-		Le istituzioni pubbliche guidano i PPP nel loro complesso? Ad esempio, un unico punto di contatto del settore pubblico che disciplina e coordina il PPP, enti pubblici che concordano preventivamente i risultati da conseguire, linee guida chiare da parte delle amministrazioni pubbliche sulle loro esigenze e limiti al settore privato, ecc.	1	Vengono misurati i risultati dei PPP?	1	-	
	5	-		-		Il paese è membro del partenariato pubblico-privato contrattuale dell'Organizzazione europea per la cibersicurezza (ECSO)?	0	-		-	
	6	-		-		Vi sono uno o più PPP che lavorano su attività dei CSIRT?	0	-		-	
	7					Vi sono uno o più PPP che lavorano su tematiche di protezione delle infrastrutture critiche informatizzate?	0				
	8	-		-		Vi sono uno o più PPP che lavorano sulla sensibilizzazione e sullo sviluppo di competenza in materia di cibersicurezza?	0	-		-	
16 – Istituzionalizzare la cooperazione tra agenzie pubbliche	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
	1	Esistono canali di cooperazione informale tra agenzie pubbliche?	1	Esiste un programma di cooperazione nazionale incentrato sulla cibersicurezza? Ad esempio comitati consultivi, gruppi direttivi, forum, consigli, centri informatici o gruppi di incontro di esperti.	1	Le autorità pubbliche partecipano al programma di cooperazione?	1	Viene assicurata la presenza di canali di cooperazione dedicati alla cibersicurezza almeno tra i seguenti organismi pubblici: servizi di intelligence, attività di contrasto nazionali, autorità responsabili dell'azione penale, attori della pubblica amministrazione, CSIRT nazionali e forze armate?	1	Alle agenzie pubbliche vengono fornite informazioni minime uniformi sui più recenti sviluppi del panorama delle minacce e sulla conoscenza situazionale della cibersicurezza?	1
	2	-		-		Sono state istituite piattaforme di cooperazione per lo scambio di informazioni?	1	Vengono misurati successi e limiti dei diversi programmi di cooperazione nel promuovere una collaborazione efficace?	1	-	
16 – Istituzionalizzare la cooperazione tra agenzie pubbliche	3	-		-		È stato definito l'ambito delle piattaforme di cooperazione (ad es. compiti e responsabilità, numero di aree problematiche)?	1	-		-	
	4	-		-		Vengono organizzate riunioni annuali?	1	-		-	
	5	-		-		Si dispone di meccanismi di cooperazione tra le autorità competenti nelle varie regioni geografiche? Ad esempio rete di corrispondenti per la sicurezza in base alla regione, responsabile della sicurezza informatica nelle camere dell'economia regionali, ecc.	1	-		-	
17 – Impegnarsi nella cooperazione internazionale (non solo con gli Stati membri dell'UE)	a	L'obiettivo è trattato nella NCSS attuale o si pensa di trattarlo nella prossima edizione?	1	Esistono pratiche o attività informali che concorrono al raggiungimento dell'obiettivo in modo non coordinato?	1	Si dispone di un piano d'azione formalmente definito e documentato?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificarne le prestazioni?	1	Sono in atto meccanismi per assicurare che il piano d'azione venga adattato in modo dinamico agli sviluppi ambientali?	1
	b			Sono stati definiti i risultati attesi, i principi guida o le attività chiave del piano d'azione?	1	Si dispone di un piano d'azione con assegnazione e governance delle risorse chiare?	1	Il piano d'azione viene rivisto rispetto all'obiettivo per verificare che gli sia assegnata la giusta priorità e che sia ottimizzato correttamente?	1		
	c			Se pertinente, il piano d'azione è implementato e già efficace con una portata limitata?	0						

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
17 – Impegnarsi nella cooperazione internazionale (non solo con gli Stati membri dell'UE)	1	Si dispone di una strategia di impegno internazionale?	1	Esistono accordi di cooperazione con altri paesi (bilaterali, multilaterali) o partner in altri paesi? Ad esempio condivisione di informazioni, sviluppo di capacità, assistenza, ecc.	1	È previsto lo scambio di informazioni a livello strategico? Ad esempio politica di alto livello, percezione del rischi, ecc.	1	Le agenzie pubbliche nazionali di cibersicurezza del paese sono coinvolte in programmi di cooperazione internazionale?	1	Vengono condotte discussioni su uno o più argomenti nell'ambito di accordi multilaterali?	1
	2	Vi sono canali di cooperazione informali con altri paesi?	1	Esiste un unico punto di contatto in grado di esercitare una funzione di collegamento, per assicurare la cooperazione transfrontaliera con le autorità degli Stati membri (gruppo di cooperazione, rete di CSIRT, ecc.)?	1	Vi è uno scambio informazioni a livello tattico? Ad esempio bollettino sugli autori delle minacce, centri di condivisione e di analisi delle informazioni (ISAC), tattiche, tecniche e procedure (TTP), ecc.	1	Vengono valutati regolarmente gli esiti delle iniziative di cooperazione internazionale?	1	Vengono condotte discussioni su uno o più argomenti nell'ambito di trattati o convenzioni internazionali?	1
	3	La leadership pubblica ha espresso l'intenzione di impegnarsi nella cooperazione internazionale nel campo della cibersicurezza?	1	Vengono assegnati addetti specializzati alla cooperazione internazionale?	1	Esiste uno scambio di informazioni a livello operativo? Ad esempio informazioni sul coordinamento operativo, incidenti in corso, indicatori di compromissione (IOC), ecc.	1	-		Vengono condotte discussioni o negoziazioni su uno o più argomenti all'interno di gruppi internazionali di esperti? Ad esempio la Coalizione globale sulla stabilità del ciberspazio (GCSC), il gruppo di cooperazione NIS dell'ENISA, il gruppo di esperti governativi delle Nazioni Unite sulla sicurezza dell'informazione (GGE), ecc.	1
	4	-		-		Vengono effettuate esercitazioni di cibersicurezza internazionali?	1	-		-	
	5	-		-		Vengono intraprese iniziative internazionali di sviluppo delle capacità? Ad esempio formazione, sviluppo di competenze, elaborazione di procedure standard, ecc.	0	-		-	
	6	-		-		Sono stati stabiliti accordi di mutua assistenza con altri paesi ? Ad esempio attività delle autorità di contrasto, procedimenti legali, condivisione delle capacità di risposta agli incidenti, condivisione di risorse di cibersicurezza, ecc.	0	-		-	

Obiettivo della NCSS	#	Livello 1	R	Livello 2	R	Livello 3	R	Livello 4	R	Livello 5	R
	7	-		-		Sono stati firmati o ratificati trattati o convenzioni internazionali nell'area della cibersicurezza? Ad es. codice di condotta internazionale per la sicurezza delle informazioni, Convenzione sulla criminalità informatica.	0	-		-	

4.2 ORIENTAMENTI PER L'UTILIZZO DEL QUADRO

Questa sezione intende fornire agli Stati membri alcuni orientamenti e raccomandazioni per la presentazione del quadro e la compilazione del questionario. Le raccomandazioni elencate di seguito derivano principalmente dal feedback raccolto dalle interviste con i rappresentanti degli Stati membri.

- **Prevedere attività di coordinamento per raccogliere e consolidare i dati.** La maggior parte degli Stati membri riconosce che eseguire tale esercizio di autovalutazione dovrebbe richiedere circa 15 giorni-persona. Al fine di eseguire l'autovalutazione, occorrerà rivolgersi a una vasta gamma di portatori di interessi diversi. Si raccomanda perciò di destinare il tempo necessario alla fase di preparazione per individuare tutti i portatori di interessi all'interno degli organismi governativi, delle agenzie pubbliche e del settore privato.
- **Identificare un organismo centrale incaricato di completare l'autovalutazione a livello nazionale.** Poiché la raccolta di materiale per tutti gli indicatori dell'NCAF potrebbe coinvolgere molti portatori di interessi, si raccomanda di avere un organismo o un'agenzia centrale incaricati di completare l'autovalutazione fungendo da collegamento e coordinandosi con tutti i portatori di interessi.
- **Usare l'esercizio di valutazione come mezzo di condivisione e comunicazione in merito ai temi della cibersicurezza.** Le lezioni apprese condivise dagli Stati membri hanno mostrato che le discussioni (sotto forma di interviste individuali o workshop collettivi) rappresentano una buona opportunità per promuovere il dialogo sui temi della cibersicurezza e per condividere opinioni comuni e aree di miglioramento. Oltre a mettere in luce i risultati chiave, la condivisione dei risultati può anche contribuire a promuovere i temi della cibersicurezza.
- **Utilizzare la NCSS come ambito per definire gli obiettivi sottoposti alla valutazione.** I 17 obiettivi che compongono l'NCAF sono stati elaborati sulla base degli obiettivi comunemente trattati dagli Stati membri nelle rispettive NCSS. Gli obiettivi trattati nell'ambito della NCSS devono essere usati come mezzo per definire l'ambito della valutazione. La NCSS non deve però limitare la valutazione. Poiché la NCSS si concentra naturalmente sulle priorità, alcune aree sono volutamente omesse da tale strategia. Ciò non implica tuttavia che una data capacità non sia presente. Ad esempio, nel caso in cui un obiettivo specifico sia omesso dalla NCSS, ma il paese disponga di capacità di cibersicurezza al riguardo, la valutazione di tale obiettivo può avere luogo.
- **Quando l'ambito della NCSS evolve, assicurare che l'interpretazione del punteggio rimanga coerente con tale evoluzione.** Il ciclo di vita della NCSS è un processo pluriennale. Le NCSS di alcuni Stati membri vengano in genere applicate con una tabella di marcia da compresa fra 3 e 5 anni e tra le due versioni successive sono apportati cambiamenti in termini di ambito. In tale ottica, occorre prestare particolare attenzione quando si presentano i risultati dell'autovalutazione tra due edizioni della NCSS: i cambiamenti in termini di ambito potrebbero infatti influire sul punteggio di maturità finale. Si raccomanda di confrontare i punteggi sull'intero ambito degli obiettivi strategici da un anno all'altro (vale a dire il punteggio generale complessivo).

Promemoria sul meccanismo di assegnazione del punteggio - esempio sul tasso di copertura

Il meccanismo di assegnazione del punteggio prevede due livelli di punteggio:
(i) un **tasso di copertura generale complessivo** basato sull'elenco completo degli obiettivi strategici presenti nel quadro di autovalutazione e
(ii) **un tasso di copertura specifico complessivo** basato su obiettivi strategici selezionati dallo Stato membro (di solito corrispondenti agli obiettivi presenti nella NCSS di tale paese).

Fin dalla progettazione (cfr. la sezione 3.1 sul meccanismo di assegnazione del punteggio), il tasso di copertura specifico complessivo sarà pari o superiore al tasso di copertura generale complessivo, poiché quest'ultimo può includere obiettivi che non sono trattati dallo Stato membro, abbassando così il tasso di copertura generale complessivo. Quando uno Stato membro aggiunge un nuovo obiettivo, il tasso di copertura complessivo aumenterà (vale a dire che sono trattati più indicatori di maturità), mentre il grado di maturità specifica complessiva può diminuire (nel caso in cui il nuovo obiettivo aggiunto sia in una fase iniziale e abbia quindi un basso livello di maturità).

- **Nella compilazione del questionario di autovalutazione, tenere presente che l'obiettivo primario è sostenere gli Stati membri nello sviluppo delle capacità di cibersicurezza.** Pertanto, quando si compila l'autovalutazione, anche se in alcune situazioni può essere difficile rispondere alla domanda in modo preciso, si raccomanda di scegliere la risposta più generalmente accettata. Se, ad esempio, la risposta a una domanda è SÌ in un certo ambito ma NO in un altro, gli Stati membri dovrebbero considerare che una risposta NO richiede un'azione: un piano di riparazione o un piano per intervenire su un'area di miglioramento da considerare negli sviluppi futuri.

5. TAPPE SUCCESSIVE

5.1 MIGLIORAMENTI FUTURI

Nel corso delle interviste con i rappresentanti degli Stati membri e durante la fase di ricerca a tavolino, sono state individuate anche le seguenti raccomandazioni per migliorare l'attuale quadro di valutazione delle capacità a livello nazionale, come potenziali evoluzioni future.

- **Sviluppare il sistema di assegnazione del punteggio per consentire una maggiore accuratezza.** Ad esempio, si potrebbe introdurre una percentuale di copertura al posto della risposta binaria SÌ/NO per meglio considerare la complessità del consolidamento delle capacità a livello nazionale. Come primo passo, è stato scelto un approccio semplice con risposte SÌ/NO.
- **Introdurre metriche quantitative per misurare l'efficacia della NCSS degli Stati membri.** Il quadro di valutazione delle capacità a livello nazionale si concentra infatti sulla valutazione del livello di maturità delle capacità di cibersicurezza degli Stati membri. Ciò potrebbe essere integrato da metriche per misurare l'efficacia delle attività e dei piani d'azione attuati dagli Stati membri per creare le suddette capacità. Non è sembrato realistico sviluppare tali metriche di efficacia nella fase attuale, considerate la scarsità di feedback dal campo, la difficoltà a trovare indicatori significativi che colleghino i risultati prodotti con l'attuazione della NCSS e la difficoltà di creare indicatori realistici che possano essere successivamente raccolti. Tuttavia, rimane un tema da considerare in futuro.
- **Passaggio da un esercizio di autovalutazione a un approccio di valutazione.** Una potenziale evoluzione futura del quadro potrebbe essere lo spostamento verso un approccio di valutazione al fine di valutare la maturità delle capacità di cibersicurezza informatica degli Stati membri. Avvalersi di terzi per l'esecuzione della valutazione potrebbe infatti consentire di minimizzare potenziali distorsioni.

ALLEGATO A – PANORAMICA DEI RISULTATI DELLA RICERCA A TAVOLINO

L'allegato A fornisce una sintesi del precedente lavoro svolto dall'ENISA sulla NCSS e una revisione dei modelli di maturità sulla capacità di cibersicurezza disponibili pubblicamente. Per la selezione e la revisione dei modelli sono state prese in considerazione le seguenti ipotesi:

- Non tutti i modelli si basano su una metodologia di ricerca rigorosa.
- La struttura e i risultati dei modelli non sono sempre spiegati in modo esauriente con collegamenti chiari fra i diversi elementi che caratterizzano ogni modello.
- Alcuni modelli non forniscono dettagli sul processo di sviluppo, sulla struttura e sulla metodologia di valutazione.
- Altri modelli e strumenti da noi trovati non offrono dettagli in merito alla struttura e al contenuto e quindi non sono elencati.
- La selezione dei modelli per la revisione si basa sulla distribuzione geografica. L'attenzione sarà incentrata principalmente sui modelli di maturità della capacità di cibersicurezza costruiti per valutare le prestazioni dei paesi europei. È tuttavia importante ampliare la distribuzione geografica per analizzare le buone pratiche nella costruzione di modelli di maturità in tutto il mondo.

La presente revisione sistematica dei pertinenti modelli di maturità accessibili pubblicamente sulla capacità di cibersicurezza è stata condotta utilizzando un quadro di analisi personalizzato, basato sulla metodologia definita da Becker per lo sviluppo di modelli di maturità ([22]). Per ogni modello di maturità esistente sono stati analizzati i seguenti elementi:

- **nome del modello di maturità:** nome del modello di maturità e riferimenti principali;
- **ente di origine:** ente pubblico o privato incaricato della progettazione del modello;
- **finalità generale e obiettivo:** ambito generale del modello e gli obiettivi previsti;
- **numero e definizione dei livelli:** numero di livelli di maturità del modello e loro descrizione generale;
- **numero e nome degli attributi:** numero e nome degli attributi utilizzati dal modello di maturità. L'analisi degli attributi ha un triplice obiettivo:
  - suddividere il modello di maturità in sezioni di facile comprensione;
  - aggregare diversi attributi in gruppi di attributi che soddisfano lo stesso obiettivo e
  - fornire diversi punti di vista sull'argomento del livello di maturità;
- **metodo di valutazione:** metodo di valutazione del modello di maturità;
- **rappresentazione dei risultati**: definire il metodo di visualizzazione per i risultati de modello di maturità. La logica dietro questa fase è che i modelli di maturità tendono a non

([22]) J. Becker, R. Knackstedt, e J. Pöppelbuß, «Developing Maturity Models for IT Management: A Procedure Model and its Application», Business & Information Systems Engineering, vol. 1, n. 3, pp. 213–222, giugno 2009.
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

avere successo se sono troppo complessi e quindi, la modalità di rappresentazione deve soddisfare esigenze pratiche.

Precedenti lavori sulla NCSS

L'ENISA ha pubblicato nel 2012 due documenti sul tema della NCSS nell'ambito dei propri sforzi iniziali. In primo luogo, la guida pratica sulla fase di sviluppo e di attuazione della NCSS ([23]) proponeva una serie di azioni concrete per l'attuazione efficiente di una NCSS e ne presentava il ciclo di vita in quattro fasi: sviluppo della strategia, esecuzione della strategia, valutazione della strategia e mantenimento della strategia. In secondo luogo, il documento dal titolo «Setting the course for national efforts to strengthen security in cyberspace» ([24]) delineava la situazione delle strategie di cibersicurezza nell'UE e oltre nel 2012 e proponeva agli Stati membri di individuare temi comuni e differenze tra le rispettive NCSS.

Nel 2014 è stato pubblicato il primo quadro dell'ENISA per la valutazione delle NCSS di uno Stato membro ([25]). Tale quadro contiene raccomandazioni e buone prassi, oltre a una serie di strumenti di sviluppo delle capacità per la valutazione di una NCSS (ad esempio obiettivi identificati, contributi, risultati prodotti, indicatori chiave di prestazione, ecc.). Tali strumenti sono adattati alle varie esigenze dei paesi a diversi livelli di maturità nella loro pianificazione strategica. Nello stesso anno l'ENISA ha pubblicato la mappa interattiva online delle NCSS ([26]), che permette agli utenti di consultare rapidamente le NCSS di tutti gli Stati membri e dei paesi EFTA, compresi i loro obiettivi strategici e i buoni esempi di attuazione. Concepita inizialmente come un archivio di NCSS (2014), è stata aggiornata con esempi di attuazione nel 2018, e dal 2019 la mappa funge da *polo d'informazione* per centralizzare i dati forniti dagli Stati membri in merito agli sforzi compiuti per migliorare la sicurezza informatica nazionale.

Pubblicata nel 2016, la guida «NCSS Good Practice Guide» ([27]) individua quindici obiettivi strategici; inoltre, analizza lo stato di attuazione della NCSS di ogni Stato membro e identifica varie lacune e sfide riguardo a tale attuazione.

Nel 2018 l'ENISA ha poi pubblicato il «National Cybersecurity Strategies Evaluation Tool» ([28]), uno strumento interattivo di autovalutazione per aiutare gli Stati membri a valutare le priorità strategiche e gli obiettivi relativi alla loro NCSS. Attraverso una serie di semplici domande, lo strumento fornisce agli Stati membri raccomandazioni specifiche per l'attuazione di ciascun obiettivo. Infine, le «Good practices in innovation on Cybersecurity under the NCSS» ([29]), pubblicate nel 2019, presentano il tema dell'innovazione nella cibersicurezza nell'ambito della NCSS. Il documento illustra le sfide e le buone prassi in diverse dimensioni dell'innovazione, sulla base della percezione di esperti in materia, al fine di contribuire alla stesura dei futuri obiettivi strategici innovativi.

([23]) NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
([24]) NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
([25]) An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
([26]) National Cybersecurity Strategies - Interactive Map (ENISA, 2014, aggiornata nel 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
([27]) Si tratta dell'aggiornamento della guida del 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
([28]) National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
([29]) https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

A.1 Cybersecurity Capacity Maturity Model for Nations (CMM)

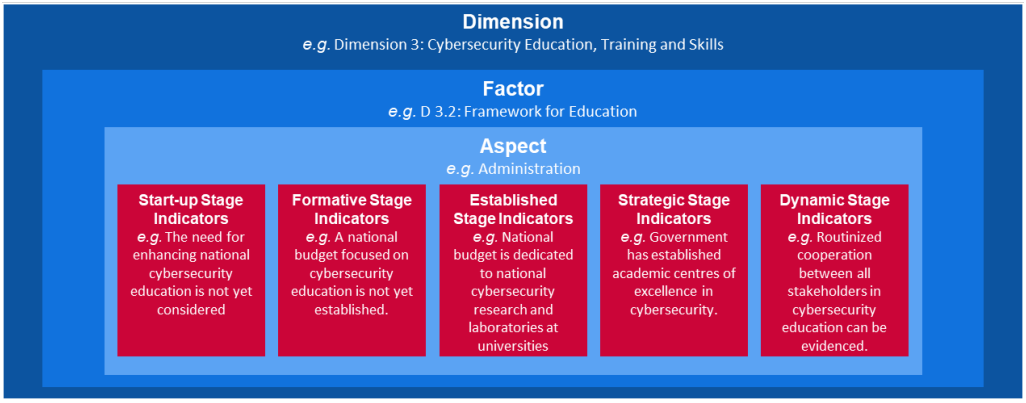
Il Cybersecurity Capacity Maturity Model for Nations (CMM, modello di maturità della capacità di cibersicurezza per le nazioni) è stato messo a punto dal Global Cyber Security Capacity Centre (Capacity Centre), nell'ambito della Oxford Martin School dell'Università di Oxford. L'obiettivo del Capacity Centre è aumentare la portata e l'efficacia dello sviluppo delle capacità di cibersicurezza, sia all'interno del Regno Unito sia a livello internazionale, attraverso l'attuazione del Cybersecurity Capacity Maturity Model (CMM). Il CMM è direttamente rivolto ai paesi che desiderano aumentare la propria capacità di cibersicurezza nazionale. Implementato inizialmente nel 2014, il CMM è stato rivisto nel 2016 a seguito del suo utilizzo nella revisione di 11 capacità di cibersicurezza nazionali.

Attributi/Dimensioni

Secondo il CMM, la capacità di cibersicurezza è costituita da **cinque dimensioni** che rappresentano i poli tematici di tale capacità. Ogni polo tematico rappresenta una diversa «lente» di ricerca attraverso la quale è possibile studiare e comprendere la capacità di cibersicurezza. All'interno delle cinque dimensioni, i **fattori** descrivono i dettagli del possesso della capacità di cibersicurezza. Questi dettagli sono elementi che contribuiscono a incrementare il grado di maturità della capacità di cibersicurezza all'interno di ogni dimensione. Per ogni fattore, diversi **aspetti** rappresentano diverse componenti del fattore. Gli aspetti rappresentano un metodo organizzativo per dividere gli indicatori in poli tematici più piccoli, di più facile comprensione. Ogni aspetto viene poi valutato attraverso **indicatori** per descrivere i passi, le azioni o gli elementi che sono indicativi di uno specifico stadio di maturità (definito nella sezione seguente) all'interno di un aspetto, fattore e dimensione distinti.

La struttura gerarchica dei termini sopra menzionati è illustrata nella figura seguente.

Figura 4. Esempio di indicatori CMM



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Dimensione es. Dimensione 3: Istruzione, formazione e competenze di cibersicurezza
Factor e.g. D 3.2: Framework for Education	Fattore es. D 3.2: Quadro per l'istruzione
Aspect e.g. Administration	Aspetto es. Amministrazione
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Indicatori della fase di avvio es. non è ancora stata considerata la necessità di migliorare l'istruzione nazionale in materia di cibersicurezza

Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Indicatori della fase di crescita es. non è ancora stato costituito un budget nazionale incentrato sull'istruzione in materia di cibersicurezza
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Indicatori della fase consolidata es. il budget nazionale è dedicato alla ricerca e ai laboratori nazionali sulla cibersicurezza presso le università
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Indicatori della fase strategica es. il governo ha istituito centri accademici di eccellenza in materia di cibersicurezza.
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Indicatori della fase dinamica es. si può attestare una cooperazione di routine tra tutti i portatori di interessi nell'educazione in materia di cibersicurezza.

Le cinque dimensioni sono illustrate in dettaglio di seguito:

i ideare una politica e una strategia di cibersicurezza (6 fattori);
ii incoraggiare una cultura della cibersicurezza responsabile all'interno della società (5 fattori);
iii sviluppare la conoscenza della cibersicurezza (3 fattori);
iv creare quadri giuridici e normativi efficaci (3 fattori) e
v controllare i rischi attraverso norme, organizzazioni e tecnologie (7 fattori).

Livelli di maturità

Il CMM utilizza **5 livelli di maturità** per determinare il grado di progresso raggiunto da un paese in relazione a un certo fattore/aspetto della capacità di cibersicurezza. Questi livelli offrono una panoramica della capacità di cibersicurezza esistente:

- **avvio**: in questa fase non esiste alcuna maturità di cibersicurezza oppure è allo stadio embrionale. È possibile che vi siano discussioni iniziali sullo sviluppo di capacità di cibersicurezza, ma non sono state intraprese azioni concrete. In questa fase non vi sono prove osservabili;
- **crescita**: alcune caratteristiche degli aspetti hanno iniziato a crescere e ad essere formulate, ma potrebbero essere ad-hoc, disorganizzate, mal definite, o semplicemente «nuove». Tuttavia, le prove di tale attività possono essere chiaramente dimostrate.
- **consolidato**: gli elementi dell'aspetto sono in atto e funzionano. La relativa allocazione delle risorse, tuttavia, non è sottoposta a valutazione ben ponderata. Sono state compiute poche decisioni di compromesso riguardo all'investimento «relativo» nei vari elementi dell'aspetto. L'aspetto è tuttavia funzionale e definito;
- **strategico**: sono state compiute scelte riguardo a quali parti dell'aspetto sono importanti e quali sono meno importanti per la specifica organizzazione o nazione. La fase strategica rispecchia le scelte compiute subordinatamente alle particolari circostanze della nazione o dell'organizzazione;
- **dinamico**: in questa fase, vi sono chiari meccanismi in atto per modificare la strategia a seconda delle circostanze prevalenti, ad es. tecnologia dell'ambiente delle minacce, conflitto globale o cambiamento significativo in un'area di interesse (ad es. criminalità informatica o privacy). Le organizzazioni dinamiche hanno sviluppato metodi per modificare le strategie con facilità. Il rapido processo decisionale, la riallocazione delle risorse e la costante attenzione all'ambiente in evoluzione sono caratteristiche di questa fase.

Metodo di valutazione

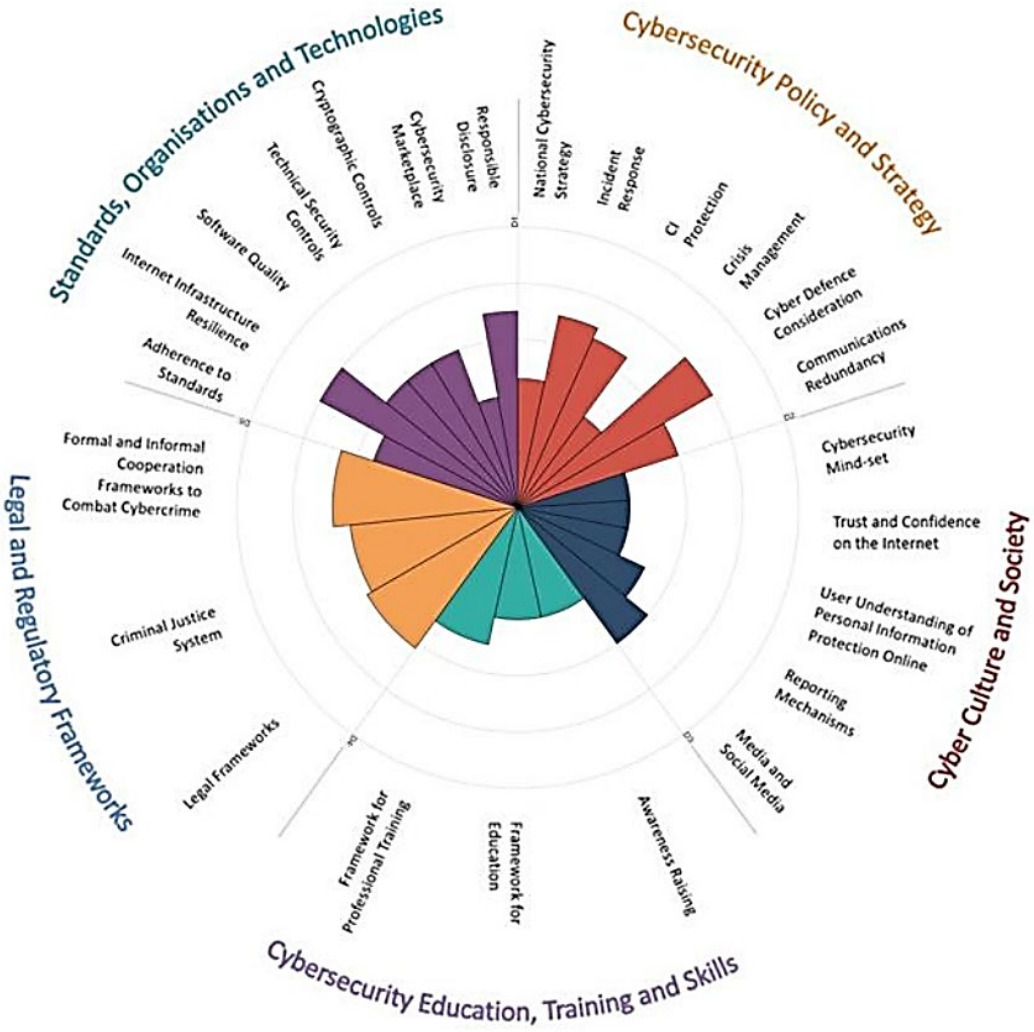
Poiché il Capacity Centre non ha una comprensione esaustiva e approfondita di ogni contesto nazionale in cui il modello viene utilizzato, lavora a fianco delle organizzazioni internazionali, dei ministeri o delle organizzazioni ospitanti all'interno del rispettivo paese per esaminare la maturità della capacità di cibersicurezza. Per valutare il livello di maturità delle cinque

dimensioni incluse nel CMM, il Capacity Centre e l'organizzazione ospitante si incontrano con i portatori di interessi nazionali pertinenti del settore pubblico e privato nell'arco di due o tre giorni per condurre dei gruppi specifici sulle dimensioni del CMM. Ogni dimensione viene discussa almeno due volte da diversi gruppi di portatori di interessi. In tal modo vendono condivisi preliminarmente i dati al fine della successiva valutazione.

Modalità di rappresentazione dei risultati

Il CCM fornisce una panoramica del livello di maturità di ogni paese attraverso un grafico a radar composto da cinque sezioni, una per ogni dimensione. Ogni dimensione rappresenta un quinto del grafico, con i cinque stadi di maturità per ogni fattore che si estendono dal centro del grafico verso l'esterno; come illustrato di seguito, «avvio» è il più vicino al centro del grafico mentre il livello «dinamico» si trova sull'esterno.

Figura 5. CMM: Panoramica dei risultati



Standards, Organisations and Technologies	Norme, organizzazioni e tecnologie
Legal Regulatory Frameworks	Quadri giuridici e normativi
Cybersecurity Education, Training and Skills	Istruzione, formazione e competenze di cibersicurezza
Cybersecurity Policy and Strategy	Politica e strategia di cibersicurezza
Cyber Culture and Society	Cultura e società in materia di informatica
Responsible Disclosure	Divulgazione responsabile
Cybersecurity market place	Mercato della cibersicurezza
Cryptographic Controls	Controlli crittografici
Technical Security Controls	Controlli di sicurezza tecnica
Software Quality	Qualità del software

Internet Infrastructure Resilience	Resilienza delle infrastrutture internet
Adherence to Standards	Adesione alle norme
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Quadri di cooperazione formali e informali per combattere la criminalità informatica
Criminal Justice System	Sistema di giustizia penale
Legal Frameworks	Quadri giuridici
Framework for Professional Training	Quadro per la formazione professionale
Framework for Education	Quadro per l'istruzione
Awareness Raising	Sensibilizzazione
Media and Social Media	Mezzi di comunicazione e social media
Reporting Mechanisms	Meccanismi di segnalazione
User Understanding of Personal Information Protection Online	Comprensione degli utenti della protezione dei dati personali online
Trust and Confidence on the Internet	Fiducia e sicurezza su internet
Cybersecurity Mind-set	Mentalità di cibersicurezza
Communications Redundancy	Ridondanza delle comunicazioni
Cyber Defence Consideration	Considerazione della ciberdifesa
Crisis Management	Gestione delle crisi
CI Protection	Protezione delle infrastrutture critiche
Incident Response	Risposta agli incidenti
National Cybersecurity Strategy	Strategie nazionale per la cibersicurezza

Global Cyber Security Capacity Centre Oxford Martin School, Università di Oxford, 2017.

A.2 Cybersecurity Capability Maturity Model (C2M2)

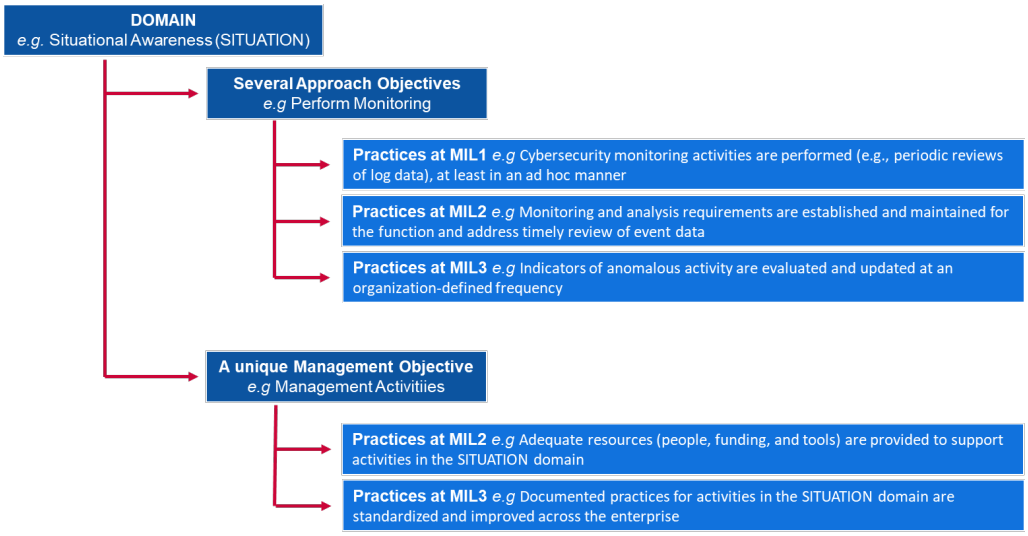
Il Cybersecurity Capacity Maturity Model (C2M2, modello di maturità delle capacità di cibersicurezza) è stato elaborato dal Dipartimento dell'energia degli Stati Uniti in collaborazione con esperti del settore pubblico e privato. L'obiettivo del Capacity Centre è aiutare le organizzazioni di tutti i settori, tipi e dimensioni a valutare e apportare miglioramenti ai loro programmi di cibersicurezza e a rafforzare la loro resilienza operativa. Il C2M2 è incentrato sull'attuazione e sulla gestione delle pratiche di cibersicurezza associate alle risorse di informazioni, tecnologia dell'informazione (IT) e alla tecnologia delle operazioni (OT) e agli ambienti in cui operano. Il C2M2 definisce i modelli di maturità come: «un insieme di caratteristiche, attributi, indicatori o schemi che rappresentano la capacità e l'avanzamento in una particolare disciplina». Inizialmente implementato nel 2014, il C2M2 è stato rivisto nel 2019.

Attributi/Dimensioni

Il C2M2 individua **dieci domini** che rappresentano un gruppo logico di pratiche di cibersicurezza. Ogni insieme di pratiche rappresenta le attività che un'organizzazione può eseguire per costituire e far maturare la capacità nel dominio. Ogni dominio è poi associato a un **obiettivo di gestione unico** e a **diversi obiettivi di approccio**. All'interno degli obiettivi sia relativi all'approccio sia di gestione vengono specificate **diverse pratiche** per descrivere le attività istituzionalizzate.

La relazione tra queste nozioni è riassunta di seguito:

Figura 6. Esempi dell'indicatore C2M2



Domain eg Situational Awareness (SITUATION)
Several Approaches Objectives e.g. Perform Monitoring
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner

Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data

Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency
A unique Management Objectve e.g. Management Activities
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain

Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise

Dominio es. conoscenza situazionale (SITUAZIONE)
Diversi obiettivi di approccio es. eseguire il monitoraggio
Prassi a livello MIL1 es. vengono eseguite attività di monitoraggio della cibersicurezza (ad es. revisioni periodiche dei dati di registro) almeno in modalità ad hoc
Prassi a livello MIL2 es. i requisiti di monitoraggio e analisi sono stabiliti e mantenuti per la funzione e affrontano la revisione tempestiva dei dati degli eventi
Prassi a livello MIL3 es. gli indicatori di attività anomala sono valutati e aggiornati con una frequenza definita dall'organizzazione
Un obiettivo di gestione unico, es. attività di gestione
Prassi a livello MIL2 es. vengono fornite risorse adeguate (persone, finanziamenti e strumenti) per sostenere le attività nel dominio SITUAZIONE

Prassi a livello MIL3 es. le pratiche documentate per le attività nel dominio SITUAZIONE sono standardizzate e migliorate in tutta l'impresa

I dieci domini sono illustrati in dettaglio di seguito:

i Gestione del rischio (RISCHIO)
ii Gestione di risorse, cambiamento e configurazione (ASSET)
iii Gestione dell'identità e dell'accesso (ACCESSO)
iv Gestione delle minacce e delle vulnerabilità (MINACCIA)
v Conoscenza situazionale (SITUAZIONE)
vi Risposta agli eventi e agli incidenti (RISPOSTA)
vii Gestione della catena di fornitura e delle dipendenze esterne (DIPENDENZE)
viii Gestione della forza lavoro (FORZA LAVORO)
ix Architettura di cibersicurezza (ARCHITETTURA)
x Gestione del programma di cibersicurezza (PROGRAMMA)

Livelli di maturità

Il modello C2M2 utilizza **4 livelli di maturità** (denominati *Maturity Indicator Levels*, MIL) per determinare una duplice progressione della maturità: una progressione di approccio e una progressione di gestione. I MIL vanno da MIL0 a MIL3 e vengono applicati in modo indipendente ad ogni dominio.

- **MIL0**: Non sono eseguite prassi.
- **MIL1**: Vengono eseguite prassi iniziali vengono ma potrebbero essere ad hoc.
- **MIL2**: Caratteristiche della gestione:
  - le prassi sono documentate;
  - vengono fornite risorse adeguate per sostenere il processo;
  - il personale che esegue le prassi ha competenze e conoscenze adeguate e

- la responsabilità e l'autorità per l'esecuzione delle prassi sono assegnate.

Caratteristiche di approccio:

- le pratiche sono più complete o avanzate rispetto a MIL1.

- **MIL3**: Caratteristiche della gestione:
  - le attività sono guidate da politiche (o altre direttive dell'organizzazione);
  - gli obiettivi di performance per le attività del dominio sono stabiliti e monitorati per tenere traccia del conseguimento e
  - le pratiche documentate per le attività del dominio sono standardizzate e migliorate in tutta l'impresa.

  Caratteristiche di approccio:
  - Le pratiche sono più complete o avanzate rispetto a MIL2.

Metodo di valutazione

Il C2M2 è concepito per essere utilizzato con una **metodologia di autovalutazione** e un insieme di strumenti (disponibile su richiesta) per consentire a un'organizzazione di misurare e migliorare il suo programma di cibersicurezza. Un'autovalutazione eseguita utilizzando l'insieme di strumenti può essere completata in un giorno, ma è possibile adattare l'insieme di strumenti per uno sforzo di valutazione più rigoroso. Inoltre, il C2M2 può essere utile per guidare lo sviluppo di un nuovo programma di cibersicurezza.

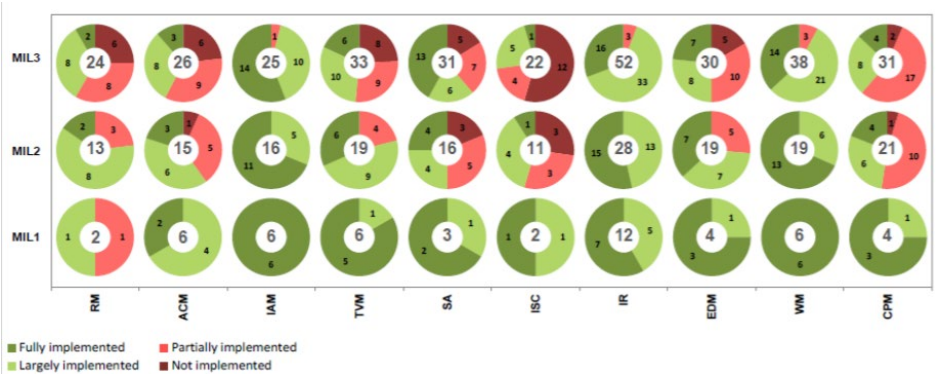
Il contenuto del modello è presentato a un livello di astrazione elevato, in modo che possa essere interpretato da organizzazioni di vari tipi, strutture, dimensioni e settori. L'ampio uso del modello da parte di un settore può favorire l'analisi comparativa delle capacità di cibersicurezza del settore stesso.

Modalità di rappresentazione dei risultati

Il C2M2 fornisce un report del punteggio di valutazione generato dai risultati dell'indagine. Il report presenta i risultati in due panoramiche: la panoramica Obiettivo, che mostra le risposte alle domande sulle pratiche per ogni dominio e i suoi obiettivi, e la panoramica Dominio, che mostra le risposte per tutti i domini e MIL. Entrambe le panoramiche si basano su un sistema di rappresentazione caratterizzato da diagrammi a torta (o «ciambelle»), uno per ogni risposta, e un meccanismo di punteggio «a semaforo». Come illustrato nella Figura 7, i settori rossi in un diagramma a ciambella mostrano il calcolo del numero di domande del sondaggio per le quali è stato risposto «non attuato» (rosso scuro) o «parzialmente attuato» (rosso chiaro). I settori verdi mostrano il numero di domande per le quali è stato risposto «ampiamente attuato» (verde chiaro) o «completamente attuato» (verde scuro).

La Figura 7 di seguito è un esempio di una scheda di punteggio al termine di una valutazione del grado di maturità. Sull'asse X vi sono i 10 domini del C2M2 e sull'asse Y i livelli di maturità (MIL). Osservando il diagramma e considerando il dominio di gestione del rischio (Risk Management, RM), è possibile notare tre diagrammi a torta, uno corrispondente a ogni livello di maturità: MIL1, MIL2 e MIL3. Per il dominio di gestione del rischio, il diagramma evidenzia che vi sono due elementi da valutare per raggiungere il primo livello di maturità, MIL1. In questo caso, un punteggio «ampiamente attuato» e un punteggio «parzialmente attuato». Per il secondo livello di maturità, MIL2, il modello prevede 13 elementi da valutare. Due di questi 13 elementi appartengono al primo livello, MIL1, e 11 al secondo livello, MIL2. Lo stesso vale per il terzo livello MIL3.

Figura 7. C2M2 – Esempio di panoramica del dominio



Fully implemented	Completamente attuato
Largely implemented	Ampiamente attuato
Partially implemented	Parzialmente attuato
Not implemented	Non attuato
MIL1	MIL1
MIL2	MIL2
MIL3	MIL3
RM	Gestione del rischio
ACM	Gestione di asset, cambiamento e configurazione
IAM	Gestione dell'identità e dell'accesso
TVM	Gestione delle minacce e delle vulnerabilità
SA	Conoscenza situazionale
ISC	Condivisione di informazioni e comunicazione
IR	Risposta agli eventi e agli incidenti
EDM	Gestione della catena di fornitura e delle dipendenze esterne
WM	Gestione della forza lavoro
CPM	Gestione del programma di cibersicurezza

Fonte: Dipartimento dell'energia degli Stati Uniti, Office of electricity delivery and energy reliability, 2015.

A.3 Framework for Improving Critical Infrastructure Cybersecurity

Il Framework for Improving Critical Infrastructure Cybersecurity [quadro per il miglioramento della cibersicurezza nelle infrastrutture critiche] è stato sviluppato dall'Istituto nazionale per gli standard e la tecnologia (NIST). È incentrato sull'orientamento delle attività di cibersicurezza e sulla gestione dei rischi all'interno di un'organizzazione. Si rivolge a tutti i tipi di organizzazioni indipendentemente dalle dimensioni, dal grado di rischio connesso alla cibersicurezza o dalla complessità della sicurezza informatica. Trattandosi di un quadro e non di un modello, è costruito in modo diverso dai modelli analizzati in precedenza.

Il quadro si compone di tre parti: il nucleo del quadro (Framework Core), i livelli di attuazione (Implementation Tiers) e i profili del quadro (Framework Profiles).

- Il **nucleo del quadro** è un insieme di attività di cibersicurezza, risultati desiderati e riferimenti applicabili che sono comuni a tutti i settori delle infrastrutture critiche. Sono simili agli attributi o alle dimensioni presenti nei modelli di maturità delle capacità di cibersicurezza.
- I **livelli di attuazione del quadro** («livelli») forniscono il contesto in merito al modo in cui un'organizzazione considera il rischio connesso alla cibersicurezza e ai processi in atto per gestire tale rischio. I livelli, compresi in un intervallo da parziale (livello 1) ad adattivo (livello 4), descrivono un grado crescente di rigore e sofisticatezza nelle pratiche di gestione del rischio connesso alla cibersicurezza. Tali livelli non rappresentano livelli di maturità, sono piuttosto intesi a fornire sostegno al processo decisionale dell'organizzazione riguardo alla modalità di gestione del rischio connesso alla cibersicurezza, nonché riguardo a quali dimensioni dell'organizzazione sono di maggiore priorità e potrebbero ricevere risorse aggiuntive.
- Un **profilo del quadro** («profilo») rappresenta i risultati basati sulle esigenze operative che un'organizzazione ha selezionato dalle categorie e sottocategorie del quadro. Il profilo può essere delineato relativamente all'allineamento di norme, linee guida e pratiche al nucleo del quadro in un particolare scenario di attuazione. I profili possono

essere usati per individuare opportunità di miglioramento della posizione di sicurezza informatica, confrontando il profilo «attuale» con quello «obiettivo» (lo stato futuro desiderato).

Nucleo del quadro

Il nucleo del quadro consiste di cinque **funzioni**. Considerate nel loro complesso, queste funzioni forniscono una panoramica strategica di alto livello del ciclo di vita della gestione del rischio connesso alla cibersicurezza di un'organizzazione. Il nucleo del quadro identifica poi le **categorie** e le **sottocategorie** chiave sottostanti per ogni funzione e le abbina a riferimenti informativi di esempio, come norme, linee guida e pratiche esistenti per ogni sottocategoria.

Le funzioni e le categorie sono illustrate in dettaglio di seguito:

i **Identificare**: sviluppare una comprensione a livello di organizzazione della modalità di gestione dei rischi di cibersicurezza per sistemi, persone, risorse, dati e capacità.
- Sottocategorie: gestione delle risorse; ambiente aziendale; governance; valutazione del rischio; strategia di gestione del rischio

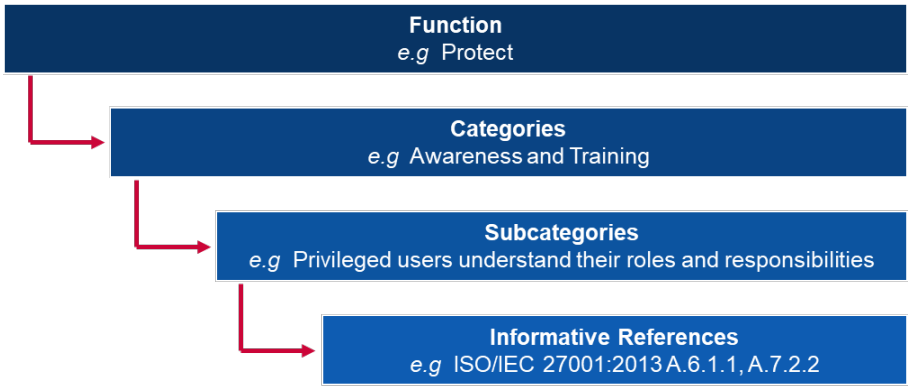
ii **Proteggere**: sviluppare e attuare salvaguardie appropriate per assicurare la fornitura di servizi critici.
- Sottocategorie: gestione dell'identità e controllo degli accessi; sensibilizzazione e formazione; sicurezza dei dati; processi e procedure di protezione delle informazioni; manutenzione; tecnologia di protezione

iii **Rilevare**: sviluppare e implementare attività appropriate per identificare il verificarsi di un evento di cibersicurezza.
- Sottocategorie: anomalie ed eventi; controllo continuo della sicurezza; processi di rilevazione.

iv **Rispondere**: sviluppare e implementare attività appropriate per intervenire riguardo a un incidente di cibersicurezza rilevato.
- Sottocategorie: pianificazione della risposta; comunicazioni; analisi; mitigazione; miglioramenti.

v **Recuperare**: sviluppare e implementare attività appropriate per mantenere piani di resilienza e per ripristinare le capacità o i servizi eventualmente compromessi a causa di un incidente di cibersicurezza.
- Sottocategorie: pianificazione del recupero; miglioramenti; comunicazioni

Figura 8. Esempio del Framework for Improving Critical Infrastructure Cybersecurity



Function e.g Project
Categories e.g Awarness and Training
Subcategories e.g Privileged users understand their roles and responsibilities
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Funzione es. proteggere
Categorie es. sensibilizzazione e formazione
Sottocategorie es. gli utenti privilegiati comprendono i loro ruoli e le loro responsabilità
Riferimenti informativi es. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Livelli

Il Framework for Improving Critical Infrastructure Cybersecurity presenta **4 livelli**, ciascuno dei quali è definito su tre assi: processo di gestione del rischio, programma integrato di gestione del

rischio e partecipazione esterna. I livelli non corrispondono a livelli di maturità, ma costituiscono un quadro di supporto per fornire alle organizzazioni una contestualizzazione delle proprie visioni del rischio connesso alla cibersicurezza e dei processi in atto per gestire tale rischio.

- **Livello 1: parziale**
  - **Processo di gestione del rischio**: le pratiche di gestione del rischio connesso alla cibersicurezza dell'organizzazione non sono formalizzate e il rischio è gestito ad hoc e talvolta in modo reattivo.
  - **Programma integrato di gestione del rischio**: esiste una consapevolezza limitata del rischio connesso alla cibersicurezza a livello di organizzazione. L'organizzazione attua la gestione del rischio connesso alla cibersicurezza in modo irregolare, caso per caso, ed è possibile che non disponga di processi che permettano di condividere le informazioni sulla cibersicurezza al suo interno.
  - **Partecipazione esterna**: l'organizzazione non comprende il proprio ruolo nell'ecosistema più ampio per quanto riguarda le sue dipendenze o i suoi dipendenti. L'organizzazione non è in genere consapevole dei rischi informatici della catena di fornitura per i prodotti e i servizi che fornisce e che utilizza.
- **Livello 2: consapevole dei rischi**
  - **Processo di gestione del rischio**: le pratiche di gestione del rischio sono approvate dalla direzione, ma potrebbero non essere consolidate come politiche a livello dell'intera organizzazione.
  - **Programma integrato di gestione del rischio**: esiste una consapevolezza del rischio connesso alla cibersicurezza a livello di organizzazione, ma non è stato stabilito un approccio alla relativa gestione che coinvolga l'intera organizzazione. La valutazione del rischio informatico delle risorse dell'organizzazione ed esterni viene effettuata, ma in genere non è ripetibile o ricorrente.
  - **Partecipazione esterna**: in generale, l'organizzazione comprende il proprio ruolo nell'ecosistema più ampio per quanto riguarda le proprie dipendenze o i propri dipendenti, ma non entrambi. Inoltre, l'organizzazione è consapevole dei rischi informatici della catena di fornitura associati ai prodotti e ai servizi che fornisce e utilizza, ma non agisce in modo coerente o formale in base a tali rischi.
- **Livello 3: ripetibile**
  - **Processo di gestione del rischio**: le pratiche di gestione del rischio dell'organizzazione sono formalmente approvate ed espresse come politica. Le pratiche di cibersicurezza dell'organizzazione vengono regolarmente aggiornate, in base all'applicazione dei processi di gestione del rischio, ai cambiamenti dei requisiti di business/missione e all'evoluzione del panorama delle minacce e della tecnologia.
  - **Programma integrato di gestione del rischio**: esiste un approccio a livello di organizzazione alla gestione del rischio connesso alla cibersicurezza. Le politiche, i processi e le procedure che tengono conto del rischio vengono definiti, attuati come previsto e rivisti. Gli alti dirigenti garantiscono che la cibersicurezza sia presa in considerazione in tutte le linee operative dell'organizzazione.
  - **Partecipazione esterna**: l'organizzazione comprende il proprio ruolo, dipendenze e dipendenti nell'ecosistema più ampio e potrebbe contribuire a una più diffusa comprensione dei rischi da parte della comunità. L'organizzazione è consapevole dei rischi informatici della catena di fornitura associati ai prodotti e ai servizi che fornisce e che utilizza.
- **Livello 4: adattivo**
  - **Processo di gestione del rischio**: l'organizzazione adatta le proprie pratiche di cibersicurezza in base alle attività di cibersicurezza precedenti e attuali, comprese le lezioni apprese e gli indicatori predittivi.
  - **Programma integrato di gestione del rischio**: esiste un approccio a livello di organizzazione alla gestione del rischio connesso alla cibersicurezza che si avvale di politiche, processi e procedure che tengono conto del rischio per affrontare potenziali eventi di sicurezza informatica.
  - **Partecipazione esterna**: l'organizzazione comprende il proprio ruolo, dipendenze e dipendenti nell'ecosistema più ampio e contribuisce a una più diffusa comprensione dei rischi da parte della comunità.

Metodo di valutazione

Il Framework for Improving Critical Infrastructure Cybersecurity è destinato alle organizzazioni che vogliono eseguire un'autovalutazione del rischio, al fine di rendere il loro approccio alla cibersicurezza e i relativi investimenti più razionali, efficaci e utili. Per esaminare l'efficacia degli investimenti, un'organizzazione deve avere innanzitutto una chiara comprensione dei propri obiettivi, della relazione tra tali obiettivi e dei risultati di cibersicurezza di supporto. I risultati del nucleo del quadro supportano l'autovalutazione dell'efficacia degli investimenti e delle attività di cibersicurezza.

A.4 Qatar Cybersecurity Capability Maturity Model (Q-C2M2)

Il Qatar Cybersecurity Capability Maturity Model (Q-C2M2, modello di maturità delle capacità di cibersicurezza del Qatar) è stato elaborato dal College of Law dell'Università del Qatar nel 2018. Il Q-C2M2 si basa su vari modelli esistenti per costruire una metodologia di valutazione completa per migliorare il quadro di cibersicurezza del Qatar.

Attributi/Dimensioni

Il Q-C2M2 adotta l'approccio del quadro dell'Istituto nazionale per gli standard e la tecnologia (NIST), che prevede l'utilizzo di cinque funzioni fondamentali come domini principali del modello. Le cinque funzioni fondamentali sono applicabili nel contesto del Qatar, essendo comuni a tutti i settori delle infrastrutture critiche, un elemento importante nel quadro della cibersicurezza di tale paese. Il Q-C2M2 si basa su **cinque domini**, ciascuno dei quali è poi diviso in diversi **sotto-domini** per coprire l'intera gamma di maturità delle capacità di cibersicurezza.

I cinque domini sono illustrati in dettaglio di seguito:

i. Il **dominio «Comprendere»** include quattro sotto-domini: governance informatica, risorse, rischi e formazione.
ii. I sotto-domini del **dominio «Proteggere»** includono sicurezza dei dati, sicurezza della tecnologia, sicurezza del controllo degli accessi, sicurezza delle comunicazioni e sicurezza del personale.
iii. Il **dominio «Esporre»** comprende i sotto-domini monitoraggio, gestione degli incidenti, rilevamento, analisi ed esposizione.
iv. Il **dominio «Rispondere»** comprende pianificazione della risposta, mitigazione e comunicazione della risposta.
v. Il **dominio «Sostenere»** comprende pianificazione del recupero, gestione della continuità, miglioramento e dipendenze esterne.

Livelli di maturità

Il Q-C2M2 utilizza **5 livelli di maturità** che misurano il grado di maturità delle capacità di un'entità statale o di un'organizzazione non statale a livello di funzioni fondamentali. Tali livelli mirano a valutare la maturità nei cinque domini illustrati nella sezione precedente.

- **In fase di avvio**: attua pratiche e processi di cibersicurezza ad hoc in alcuni domini.
- **In fase di attuazione**: ha adottato politiche per implementare tutte le attività di cibersicurezza nell'ambito dei domini, con l'obiettivo di completare l'attuazione in un tempo definito.
- **In fase di sviluppo**: ha attuato politiche e pratiche per sviluppare e migliorare le attività di cibersicurezza nell'ambito dei domini con l'obiettivo di proporre nuove attività da attuare.
- **Adattivo**: rivede e riesamina le attività di cibersicurezza e adotta pratiche basate su indicatori predittivi derivati da esperienze e misure precedenti.
- **Agile**: continua a praticare la fase adattiva ponendo un ulteriore accento sull'agilità e sulla velocità nell'implementazione delle attività nei domini.

Metodo di valutazione

Il Q-C2M2 si trova in una fase iniziale di ricerca e non è ancora pronto per essere attuato. Si tratta di quadro che potrebbe essere utilizzato per attuare un modello di valutazione dettagliata per le organizzazioni del Qatar in futuro.

A.5 Cybersecurity Maturity Model Certification (CMMC)

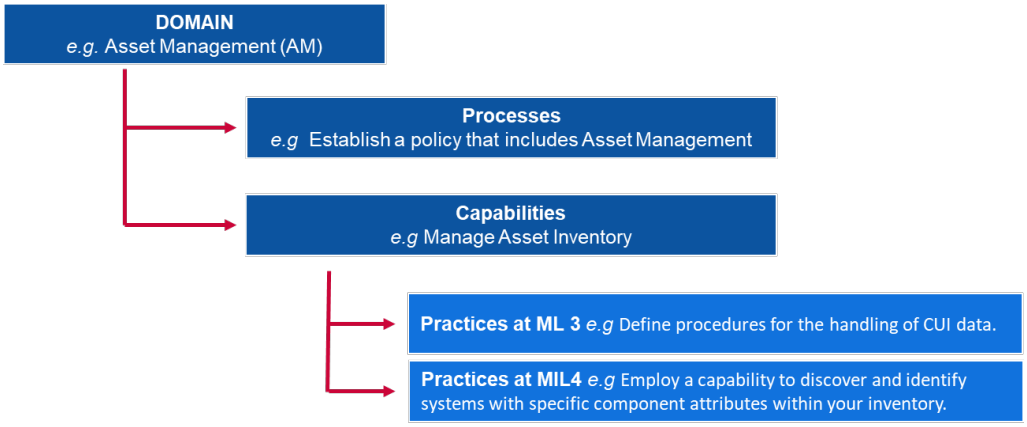
La *Cybersecurity Maturity Model Certification* (CMMC, certificazione del modello di maturità della cibersicurezza) è stata sviluppata dal Dipartimento della difesa degli Stati Uniti in collaborazione con la Carnegie Mellon University e l'*Applied Physics Laboratory* della Johns Hopkins University. L'obiettivo principale del Dipartimento della difesa nella progettazione di questo modello è proteggere le informazioni del settore della base industriale di difesa (*Defense Industrial Base*, DIB) Le informazioni oggetto della CMMC sono classificate come «Federal Contract Information» (FCI), informazioni fornite o generate per il governo nell'ambito di un contratto non destinate alla divulgazione pubblica, o «Controlled Unclassified Information» (CUI), informazioni che richiedono tutela e controlli alla diffusione in conformità e coerentemente con le leggi, i regolamenti e le politiche governative. La CMMC misura la maturità della cibersicurezza e fornisce le migliori pratiche, unitamente a un elemento di certificazione, per garantire l'attuazione di pratiche associate a ciascun livello di maturità. L'ultima versione della CMMC è stata pubblicata nel 2020.

Attributi/Dimensioni

La CMMC prende in considerazione **diciassette domini** che rappresentano gruppi di processi e capacità di cibersicurezza. Ogni dominio è poi suddiviso in più **processi,** che sono simili tra i domini, e una o più **capacità** che presenta cinque livelli di maturità. Le capacità sono poi ulteriormente suddivise in **pratiche** per ogni livello di maturità pertinente.

La relazione tra queste nozioni è la seguente:

Figura 9. Esempio di indicatori CMMC



DOMAIN e.g. Asset Management (AM)
Processes
e.g Establish a policy that includes Asset Management
Capabilities
e.g Manage Asset Inventory
Practices at ML 3 e.g Define procedures for the handling of CUI data

Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory

DOMINIO es. gestione delle risorse (AM)
Processi
es. istituire una politica che comprende la gestione delle risorse
Capacità
es. gestire l'inventario delle risorse
Pratiche a MIL 3 es. definire procedure per il trattamento dei dati che costituiscono informazioni di tipo CUI
Pratiche a MIL4 es. impiegare una capacità per scoprire e identificare sistemi con attributi di componenti specifici all'interno dell'inventario

I diciassette domini sono illustrati in dettaglio di seguito:

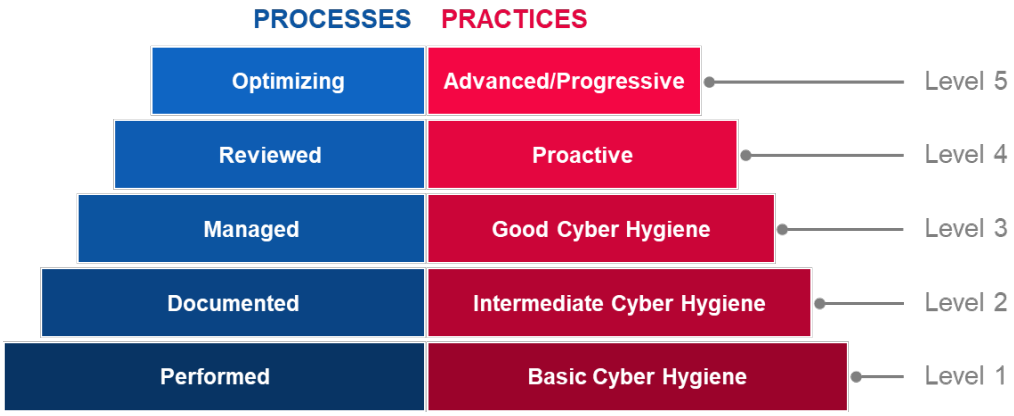
i controllo degli accessi (Access Control, AC);
ii gestione delle risorse (Asset Management, AM);

iii audit e rendicontazione (Audit and Accountability, AU);
iv sensibilizzazione e formazione (Awareness and Training, AT);
v gestione della configurazione (Configuration Management, CM);
vi identificazione e autenticazione (Identification and Authentication, IA);
vii risposta agli incidenti (Incident Response, IR);
viii manutenzione (Maintenance, MA);
ix protezione dei supporti (Media Protection, MP);
x sicurezza del personale (Personnel Security, PS);
xi protezione fisica (Physical Protection, PE);
xii recupero (Recovery, RE);
xiii gestione del rischio (Risk Management, RM);
xiv valutazione della sicurezza (Security Assessment CA);
xv conoscenza situazionale (Situational Awareness, SA);
xvi protezione dei sistemi e delle comunicazioni (System and Communications Protection, SC);
xvii integrità dei sistemi e delle informazioni (System and Information Integrity, SI).

Livelli di maturità

La CMMC individua **5 livelli di maturità** definiti in base a processi e pratiche. Per raggiungere un determinato livello di maturità nella CMMC, un'organizzazione deve soddisfare i prerequisiti relativi ai processi e alle pratiche stabiliti per tale livello. Questo implica anche l'adempimento dei prerequisiti di tutti i livelli inferiori.

Figura 10. Livelli di maturità CMMC



PROCESSES	PROCESSI
Optimizing	Ottimizzazione
Reviewed	Rivisti
Managed	Gestiti
Documented	Documentati
Performed	Eseguiti
PRACTICES	PRATICHE
Advanced/Progressive	Avanzata/Progressiva
Proactive	Proattiva
Good Cyber Hygiene	Igiene cibernetica buona
Intermediate Cyber Hygiene	Igiene cibernetica intermedia
Basic Cyber Hygiene	Igiene cibernetica di base
Level 5	Livello 5
Level 4	Livello 4
Level 3	Livello 3
Level 2	Livello 2
Level 1	Livello 1

- **Livello 1**
  - **Processi – Eseguiti**: perché l'organizzazione può essere in grado di eseguire queste pratiche solo in modo ad hoc e potrebbe non fare affidamento sulla documentazione. La maturità dei processi non è valutata per il livello 1.

- **Pratiche – Igiene cibernetica di base**: il livello 1 si concentra sulla protezione delle informazioni di tipo FCI e consiste unicamente in pratiche che corrispondono ai requisiti di salvaguardia di base.

- **Livello 2**
  - **Processi – Documentati**: il livello 2 prevede che un'organizzazione stabilisca e documenti pratiche e politiche per orientare l'implementazione degli sforzi nell'ambito della CMMC. La documentazione delle pratiche permette ai soggetti di eseguirle in modo ripetibile. Le organizzazioni sviluppano capacità mature documentando i loro processi e poi mettendoli in pratica come documentato.
  - **Pratiche – Igiene cibernetica intermedia**: il livello 2 serve da transizione dal livello 1 al livello 3 e consiste in un sottoinsieme dei requisiti di sicurezza specificati in NIST SP 800-171, nonché di pratiche derivanti da altre norme e riferimenti.

- **Livello 3**
  - **Processi – Gestiti**: il livello 3 prevede che un'organizzazione elabori, mantenga e finanzi un piano che dimostri la gestione delle attività per l'implementazione della pratica. Il piano può includere informazioni su missioni, obiettivi, piani di progetto, assegnazione di risorse, formazione richiesta e coinvolgimento dei portatori di interessi pertinenti.
  - **Pratiche – Igiene cibernetica buona**: il livello 3 è incentrato sulla protezione delle informazioni di tipo CUI e comprende tutti i requisiti di sicurezza specificati in NIST SP 800-171 oltre a pratiche aggiuntive derivanti da altre norme e riferimenti per mitigare le minacce.
- **Livello 4**
  - **Processi – Rivisti**: il livello 4 prevede che un'organizzazione riveda e misuri le pratiche in termini di efficacia. Oltre a misurare l'efficacia delle pratiche, le organizzazioni a questo livello sono in grado di intraprendere azioni correttive quando necessario e di informare la dirigenza di livello superiore in merito allo stato o ai problemi in maniera ricorrente.
  - **Pratiche – Proattive**: il livello 4 si concentra sulla protezione delle informazioni di tipo CUI e comprende un sottoinsieme dei requisiti di sicurezza avanzata. Queste pratiche migliorano le capacità di rilevamento e di risposta di un'organizzazione per affrontare e adattarsi all'evoluzione delle tattiche, tecniche e procedure.
- **Livello 5**
  - **Processi – Ottimizzazione**: il livello 5 richiede che un'organizzazione standardizzi e ottimizzi l'attuazione dei processi in tutta l'organizzazione.
  - **Pratiche – Avanzate/Proattive**: il livello 5 è incentrato sulla protezione delle informazioni di tipo CUI. Le pratiche aggiuntive approfondiscono e rendono più sofisticate le capacità di cibersicurezza.

Metodo di valutazione

La CMMC è un modello relativamente giovane, ultimato nel primo trimestre del 2020, pertanto non ancora implementato in alcuna organizzazione. Tuttavia, gli appaltatori del Dipartimento della difesa prevedono di rivolgersi a esaminatori terzi certificati per la conduzione di audit. Il Dipartimento richiede ai suoi appaltatori di attuare le migliori pratiche per promuovere la sicurezza informatica e la protezione delle informazioni sensibili.

A.6 Community Cyber Security Maturity Model (CCSMM)

Il *Community Cyber Security Maturity Model* (CCSMM, modello di maturità della cibersicurezza per le comunità) è stato messo a punto dal *Centre for Infrastructure Assurance and Security* dell'Università del Texas. L'obiettivo del CCSMM è definire meglio i metodi per determinare lo stato attuale di una comunità nella sua preparazione informatica e fornire una tabella di marcia che le comunità possano seguire nei loro sforzi di preparazione. Le comunità a cui si rivolge il CCSMM sono principalmente enti pubblici locali o statali. Il CCSMM è stato progettato nel 2007.

Attributi/Dimensioni

I livelli di maturità sono definiti secondo **6 dimensioni principali** che coprono i diversi aspetti della sicurezza informatica all'interno delle comunità e delle organizzazioni. Queste sei dimensioni sono chiaramente definite per ogni livello di maturità (specificato nella Figura 11. Riassunto delle dimensioni **CCSMM**) e sono:

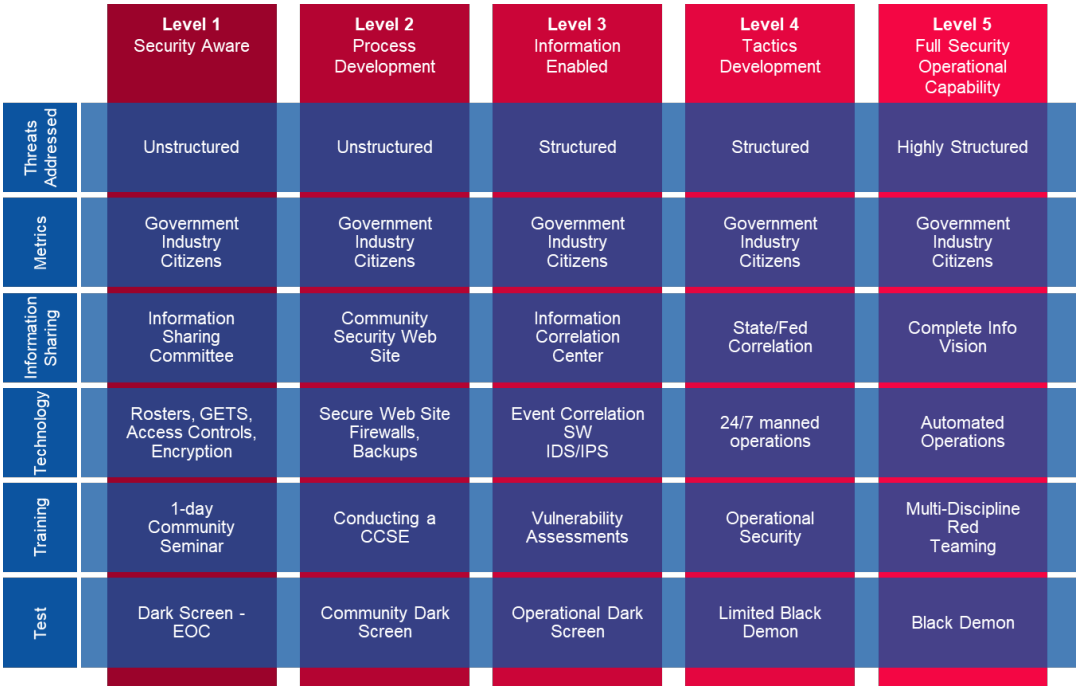
i minacce affrontate;
ii metriche;
iii condivisione delle informazioni;
iv tecnologia;
v formazione;
vi test.

Livelli di maturità

Il CCSMM si fonda su **5 livelli di maturità** basati sui principali tipi di minacce e attività affrontate al rispettivo livello:

- **Livello 1: Consapevole della sicurezza**
  Il tema principale delle attività a questo livello è sensibilizzare individui e organizzazioni in merito alle minacce, ai problemi e alle questioni correlati alla cibersicurezza.
- **Livello 2: Sviluppo dei processi**
  Livello concepito per aiutare le comunità a stabilire e migliorare i processi di sicurezza necessari per affrontare i problemi di cibersicurezza in modo efficace.
- **Livello 3: Supportato dalle informazioni**
  Progettato per migliorare i meccanismi di condivisione delle informazioni all'interno della comunità per consentire un'efficace correlazione di singole informazioni apparentemente eterogenee.
- **Livello 4: Sviluppo di tattiche**
  Gli elementi di questo livello sono concepiti per sviluppare metodi migliori e più proattivi per rilevare e rispondere agli attacchi. A questo livello, la maggior parte dei metodi di prevenzione dovrebbe essere in atto.
- **Livello 5: Piena capacità operativa di sicurezza**
  Questo livello rappresenta gli elementi che dovrebbero essere in atto affinché un'organizzazione possa considerarsi completamente pronta dal punto di vista operativo ad affrontare qualsiasi tipo di minaccia informatica.

Figura 11. Riassunto delle dimensioni CCSMM per livello



Level 1
Security Aware
Level 2
Process Development
Level 3
Information Enabled
Level 4
Tactics Development
Level 5
Full Security Operational Capability
Threats Addressed
Metrics
Information sharing
Technology
Training
Test
Unstructured
Government
Industry
Citizens
Information Sharing Committee
Rosters, GETS, Assess Controls, Encryption
1-day Community Seminar
Dark Screen – EOC
Unstructured
Government
Industry
Citizens
Community Security Web site
Secure Web Site Firewalls, Backups
Conducting a CCSE
Community Dark Screen
Structured
Government
Industry
Citizens
Information Correlation Center
Event Correlation SW IDS/IPS
Vulnerability Assessment
Operational Dark Screen
Structured
Government
Industry
Citizens
State/Fed Correlation
24/7 manned operations

Livello 1
Consapevole della sicurezza
Livello 2
Sviluppo dei processi
Livello 3
Supportato dalle informazioni
Livello 4
Sviluppo delle tattiche
Livello 5
Piena capacità operativa di sicurezza
Minacce affrontate
Metriche
Condivisione delle informazioni
Tecnologia
Formazione
Test
Non strutturato
Pubblica amministrazione
Industria
Cittadini
Comitato di condivisione delle informazioni
Registro di servizio, GETS, controllo accessi, crittografia
Seminario per la comunità di 1 giornata
Dark Screen – EOC
Non strutturato
Pubblica amministrazione
Industria
Cittadini
Sito web sulla sicurezza della comunità
Firewall e backup per sito web sicuro
Conduzione di CCSE
Community Dark Screen
Strutturato
Pubblica amministrazione
Industria
Cittadini
Centro di correlazione delle informazioni
Correlazione eventi SW IDS/IPS
Valutazione della vulnerabilità
Operational Dark Screen
Strutturato
Pubblica amministrazione
Industria
Cittadini
Correlazione statale/federale
Operazioni con personale 24/7

Operational Security	Sicurezza operativa
Limited Black Demon	Limited Black Demon
Highly Structured	Altamente strutturato
Complete Info	Visione completa
Vision	delle informazioni
Automated	Operazioni
Operations	automatizzate
Multi-Discipline	Red
Red	Team
Teaming	multidisciplinare
Black Demon	Black Demon
Highly Structured	Altamente strutturato

Metodo di valutazione

Il CCSMM come metodologia di valutazione è concepito per essere utilizzato dalle comunità con il contributo delle agenzie di contrasto statali e federali. Mira ad aiutare la comunità a definire che cosa è più importante, quali sono i bersagli più probabili e che cosa deve essere protetto (e in quale misura). Tenendo presente questi obiettivi, è possibile sviluppare piani per portare ogni aspetto della comunità al livello di maturità richiesto in termini di cibersicurezza. L'intelligence specifica generata dal CCSMM aiuta a definire gli obiettivi di vari test ed esercitazioni, utilizzabili per misurare l'efficacia dei programmi stabiliti.

A.7 Information Security Maturity Model for NIST Cyber Security Framework (ISMM)

L'*Information Security Maturity Model* (ISMM, modello di maturità per la sicurezza delle informazioni) è stato sviluppato nel College of Computer Sciences and Engineering della King Fahd University of Petroleum and Minerals in Arabia Saudita. Propone un nuovo modello di maturità delle capacità per misurare l'attuazione delle misure di cibersicurezza. L'obiettivo dell'ISMM è consentire alle organizzazioni di valutare i progressi compiuti nell'attuazione nel corso del tempo utilizzando regolarmente lo stesso strumento di misurazione per garantire il mantenimento della posizione di sicurezza desiderata. L'ISMM è stato sviluppato nel 2017.

Attributi/Dimensioni

L'ISMM si basa sulle aree valutate dell'ambito del quadro NIST e aggiunge una dimensione alla valutazione della conformità. Questo porta il modello a **23 aree valutate** per il livello di sicurezza di un'organizzazione. Le 23 aree valutate sono:

i gestione delle risorse;
ii ambiente aziendale;
iii governance;
iv valutazione del rischio;
v strategia di gestione del rischio;
vi valutazione della conformità;
vii controllo degli accessi;
viii sensibilizzazione e formazione;
ix sicurezza dei dati;
x processi e procedure di protezione delle informazioni
xi manutenzione;
xii tecnologia di protezione;
xiii anomalie ed eventi;
xiv monitoraggio continuo della sicurezza;
xv processi di rilevamento;
xvi pianificazione della risposta;
xvii comunicazioni della risposta;
xviii analisi della risposta;
xix mitigazione della risposta;
xx miglioramenti della risposta;
xxi pianificazione del recupero;
xxii miglioramenti del recupero;

[xxiii] comunicazioni del recupero.

Livelli di maturità

L'ISMM si basa su **5 livelli di maturità**, che purtroppo non sono descritti in dettaglio nella documentazione disponibile.

- **Livello 1:** Processo eseguito
- **Livello 2:** Processo gestito
- **Livello 3:** Processo consolidato
- **Livello 4:** Processo prevedibile
- **Livello 5:** Processo in fase di ottimizzazione

Metodo di valutazione

L'ISMM non propone alcuna metodologia specifica per condurre la valutazione per le organizzazioni.

A.8 Internal Audit Capability Model (IA-CM) per il settore pubblico

L'*Internal Audit Capability Model* (IA-CM, modello delle capacità per audit interno) è stato sviluppato dall'*Institute of Internal Auditors Research Foundation* con l'intenzione di rafforzare capacità e sostegno attraverso l'autovalutazione nel settore pubblico. Destinato ai professionisti dell'audit, l'IA-CM fornisce una panoramica del modello stesso insieme a una guida all'applicazione, per offrire assistenza nell'uso del modello come strumento di autovalutazione.

Sebbene l'IA-CM sia incentrato sulla capacità di audit interno, piuttosto che sullo sviluppo delle capacità di cibersicurezza, il modello è realizzato come strumento di autovalutazione della maturità per le entità del settore pubblico, che può essere applicato globalmente per migliorare i processi e l'efficacia. Poiché il suo ambito non è focalizzato sulla cibersicurezza, gli attributi non saranno analizzati. L'IA-CM è stato completato nel 2009.

Livelli di maturità

L'*Internal Audit Capability Model* (IA-CM) prevede **5 livelli di maturità**, ognuno dei quali descrive le caratteristiche e le capacità di un'attività di audit interno a tale livello. I livelli di capacità descritti nel modello forniscono una tabella di marcia per il miglioramento continuo.

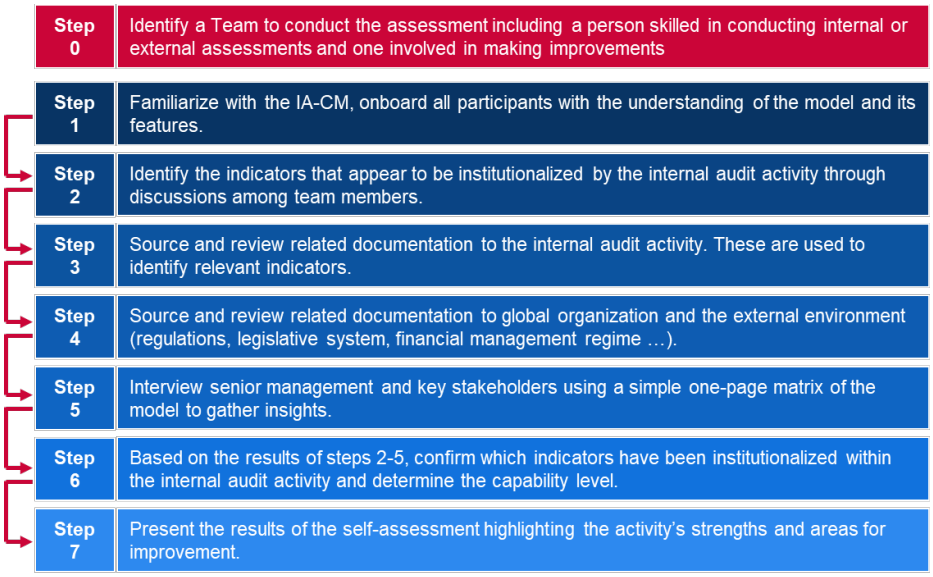
- **Livello 1: Iniziale**
  Nessuna capacità sostenibile e ripetibile - dipende dagli sforzi individuali
  - Ad hoc o non strutturato.
  - Audit o revisioni singoli e isolati di documenti e transazioni singoli isolati, per valutazione di accuratezza e conformità.
  - I risultati prodotti dipendono dalle competenze della persona specifica che ricopre la posizione.
  - Nessuna pratica professionale stabilita, eccetto quelle fornite dalle associazioni professionali.
  - Approvazione del finanziamento da parte della direzione, ove necessario.
  - Assenza di infrastrutture.
  - Gli auditor fanno probabilmente parte di un'unità organizzativa più grande.
  - La capacità istituzionale non è sviluppata.
- **Livello 2: Infrastruttura**
  Pratiche e procedure sostenibili e ripetibili
  - La domanda chiave o la sfida per il livello 2 è come stabilire e mantenere la ripetibilità dei processi e quindi una capacità ripetibile.
  - Vengono create relazioni di reporting dell'audit interno, infrastrutture gestionali e amministrative, nonché pratiche e processi professionali (orientamento, processi e procedure per l'audit interno).
  - Pianificazione degli audit basata principalmente sulle priorità della direzione.
  - Affidamento continuo essenzialmente sulle capacità e competenze di persone specifiche.
  - Conformità parziale alle norme.

- **Livello 3: Integrato**
  Pratiche di gestione e professionali applicate in modo uniforme
  - Le politiche, i processi e le procedure di audit interno sono definiti, documentati e integrati tra loro e nell'infrastruttura dell'organizzazione.
  - Le pratiche di gestione e professionali di audit interno sono ben consolidate e applicate uniformemente in tutta l'attività di audit interno.
  - L'audit interno inizia ad allinearsi all'attività dell'organizzazione e ai rischi che affronta.
  - L'audit interno si evolve dal condurre esclusivamente l'audit interno tradizionale a integrarsi a pieno titolo e a fornire consulenza sulle prestazioni e sulla gestione dei rischi.
  - L'attenzione si concentra sullo sviluppo del team, sulla capacità dell'attività di audit interno e sulla sua indipendenza e obiettività.
  - È generalmente conforme alle norme.
- **Livello 4: Gestito**
  Integra le informazioni provenienti da tutta l'organizzazione per migliorare la governance e la gestione del rischio
  - L'audit interno e le aspettative dei principali portatori di interessi sono allineati.
  - Sono in essere metriche di performance per misurare e monitorare i processi e i risultati dell'audit interno.
  - È riconosciuta la capacità dell'audit interno di apportare contributi significativi all'organizzazione.
  - L'audit interno funziona come parte integrante della governance e della gestione dei rischi dell'organizzazione.
  - L'audit interno è un'unità aziendale ben gestita.
  - I rischi sono misurati e gestiti quantitativamente.
  - Le abilità e le competenze richieste sono in atto, con capacità di rinnovamento e di condivisione delle conoscenze (nell'ambito dell'audit interno e in tutta l'organizzazione).
- **Livello 5: Ottimizzazione**
  Apprendere dall'interno e dall'esterno dell'organizzazione per un miglioramento continuo
  - L'audit interno è un'organizzazione «in apprendimento» con miglioramenti dei processi e innovazione continui.
  - L'audit interno sfrutta le informazioni provenienti dall'interno e dall'esterno dell'organizzazione per contribuire al raggiungimento degli obiettivi strategici.
  - Performance di altissimo livello/raccomandate/migliori pratiche.
  - L'audit interno è una parte cruciale della struttura di governance dell'organizzazione.
  - Competenze professionali e specialistiche di altissimo livello.
  - Le misure di performance a livello individuale, di unità e di organizzazione sono pienamente integrate per
  - stimolare miglioramenti delle prestazioni.

Metodo di valutazione

L'Internal Audit Capability Model è chiaramente concepito per l'autovalutazione. Fornisce fasi dettagliate da seguire per l'utilizzo dell'IA-CM e diapositive campione da personalizzare. Prima di iniziare l'autovalutazione, è necessario individuare un team specifico che includa, come minimo, una persona esperta nella conduzione di valutazioni interne o esterne degli audit interni e una persona che si occupa di apportare miglioramenti in quest'area.

Figura 12. Fasi di autovalutazione di IC-AM



Step 0	Fase 0
Step 1	Fase 1
Step 2	Fase 2
Step 3	Fase 3
Step 4	Fase 4
Step 5	Fase 5
Step 6	Fase 6
Step 7	Fase 7
Identify a Team to conduct the assessment including a person skilled in conducting internal of external assessments and one involved in making improvements.	Individuare un team per eseguire la valutazione che includa una persona esperta nella conduzione di valutazioni interne o esterne e una che si occupa di apportare miglioramenti.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Acquisire familiarità con l'IA-CM, assicurare che tutti i partecipanti comprendano il modello e le sue caratteristiche.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Identificare gli indicatori che sembrano essere istituzionalizzati dall'attività di audit interno attraverso la discussione tra i membri del team.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Acquisire ed esaminare la documentazione relativa all'attività di audit interno, che viene utilizzata per identificare gli indicatori pertinenti.
Source and review related documentation to global organization and the external environment (regulations, legislative system, financial management regime …).	Acquisire ed esaminare la documentazione relativa all'organizzazione globale e all'ambiente esterno (regolamenti, sistema legislativo, regime di gestione finanziaria, ecc.).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Intervistare gli alti dirigenti e i principali portatori di interessi utilizzando una semplice matrice di una pagina del modello per raccogliere informazioni.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Sulla base dei risultati delle fasi 2-5, confermare quali indicatori sono stati istituzionalizzati nell'ambito dell'attività di audit interno e determinare il livello di capacità.
Present the results of the self-assessment highlighting the activity's strengths and areas for improvement.	Presentare i risultati dell'autovalutazione evidenziando i punti di forza dell'attività e le aree di miglioramento.

A.9 Global Cybersecurity Index (GCI)

Il *Global Cybersecurity Index* (GCI, indice di cibersicurezza globale) è un'iniziativa dell'Unione internazionale delle telecomunicazioni (UIT) mirata a rivedere l'impegno e la situazione della cibersicurezza in tutte le regioni dell'UIT, Africa, Americhe, Stati Arabi, Asia-Pacifico, CSI ed Europa, e che mette al centro dell'attenzione i paesi che mostrano un impegno elevato e pratiche raccomandate. L'obiettivo del GCI è aiutare i paesi a individuare le aree di miglioramento nel campo della cibersicurezza, oltre a motivarli all'azione per migliorare la loro posizione in classifica, contribuendo così ad aumentare il livello generale di cibersicurezza in tutto il mondo.

Dal momento che il GCI è un indice e non un modello di maturità, non utilizza livelli di maturità bensì un punteggio per classificare e confrontare l'impegno globale nella cibersicurezza di nazioni e regioni.

Attributi/Dimensioni

Il *Global Cybersecurity Index* (GCI) si basa sui cinque pilastri della *Global Cybersecurity Agenda* (GCA). Questi pilastri formano i cinque sotto-indici del GCI e ognuno comprende una serie di indicatori. I cinque pilastri e gli indicatori sono descritti di seguito.

i **Giuridico**: misure basate sull'esistenza di istituzioni e quadri giuridici che si occupano di cibersicurezza e criminalità informatica.
- Legislazione in materia di criminalità informatica;
- Normativa sulla cibersicurezza;
- Legislazione sul contenimento dello spam.

ii **Tecnico**: misure basate sull'esistenza di istituzioni e quadri tecnici che si occupano di cibersicurezza.
- CERT/CIRT/CSRIT;
- Quadro di attuazione delle norme;
- Ente di normazione;
- Meccanismi tecnici e capacità impiegati per affrontare lo spam;
- Uso del cloud per finalità di cibersicurezza;
- Meccanismi di protezione dei minori online.

iii **Organizzativo**: misure basate sull'esistenza di istituzioni di coordinamento delle politiche e strategie per lo sviluppo della cibersicurezza a livello nazionale.
- Strategie nazionale per la cibersicurezza;
- Agenzia responsabile;
- Cibersicurezza.

iv **Sviluppo delle capacità**: misure basate sull'esistenza di programmi di ricerca e sviluppo, istruzione e formazione, professionisti certificati e agenzie del settore pubblico che promuovono lo sviluppo delle capacità.
- Azioni di sensibilizzazione dei cittadini;
- Quadro per la certificazione e l'accreditamento dei professionisti della cibersicurezza;
- Corsi di formazione professionale in cibersicurezza;
- Programmi educativi o piani di studi universitari in cibersicurezza;
- Programmi di ricerca e sviluppo sulla cibersicurezza;
- Meccanismi di incentivazione.

v **Cooperazione**: misure basate sull'esistenza di partenariati, quadri di cooperazione e reti di condivisione delle informazioni.
- Accordi bilaterali;
- Accordi multilaterali;
- Partecipazione a forum/associazioni internazionali;
- Partenariati pubblico-privato;
- Partenariati trasversali alle agenzie/all'interno delle agenzie;
- Migliori pratiche.

Metodo di valutazione

Il GCI è uno strumento di autovalutazione realizzato attraverso un'indagine ([30]) con domande binarie, pre-codificate e aperte. L'uso di risposte binarie elimina la valutazione basata sull'opinione e ogni possibile distorsione verso certi tipi di risposte. Le risposte pre-codificate consentono un risparmio di tempo e un'analisi più accurata dei dati. Inoltre, una semplice scala dicotomica permette una valutazione più rapida e complessa in quanto non richiede risposte lunghe, accelerando e snellendo così il processo di risposta e ulteriore valutazione. L'intervistato deve solo confermare la presenza o l'assenza di determinate soluzioni di cibersicurezza preventivamente identificate. Un meccanismo di indagine online, utilizzato per raccogliere le risposte e caricare il materiale pertinente, consente l'estrazione di buone pratiche e una serie di valutazioni qualitative tematiche da parte di un gruppo di esperti.

([30]) https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf

Il processo GCI complessivo si articola nel modo seguente.

- Una lettera d'invito viene inviata a tutti i partecipanti, informandoli dell'iniziativa e richiedendo un punto di contatto responsabile della raccolta di tutti i dati pertinenti e della compilazione del questionario GCI online. Durante l'indagine online, il punto di contatto approvato viene ufficialmente invitato dall'UIT a rispondere al questionario.
- Raccolta di dati primari (per i paesi che non rispondono al questionario):
  - l'UIT elabora una prima bozza di risposta al questionario utilizzando dati disponibili al pubblico e ricerche online;
  - la suddetta bozza viene inviata ai punti di contatto per la revisione;
  - i punti di contatto migliorano l'accuratezza e restituiscono poi la bozza di risposta al questionario;
  - la bozza corretta delle risposte al questionario viene inviata a ogni punto di contatto per l'approvazione finale;
  - il questionario convalidato è usato per l'analisi, l'assegnazione del punteggio e la classifica.
- Raccolta di dati secondari (per i paesi che rispondono al questionario):
  - l'UIT individua eventuali risposte, i documenti di supporto, link, ecc. mancanti;
  - i punti di contatto migliorano l'accuratezza delle risposte, ove necessario;
  - la bozza corretta delle risposte al questionario viene inviata a ogni punto di contatto per l'approvazione finale;
  - il questionario convalidato è usato per l'analisi l'assegnazione del punteggio e la classifica.

A.10 Cyber Power Index (CPI)

Il Cyber Power Index (CPI) è stato creato dal programma di ricerca dell'Economist Intelligence Unit sponsorizzato da Booz Allen Hamilton nel 2011. Il CPI è un «modello quantitativo e qualitativo dinamico, [...] che misura gli attributi specifici dell'ambiente cibernetico attraverso quattro fattori determinanti della potenza informatica: quadro giuridico e normativo; contesto economico e sociale; infrastruttura tecnologica e applicazione industriale, esaminando il progresso digitale nei settori chiave» ([31]). L'obiettivo del Cyber Power Index è valutare in modo comparativo la capacità dei paesi del G20 di resistere agli attacchi informatici e di implementare l'infrastruttura digitale necessaria per un'economia prospera e sicura. L'analisi comparativa fornita dal CPI si concentra su 19 paesi del G20 (esclusa l'UE). L'indice fornisce poi una classifica dei paesi per ogni indicatore.

Attributi/Dimensioni

Il Cyber Power Index (CPI) si basa su quattro fattori determinanti della potenza informatica. Ogni categoria viene poi misurata tramite diversi indicatori per assegnare a ogni paese un punteggio specifico. Le categorie e i pilastri sono i seguenti.

i **Quadro giuridico e normativo**
- Impegno dello Stato verso per lo sviluppo informatico
- Politiche di protezione informatica
- Censura informatica (o sua assenza)
- Efficacia politica
- Protezione della proprietà intellettuale

ii **Contesto economico e sociale**
- Livelli di istruzione
- Competenze tecniche
- Grado di apertura del commercio
- Grado di innovazione nell'ambiente aziendale

iii **Infrastruttura tecnologica**
- Accesso alle tecnologie dell'informazione e della comunicazione

([31]) www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

- Qualità delle tecnologie dell'informazione e della comunicazione
- Accessibilità delle tecnologie dell'informazione e della comunicazione
- Spesa per la tecnologia dell'informazione
- Numero di server sicuri

iv **Applicazione industriale**

- Reti intelligenti
- Sanità elettronica
- Commercio elettronico
- Trasporto intelligente
- E-government

Metodo di valutazione

Il CPI è un modello di assegnazione del punteggio quantitativo e qualitativo. La valutazione è stata condotta dall'Economist Intelligence Unit utilizzando indicatori quantitativi provenienti da fonti statistiche disponibili ed effettuando stime in caso di mancanza di dati. Le principali fonti utilizzate sono l'Economist Intelligence Unit, l'Organizzazione delle Nazioni Unite per l'educazione, la scienza e la cultura (UNESCO), l'Unione internazionale delle telecomunicazioni (UIT) e la Banca Mondiale.

A.11 Cyber Power Index (CPI)

In questa sezione vengono riassunti i principali risultati dell'analisi dei modelli di maturità esistenti. La Tabella 5. Panoramica dei modelli di maturità analizzati offre un quadro generale delle caratteristiche principali di ogni modello, secondo il modello modificato di Becker. La Tabella 6. Confronto dei livelli di maturità fornisce definizioni di alto livello dei livelli di maturità dei modelli analizzati. La Tabella 7 contiene una panoramica delle dimensioni o degli attributi usati in ogni modello.

Tabella 5. Panoramica dei modelli di maturità analizzati

Nome del modello	Ente di origine	Finalità	Destinatari	N. di livelli	N. di attributi	Metodo di valutazione	Rappresentazione dei risultati
Cybersecurity Capacity Maturity Model for Nations (CMM)	Global Cybersecurity Capacity Centre Università di Oxford	Aumentare la scala e l'efficacia dello sviluppo delle capacità di cibersicurezza a livello internazionale	Paesi	5	5 dimensioni principali	Collaborazione con un'organizzazione locale per mettere a punto il modello prima di applicarlo al contesto nazionale	Grafico a radar a cinque sezioni
Cybersecurity Capability Maturity Model (C2M2)	Dipartimento dell'energia degli Stati Uniti	Aiutare le organizzazioni a valutare e apportare miglioramenti ai loro programmi di cibersicurezza e a rafforzare la loro resilienza operativa	Organizzazioni di tutti i settori, tipi e dimensioni	4	10 domini principali	Metodologia e kit di strumenti di autovalutazione	Scheda di valutazione con grafici a torta
Framework for Improving Critical Infrastructure Cybersecurity	Istituto nazionale per gli standard e la tecnologia (NIST)	Quadro finalizzato a guidare le attività di cibersicurezza e a gestire i rischi all'interno di un'organizzazione	Organizzazioni	n.d. (4 livelli)	5 funzioni essenziali	Autovalutazione	-
Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	College of Law dell'Università del Qatar	Fornire un modello attuabile che possa essere utilizzato per valutare, misurare e sviluppare la struttura di cibersicurezza del Qatar	Organizzazioni del Qatar	5	5 domini principali	-	-
Cybersecurity Maturity Model Certification (CMMC)	Dipartimento della difesa degli Stati Uniti	Promuovere le migliori pratiche di cibersicurezza per salvaguardare le informazioni	Organizzazioni del settore della base industriale di difesa (DIB)	5	17 domini principali	Valutazione da parte di revisori terzi	-
Community Cybersecurity Maturity Model (CCSMM)	Centre for Infrastructure Assurance and Security dell'Università del Texas	Determinare il livello attuale della preparazione informatica di una comunità e fornire una tabella di marcia che le comunità possano seguire nei propri sforzi volti alla preparazione	Comunità (amministrazioni locali o statali)	5	6 dimensioni principali	Valutazione all'interno delle comunità con il contributo delle agenzie di contrasto statali e federali	-
Information Security Maturity Model for NIST Cybersecurity Framework (ISMM)	College of Computer Sciences and Engineering King Fahd University of Petroleum and Minerals, Dhahran, Arabia Saudita	Consentire alle organizzazioni di valutare i progressi compiuti nell'attuazione nel corso del tempo per garantire il mantenimento della posizione di sicurezza desiderata	Organizzazioni	5	23 aree valutate	-	-
Internal Audit Capability Model (IA-CM) per il settore pubblico	Institute of Internal Auditors Research Foundation	Rafforzare capacità e sostegno nell'audit interno attraverso l'autovalutazione nel settore pubblico	Organizzazioni del settore pubblico	5	6 elementi	Autovalutazione	-
Global Cybersecurity Index (GCI)	Unione internazionale delle telecomunicazioni (UIT)	Riesaminare l'impegno e la situazione di cibersicurezza e aiutare i paesi a individuare le aree di miglioramento in questo campo	Paesi	n.d.	5 pilastri	Autovalutazione	Graduatoria

Cyber Power Index (CPI)	Economist Intelligence Unit e Booz Allen Hamilton	Valutare in modo comparativo la capacità dei paesi del G20 di resistere agli attacchi informatici e di implementare l'infrastruttura digitale necessaria per un'economia prospera e sicura.	Paesi del G20	n.d.	4 categorie	Analisi comparativa a cura dell'Economist Intelligence Unit	Graduatoria

Tabella 6. Confronto dei livelli di maturità

Modello	Livello 1	Livello 2	Livello 3	Livello 4	Livello 5
Cybersecurity Capacity Maturity Model for Nations (CMM)	**Avvio** Non esiste alcuna maturità di cibersicurezza oppure è allo stadio embrionale. È possibile che vi siano discussioni iniziali sullo sviluppo di capacità di cibersicurezza, ma non sono state intraprese azioni concrete. In questa fase non vi sono prove osservabili.	**Crescita** Alcune caratteristiche degli aspetti hanno iniziato a crescere e ad essere formulate, ma potrebbero essere ad-hoc, disorganizzate, mal definite, o semplicemente «nuove». Tuttavia, le prove di questa attività possono essere chiaramente dimostrate.	**Consolidato** Gli elementi dell'aspetto sono in atto e funzionano. La relativa allocazione delle risorse, tuttavia, non è sottoposta a valutazione ben ponderata. Sono state compiute poche decisioni di compromesso riguardo all'investimento «relativo» nei vari elementi dell'aspetto. L'aspetto è tuttavia funzionale e definito.	**Strategico** Sono state compiute scelte riguardo a quali parti dell'aspetto sono importanti e quali sono meno importanti per la specifica organizzazione o nazione. La fase strategica rispecchia il fatto che queste scelte sono state compiute subordinatamente alle particolari circostanze della nazione o dell'organizzazione.	**Dinamico** Sono in atto chiari meccanismi per modificare la strategia a seconda delle circostanze prevalenti, ad es. tecnologia dell'ambiente delle minacce, conflitto globale o cambiamento significativo in un'area di interesse (ad es. criminalità informatica o privacy). Le organizzazioni dinamiche hanno sviluppato metodi per modificare le strategie con facilità. Il rapido processo decisionale, la riallocazione delle risorse e la costante attenzione all'ambiente in evoluzione sono caratteristiche di questa fase.
Cybersecurity Capability Maturity Model (C2M2)	**MIL0** Non sono eseguite prassi.	**MIL1** Vengono eseguite prassi iniziali vengono ma potrebbero essere ad hoc.	**MIL2** Caratteristiche della gestione: le prassi sono documentate; vengono fornite risorse adeguate per sostenere il processo; il personale che esegue le prassi ha competenze e conoscenze adeguate e la responsabilità e l'autorità per l'esecuzione delle prassi sono assegnate. Caratteristiche di approccio: le pratiche sono più complete o avanzate rispetto a MIL1.	**MIL3** Caratteristiche della gestione: le attività sono guidate da politiche (o altre direttive dell'organizzazione); gli obiettivi di performance per le attività del dominio sono stabiliti e monitorati per tenere traccia del conseguimento e le pratiche documentate per le attività del dominio sono standardizzate e migliorate in tutta l'impresa. Caratteristiche di approccio: Le pratiche sono più complete o avanzate rispetto a MIL2.	-
Information Security Maturity Model for NIST	**Processo eseguito**	**Processo gestito**	**Processo consolidato**	**Processo prevedibile**	**Processo in fase di ottimizzazione**

Cyber Security Framework (ISMM)					
Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	**In fase di avvio** Attua pratiche e processi di cibersicurezza ad hoc in alcuni domini.	**In fase di sviluppo** Ha attuato politiche e pratiche per sviluppare e migliorare le attività di cibersicurezza nell'ambito dei domini con l'obiettivo di suggerire nuove attività da attuare.	**In fase di attuazione** Ha adottato politiche per implementare tutte le attività di cibersicurezza nell'ambito dei domini, con l'obiettivo di completare l'attuazione in un tempo definito.	**Adattivo** Rivede e riesamina le attività di cibersicurezza e adotta pratiche basate su indicatori predittivi derivati da esperienze e misure precedenti.	**Agile** Continua a praticare la fase adattiva ponendo un ulteriore accento sull'agilità e sulla velocità nell'implementazione delle attività nei domini.
Cybersecurity Maturity Model Certification (CMMC)	**Processi: Eseguiti** Poiché l'organizzazione potrebbe essere in grado di eseguire queste pratiche solo in modo ad hoc e potrebbe non fare affidamento sulla documentazione, la maturità del processo non è valutata per il livello 1. **Pratiche: Igiene cibernetica di base** Il livello 1 si concentra sulla protezione delle informazioni di tipo FCI (Federal Contract Information) e consiste unicamente in pratiche che corrispondono ai requisiti di salvaguardia di base.	**Processi: Documentati** Il livello 2 prevede che un'organizzazione stabilisca e documenti pratiche e politiche per guidare l'implementazione degli sforzi nell'ambito della CMMC. La documentazione delle pratiche permette ai soggetti di eseguirle in modo ripetibile. Le organizzazioni sviluppano capacità mature documentando i loro processi e poi mettendoli in pratica come documentato. **Pratiche: Igiene cibernetica intermedia** Il livello 2 serve da transizione dal livello 1 al livello 3 e consiste in un sottoinsieme dei requisiti di sicurezza specificati in NIST SP 800-171, nonché di pratiche derivanti da altre norme e riferimenti.	**Processi: Gestiti** Il livello 3 prevede che un'organizzazione elabori, mantenga e finanzi un piano che dimostri la gestione delle attività per l'implementazione della pratica. Il piano può includere informazioni su missioni, obiettivi, piani di progetto, assegnazione di risorse, formazione richiesta e coinvolgimento dei portatori di interessi pertinenti. **Pratiche: Igiene cibernetica buona**. Il livello 3 è incentrato sulla protezione delle informazioni di tipo CUI (Controlled Unclassified Information) e comprende tutti i requisiti di sicurezza specificati in NIST SP 800-171 oltre a pratiche aggiuntive derivanti da altre norme e riferimenti per mitigare le minacce.	**Processi: Rivisti** Il livello 4 prevede che un'organizzazione riveda e misuri le pratiche in termini di efficacia. Oltre a misurare l'efficacia delle pratiche, le organizzazioni a questo livello sono in grado di intraprendere azioni correttive quando necessario e di informare il management di livello superiore in merito allo stato o ai problemi su base ricorrente. **Pratiche: Proattiva** Il livello 4 si concentra sulla protezione delle informazioni di tipo CUI (Controlled Unclassified Information) e comprende un sottoinsieme dei requisiti di sicurezza avanzata. Queste pratiche migliorano le capacità di rilevamento e di risposta di un'organizzazione per affrontare e adattarsi all'evoluzione delle tattiche, tecniche e procedure.	**Processi: Ottimizzazione** Il livello 5 richiede che un'organizzazione standardizzi e ottimizzi l'attuazione dei processi in tutta l'organizzazione. **Pratiche: Avanzate/Proattive** Il livello 5 si concentra sulla protezione delle informazioni di tipo CUI (Controlled Unclassified Information). Le pratiche aggiuntive approfondiscono e rendono più sofisticate le capacità di cibersicurezza.
Community Cyber Security Maturity Model (CCSMM)	**Consapevole della sicurezza** Il tema principale delle attività a questo livello è sensibilizzare individui e organizzazioni in merito alle minacce, ai problemi e alle questioni correlati alla cibersicurezza.	**Sviluppo dei processi** Livello concepito per aiutare le comunità a stabilire e migliorare i processi di sicurezza necessari per affrontare i problemi di cibersicurezza in modo efficace.	**Supportato dalle informazioni** Progettato per migliorare i meccanismi di condivisione delle informazioni all'interno della comunità per consentire un'efficace correlazione di singole informazioni apparentemente eterogenee.	**Sviluppo delle tattiche** Gli elementi di questo livello sono concepiti per sviluppare metodi migliori e più proattivi per rilevare e rispondere agli attacchi. A questo livello la maggior parte dei metodi di prevenzione dovrebbe essere in atto.	**Piena capacità operativa di sicurezza** Questo livello rappresenta gli elementi che dovrebbero essere in atto affinché un'organizzazione possa considerarsi completamente pronta dal punto di vista operativo ad affrontare qualsiasi tipo di minaccia informatica.
Internal Audit Capability Model	**Iniziale**	**Infrastruttura**	**Integrato**	**Gestito**	**Ottimizzazione**

(IA-CM) per il settore pubblico	Nessuna capacità sostenibile e ripetibile - dipende dagli sforzi individuali	Pratiche e procedure sostenibili e ripetibili	Pratiche di gestione e professionali applicate in modo uniforme	Integra le informazioni provenienti da tutta l'organizzazione per migliorare la governance e la gestione del rischio	Apprendere dall'interno e dall'esterno dell'organizzazione per un miglioramento continuo

Tabella 7. Confronto degli attributi o delle dimensioni

	Cybersecurity Capacity Maturity Model for Nations (CMM)	Cybersecurity Capability Maturity Model (C2M2)	Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	Cybersecurity Maturity Model Certification (CMMC)	Cybersecurity Maturity Model Certification (CMMC)	Information Security Maturity Model for NIST Cyber Security Framework (ISMM)	Framework for Improving Critical Infrastructure Cybersecurity	Global Cybersecurity Index (GCI)	Cyber Power Index (CPI)
Livelli	Cinque dimensioni suddivise in diversi fattori comprendenti svariati aspetti e indicatori (Figura 4)	Dieci domini, incluso un obiettivo di gestione unico e diversi obiettivi di approccio (Figura 6)	Cinque domini suddivisi in sotto-domini	Diciassette domini suddivisi in processi e una o più capacità ulteriormente dettagliate in pratiche (Figura 9).	Sei dimensioni principali	Ventitré aree valutate	Cinque funzioni con sottostanti categorie chiave e sottocategorie (Figura 8).	Cinque pilastri comprendenti diversi indicatori	Quattro categorie con diversi indicatori
Attributi/Dimensioni	i Ideare una politica e una strategia di cibersicurezza ii Incoraggiare una cultura della cibersicurezza responsabile all'interno della società iii Sviluppare la conoscenza della cibersicurezza iv Creare quadri giuridici e normativi efficaci v Controllare i rischi attraverso norme, organizzazioni e tecnologie	i Gestione del rischio ii Gestione di risorse, cambiamento e configurazione iii Gestione dell'identità e dell'accesso iv Gestione delle minacce e delle vulnerabilità v Conoscenza situazionale vi Risposta agli eventi e agli incidenti vii Gestione della catena di fornitura e delle dipendenze esterne viii Gestione della forza lavoro ix Architettura di cibersicurezza x Gestione del programma di cibersicurezza	i Comprendere (governance informatica, risorse, rischi e formazione) ii Proteggere (sicurezza dei dati, sicurezza della tecnologia, sicurezza del controllo degli accessi, sicurezza delle comunicazioni e sicurezza del personale) iii Esporre (monitoraggio, gestione degli incidenti, rilevamento, analisi ed esposizione) iv Rispondere (pianificazione della risposta, mitigazione e comunicazione della risposta) v Sostenere (pianificazione del recupero, gestione della continuità, miglioramento e dipendenze esterne)	i Controllo degli accessi ii Gestione delle risorse iii Audit e rendicontazione iv Sensibilizzazione e formazione v Gestione della configurazione vi Identificazione e autenticazione vii Risposta agli incidenti viii Manutenzione ix Protezione dei supporti x Sicurezza del personale xi Protezione fisica xii Recupero xiii Gestione del rischio xiv Valutazione della sicurezza xv Conoscenza situazionale xvi Protezione dei sistemi e delle comunicazioni xvii Integrità dei sistemi e delle informazioni	i Minacce affrontate ii Metriche iii Condivisione delle informazioni iv Tecnologia v Formazione vi Test	i Gestione delle risorse ii Ambiente aziendale iii Governance iv Valutazione del rischio v Strategia di gestione del rischio vi Valutazione della conformità vii Controllo degli accessi viii Sensibilizzazione e formazione ix Sicurezza dei dati x Processi e procedure di protezione delle informazioni xi Manutenzione xii Tecnologia di protezione xiii Anomalie ed eventi xiv Monitoraggio continuo della sicurezza xv Processi di rilevamento xvi Pianificazione della risposta xvii Comunicazioni della risposta xviii Analisi della risposta xix Mitigazione della risposta xx Miglioramenti della risposta xxi Pianificazione del recupero xxii Miglioramenti del recupero xxiii Comunicazioni del recupero	i Identificare ii Proteggere iii Rilevare iv Rispondere v Recuperare	i Giuridico ii Tecnico iii Organizzativo iv Sviluppo delle capacità v Cooperazione	i Quadro giuridico e normativo ii Contesto economico e sociale iii Infrastruttura tecnologica iv Applicazione industriale

ALLEGATO B – BIBLIOGRAFIA DELLA RICERCA A TAVOLINO

Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, (2012), *NCSS: Setting the course for national efforts to strengthen security in cyberspace*, Eraklion, ENISA.

Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, (2016), *Guidelines for SMEs on the security of personal data processing*.

Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, (2012), *NCSS: Practical Guide on Development and Execution*, Eraklion, ENISA.

Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, (2016), *NCSS good practice guide: designing and implementing national cyber security strategies*, Eraklion, ENISA.

Almuhammadi, S. e Alsaleh, M. (2017), «Information Security Maturity Model for Nist Cyber Security Framework», in Computer Science & Information Technology (CS & IT), Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. e Alsaleh, M. (2017), «Information Security Maturity Model for Nist Cyber Security Framework», in Computer Science & Information Technology (CS & IT), disponibile all'indirizzo: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016), *Stocktaking, analysis and recommendations on the protection of CIIs*, disponibile all'indirizzo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009) *Developing Maturity Models for IT Management – A Procedure Model and its Application*, disponibile all'indirizzo: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Bellasio, J. et al., (2018), *Developing Cybersecurity Capacity*: *A proof-of-concept implementation guide*, RAND Corporation. disponibile all'indirizzo: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012), *Introduction to Return on Security Investment*.

Cancelleria federale della repubblica d'Austria, (2013), Austrian Cyber Security Strategy, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019), *Cybersecurity Capability Maturity Model (C2M2) Version 2.0*, disponibile all'indirizzo: https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019), *National Cybersecurity Strategies in Comparison – Challenges for Switzerland*, disponibile all'indirizzo: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Centro nazionale per la cibersicurezza, (2015), *National Cyber Security Strategy of the Czech Republic*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Commissione europea, (2012), Regolamento del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52012PC0238&from=IT

Consiglio dei Ministri (2019), Gazzetta ufficiale portoghese, serie 1 - n. 108 - risoluzione del Consiglio dei Ministri n. 92/2019. disponibile all'indirizzo: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Consiglio del governo lussemburghese (2018), *National Cybersecurity Strategy*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Consiglio federale (2018) Strategia nazionale per la protezione della Svizzera contro i cyber-rischi.

Creese, S. (2016), *Cybersecurity Capacity Maturity Model for Nations (CMM)*, Università di Oxford.

CSIRT Maturity - Self-assessment Tool, (senza data), disponibile all'indirizzo: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool, (senza data), disponibile all'indirizzo: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E., (2017), Public Private Partnerships (PPP).

Darra, E., (no date), *Welcome to the NCSS Training Tool*.

Dekker, M. A. C. (2014), *Technical Guideline on Incident Reporting*, disponibile all'indirizzo: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C., (2014), *Technical Guideline on Security Measures*, disponibile all'indirizzo: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C., (2015), *Guideline on Threats and Assets*, disponibile all'indirizzo: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia, (2016), *Cybersecurity Strategy*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.*, (2014), *Privacy and data protection by design - from policy to engineering*, disponibile all'indirizzo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Ferette, L., (2016), *NIS Directive and national* (2015), *Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises*, disponibile all'indirizzo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., Unione europea e Agenzia per la sicurezza delle reti e dell'informazione, (2015), *The 2015 report on national and international cyber security exercises: survey, analysis and recommendations*, disponibile all'indirizzo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Galan Manso, C. et al., (2015), *Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises*, disponibile all'indirizzo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Gazzetta ufficiale dell'Unione europea (2008), Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32008L0114&from=IT

Ghent University et al., (2017), «Evaluating Business Process Maturity Models», Journal of the Association for Information Systems, disponibile all'indirizzo: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Governo danese - Ministero delle finanze (2018), *Danish Cyber and Information Security Strategy*, disponibile all'indirizzo: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Governo dei Paesi Bassi (2018), *National Cyber Security Agenda*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Governo del Belgio (2012), *Cyber Security Strategy*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Governo dell'Irlanda, (2019), *National Cyber Security Strategy*, disponibile all'indirizzo: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Governo dell'Ungheria, (2018), *Strategy for the Security of Network and Information Systems*, disponibile all'indirizzo: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Governo della Bulgaria, (2015), *National Cyber Security Strategy - Cyber-resistant Bulgaria 2020*.

Governo della Croazia, (2015), *The National Cyber Security Strategy of The Republic of Croatia*, disponibile all'indirizzo: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Governo della Grecia, (2017), *National Cyber Security Strategy*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Governo della Lettonia, (2014), *Cyber Security Strategy of Latvia*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Governo della Romania, (2013), *Cyber security strategy of Romania*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Governo della Slovacchia (2015), *Cyber Security Concept of the Slovak Republic*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Governo della Spagna, (2019), *National Cyber Security Strategy*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Governo svedese (2017), *Nationell strategi för samhällets informations- och cybersäkerhet*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Institute of Internal Auditors (ed.), (2009), *Internal audit capability model (IA-CM) for the public sector: overview and application guide*, Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

J.D., R. D. B., (2019), «Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework», International Review of Law.

Liveri, D. et al., (2014), *An evaluation framework for national cyber security strategies*, Eraklion, ENISA. disponibile all'indirizzo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. *et al.*, (2014), *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks*, disponibile all'indirizzo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Ministero degli affari economici e delle comunicazioni, (2019), *Cybersecurity Strategy – Republic of Estonia*, disponibile all'indirizzo: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministero della competitività e dell'economia digitale, marittima e dei servizi, (2016), *Malta Cyber Security Strategy*, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Ministero della difesa nazionale della Repubblica di Lituania, (2018), Malta Cyber Security Strategy.

Ministro federale dell'interno (2011), Cyber Security Strategy for Germany, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

National Cyber Security Strategies - Interactive Map (senza data). disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

National Cybersecurity Strategies Evaluation Tool (2018), disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

National Institute of Standards and Technology, (2018), *Framework for Improving Critical Infrastructure Cybersecurity*, Versione 1.1, Gaithersburg, MD: Istituto nazionale per gli standard e la tecnologia, disponibile all'indirizzo: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group, (2008), *Business Process Maturity Model*, disponibile all'indirizzo: https://www.omg.org/spec/BPMM/1.0/PDF

OCSE, Unione europea e Centro comune di ricerca - Commissione europea, (2008), *Handbook on Constructing Composite Indicators: Methodology and User Guide*, OCSE, disponibile all'indirizzo: https://www.oecd.org/sdd/42495745.pdf.

Organizzazione per la cooperazione e lo sviluppo economici (OCSE), (2012), *Cybersecurity policy making at a turning point*, disponibile all'indirizzo: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E., (2012), *Good Practice Guide on National Exercises*.

Ouzounis, E., (2012), *National Cyber Security Strategies - Practical Guide on Development and Execution*.

Portesi, S., (2017), *Improving Cooperation between CSIRTs and Law Enforcement*: *Legal and Organisational Aspects*.

Presidenza del Consiglio dei ministri (2017), The Italian Cybersecurity Action Plan, disponibile all'indirizzo: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Progetto CyberCrime@IPA del Consiglio d'Europa e dell'Unione europea, Task force per la criminalità informatica del Progetto globale sulla criminalità informatica del Consiglio d'Europa e dell'Unione europea (2011), *Specialised cybercrime units - Good practice study*, disponibile all'indirizzo: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Rady Ministrów, (2019), *Dziennik Urzędowy Rzeczypospolitej Polskiej*, disponibile all'indirizzo: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Sarri, A., Kyranoudi, P. e Agenzia dell'Unione europea per la cibersicurezza (2019), *Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies*, disponibile all'indirizzo: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Segretariato generale del comitato per la sicurezza, (2019), *Finland's Cyber Security Strategy 2019*, disponibile all'indirizzo: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Smith, R. (2015), *Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010*

Smith, R., (2016), «Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016», in Smith, R., Core EU Legislation, Londra: Macmillan Education, disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Stavropoulos, V. (2017), *European Cyber Security Month 2017*.

The White House (2018), *National Cyber Strategy of the United States of America*, disponibile all'indirizzo: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., et al. (2011), *Cyber Europe Report*, disponibile all'indirizzo: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. e Agenzia dell'Unione europea per la cibersicurezza (2013), *National-level risk assessments: an analysis report*, disponibile all'indirizzo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., et al. (2015), *Report on cyber-crisis cooperation and management*, disponibile all'indirizzo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A., et al. (2015), *Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises*, disponibile all'indirizzo: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

Ufficio del commissario delle comunicazioni elettroniche e dei regolamenti postali, (2012), *Cybersecurity Strategy of the Republic of Cyprus*.

Ufficio del Primo Ministro francese, (2014), *French National Digital Security Strategy*, disponibile all'indirizzo: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Ufficio esecutivo del Presidente, (2015), Memorandum for Heads of Executive Departments and Agencies, disponibile all'indirizzo: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

UK National Cyber Security Strategy 2016-2021 (2016), disponibile all'indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Unione europea e Agenzia per la sicurezza delle reti e dell'informazione, (2017), *Handbook on security of personal data processing*, disponibile all'indirizzo: http://dx.publications.europa.eu/10.2824/569768

Unione europea e Agenzia per la sicurezza delle reti e dell'informazione, (2014), *ENISA CERT inventory of CERT teams and activities in Europe*, disponibile all'indirizzo: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Unione internazionale delle telecomunicazioni (UIT), (2018), *Guide to developing a national cybersecurity strategy*, disponibile all'indirizzo: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Unione internazionale delle telecomunicazioni (UIT), (2018), *The Global Cybersecurity Index*, disponibile all'indirizzo: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Università di Innsbruck et al. (2009), *Understanding Maturity Models*.

Wamala, D. F. (2011), *ITU National Cybersecurity Strategy Guide*, disponibile all'indirizzo: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007), «The Community Cyber Security Maturity Model», in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)

ALLEGATO C – ALTRI OBIETTIVI STUDIATI

Gli obiettivi illustrati di seguito sono stati studiati nell'ambito della fase di ricerca a tavolino e delle interviste condotte dall'ENISA. I seguenti obiettivi non fanno parte del quadro di valutazione delle capacità a livello nazionale, ma fanno luce su argomenti che vale la pena trattare. Ognuno dei sottocapitoli sotto riportati fornirà una spiegazione del motivo per cui l'obiettivo è stato scartato.

- Sviluppare strategie di cibersicurezza specifiche per i settori
- Lottare contro le campagne di disinformazione
- Proteggere le tecnologie di punta (5G, IA, informatica quantistica, ecc.)
- Garantire la sovranità dei dati
- Fornire incentivi per lo sviluppo del settore delle assicurazioni informatiche

Sviluppare strategie di cibersicurezza specifiche per i settori

L'adozione di strategie specifiche per i settori rivolte a interventi e incentivi settoriali introduce certamente una capacità decentralizzata più forte. Si adatta in particolare agli Stati membri i cui gli OES devono confrontarsi con diversi quadri e regolamenti e dove esistono molte dipendenze a causa della natura trasversale della cibersicurezza. In diversi Stati membri è infatti comune la presenza di decine di autorità nazionali e organismi di regolamentazione che conoscono le specificità di ogni settore e che hanno il mandato di applicare una regolamentazione specifica per ogni settore.

La Danimarca, ad esempio, ha avviato sei strategie mirate che riguardano gli sforzi di cibersicurezza e sicurezza delle informazioni nei settori più critici, allo scopo di sviluppare una più forte capacità decentralizzata nella sicurezza informatica e delle informazioni. Ogni «unità settoriale» contribuirà, tra l'altro, alle valutazioni delle minacce a livello settoriale, al monitoraggio, agli esercitazioni di preparazione, alla costituzione di sistemi di sicurezza, alla condivisione delle conoscenze e alle istruzioni. Le strategie specifiche per i settori interessano i settori seguenti:

- energia;
- assistenza sanitaria;
- trasporti;
- telecomunicazione;
- finanza;
- marittimo.

Altri Stati membri hanno espresso interesse verso la considerazione di strategie di cibersicurezza specifiche per settore, per riflettere tutti i requisiti normativi. Si deve tuttavia notare che tale obiettivo potrebbe non essere adatto a tutti gli Stati membri, per via delle relative dimensioni, politiche nazionali e maturità. La grande difficoltà di garantire che il quadro possa tenere conto di tutte le specificità ha spinto l'ENISA a non inserire questo obiettivo nel quadro.

Lottare contro le campagne di disinformazione

Gli Stati membri integrano la protezione dei principi fondamentali, come i diritti umani, la trasparenza e la fiducia pubblica, nelle loro strategie nazionali di cibersicurezza. Si tratta di un

aspetto molto importante, in particolare quando si tratta di disinformazione diffusa attraverso i mezzi di comunicazione tradizionali o le piattaforme dei social media. Inoltre, la cibersicurezza è attualmente una delle maggiori sfide elettorali: attività come la diffusione di informazioni false o di propaganda negativa sono state infatti osservate in vari paesi nel periodo che precede elezioni importanti. Questa minaccia ha il potenziale di minare il processo democratico dell'UE. A livello europeo, la Commissione ha delineato un piano d'azione ([32]) per intensificare gli sforzi volti a contrastare la disinformazione in Europa. Il piano si concentra su 4 aree chiave (rilevamento, cooperazione, collaborazione con le piattaforme online e sensibilizzazione) e serve a costruire le capacità dell'UE, nonché a rafforzare la cooperazione tra gli Stati membri.

Quattro dei 19 paesi intervistati hanno espresso l'intenzione di affrontare la questione della disinformazione e della propaganda nella loro NCSS.

La NCSS francese ([33]) sottolinea ad esempio che: «è responsabilità dello Stato informare i cittadini in merito ai rischi delle tecniche di manipolazione e di propaganda utilizzate da attori malintenzionati su Internet». Ad esempio, dopo gli attacchi terroristici contro la Francia nel gennaio 2015, il governo ha costituito una piattaforma informativa sui rischi legati alla radicalizzazione islamica attraverso le reti di comunicazione elettronica: «Stop-djihadisme.gouv.fr ». Questo approccio potrebbe essere esteso per rispondere ad altri fenomeni di propaganda o destabilizzazione.

In un altro esempio, la NCSS della Polonia per il 2019-2024 ([34]) afferma che: «contro le attività di manipolazione, come le campagne di disinformazione, sono necessarie azioni sistemiche per sensibilizzare i cittadini nel contesto della verifica dell'autenticità delle informazioni e della risposta ai tentativi di distorsione».

Tuttavia, durante le interviste condotte dall'ENISA, diversi Stati membri hanno dichiarato di non affrontare la questione nell'ambito della NCSS come una minaccia alla cibersicurezza, bensì a un livello sociale più ampio, per esempio, attraverso iniziative politiche.

Proteggere le tecnologie di punta (5G, IA, l'informatica quantistica, ecc.)

Considerata la costante espansione dell'attuale panorama delle minacce informatiche, lo sviluppo di nuove tecnologie porterà molto probabilmente ad un aumento dell'intensità e del numero di attacchi informatici e alla diversificazione dei metodi, dei mezzi e degli obiettivi impiegati dagli autori delle minacce. Nel frattempo, queste nuove soluzioni tecnologiche sotto forma di tecnologie all'avanguardia hanno il potenziale per diventare gli elementi costitutivi del mercato digitale europeo. Al fine di salvaguardare la crescente dipendenza digitale degli Stati membri e l'avvento di nuove tecnologie, dovrebbero essere stabiliti incentivi e politiche complete per sostenere lo sviluppo e l'implementazione sicuri e affidabili di queste tecnologie nell'UE.

Durante la fase di ricerca a tavolino condotta sulle NCSS degli Stati membri, le seguenti tecnologie d'avanguardia sono state proposte come interessanti per gli Stati membri: 5G, IA, informatica quantistica, crittografia, edge computing, veicoli connessi e autonomi, big data e smart data, blockchain, robotica e IoT.

([32]) https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
([33]) https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
([34]) http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Nello specifico, all'inizio del 2020 la Commissione europea ha pubblicato una comunicazione che invita gli Stati membri a intervenire per attuare la serie di misure raccomandate nelle conclusioni relative all'insieme di strumenti per il 5G ([35]). Questo insieme di strumenti per il 5G fa seguito alla Raccomandazione (UE) 2019/534 sulla cibersicurezza delle reti 5G, adottata dalla Commissione nel 2019, che auspica un approccio europeo unificato alla sicurezza delle reti 5G ([36]).

Durante le interviste condotte dall'ENISA, è emerso che si tratta di un argomento trasversale che viene affrontato in tutta la NCSS, piuttosto che un obiettivo specifico di per sé.

Garantire la sovranità dei dati

Da un lato, il ciberspazio può essere considerato un formidabile spazio comune globale, facilmente accessibile, che fornisce un alto livello di connettività ed è in grado di produrre grandi opportunità di crescita socio-economica. Dall'altro, si caratterizza anche per la sua debole giurisdizione, la difficoltà di imputare le azioni ai relativi autori, la mancanza di frontiere e sistemi interconnessi che possono essere porosi e i cui dati possono essere oggetto di furto o addirittura accesso da parte di governi stranieri. Oltre a queste due prospettive, l'ecosistema digitale è contrassegnato dalla concentrazione di piattaforme di servizi online e infrastrutture nelle mani di pochissimi portatori di interessi. Tutti gli aspetti sopra citati portano gli Stati membri a promuovere la sovranità digitale. Raggiungere la sovranità digitale significa che i cittadini e le imprese sono in grado di prosperare pienamente utilizzando servizi digitali e prodotti TIC affidabili, senza alcun timore per i propri dati personali o risorse digitali, la propria autonomia economica o la propria influenza politica.

La sovranità dei dati o sovranità digitale è sostenuta dagli Stati membri a livello nazionale ed europeo. Anche se gli Stati membri non sembrano affrontare la questione direttamente nelle loro NCSS come obiettivo specifico, la trattano come principio trasversale o delineano la loro intenzione di garantire la sovranità digitale a livello nazionale in pubblicazioni ad hoc, concentrandosi sulle tecnologie chiave. Ad esempio, nella revisione strategica francese del 2018 sulla ciberdifesa, si afferma che «il controllo delle seguenti tecnologie è di fondamentale importanza per garantire la sovranità digitale: crittografia delle comunicazioni, rilevamento degli attacchi informatici, radiomobile privato, cloud computing e intelligenza artificiale» ([37]).

A livello europeo, gli Stati membri partecipano attivamente alla definizione della strategia europea per i dati (COM/2020/66 final) e alla costruzione del quadro di certificazione dell'UE per i prodotti, i servizi e i processi digitali TIC stabilito dal Regolamento dell'UE sulla cibersicurezza (2019/881) per garantire l'autonomia digitale strategica a livello europeo.

La fase di intervista con gli Stati membri ha evidenziato che il tema della sovranità digitale è spesso considerato una questione più ampia e non limitata alla cibersicurezza. Pertanto, gli Stati membri non trattano l'argomento nelle loro NCSS e, nei pochi casi in cui ciò avviene, non viene trattato come un obiettivo specifico in sé.

Fornire incentivi per lo sviluppo del settore delle assicurazioni contro i rischi informatici

Lo stato attuale del settore delle assicurazioni contro i rischi informatici mostra un'indiscussa crescita del mercato globale. Si trova tuttavia ancora nella fase iniziale, in quanto i dati devono essere raccolti e molti principi devono ancora essere stabiliti (ad es. copertura del silent cyber risk, rischi informatici sistemici, ecc.). Inoltre, le perdite stimate aggregate dovute agli attacchi informatici in tutto il mondo sono diversi ordini di grandezza superiori all'attuale capacità di copertura del settore assicurativo per il rischio informatico (documento di lavoro del FMI - Cyber

([35]) https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission
([36]) https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32019H0534
([37]) http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143). Tuttavia, lo sviluppo del settore delle assicurazioni contro i rischi informatici può certamente produrre benefici e gettare le basi per meccanismi virtuosi. Meccanismi di assicurazione contro i rischi informatici possono infatti aiutare a:

- sensibilizzare riguardo ai rischi connessi alla cibersicurezza nelle aziende;
- valutare l'esposizione ai rischi connessi alla cibersicurezza in modo quantitativo;
- migliorare la gestione dei rischi connessi alla cibersicurezza;
- fornire sostegno alle organizzazioni che sono vittime di attacchi informatici;
- coprire i danni (materiali e non) causati da un attacco informatico.

Alcuni Stati membri hanno iniziato a lavorare su questo argomento. Ad esempio:

- L'Estonia ha adottato un approccio «aspettare e vedere» nella sua NCSS: «Per mitigare i rischi informatici nel settore privato in generale, saranno analizzate la domanda e l'offerta di servizi di assicurazione contro i rischi informatici in Estonia e, su tale base, saranno concordati principi di cooperazione per le parti correlate, comprese condivisione delle informazioni, preparazione della valutazione del rischio, ecc. Attualmente, i fornitori di servizi di assicurazione contro i rischi informatici sono pochi sul mercato estone ed è necessario prima mappare chi offre cosa. La complessità della tutela assicurativa è spesso ritenuta un ostacolo allo sviluppo del mercato delle assicurazioni contro i rischi informatici».
- Il Lussemburgo sostiene specificamente lo sviluppo del settore delle assicurazioni contro i rischi informatici nella sua NCSS: «Obiettivo 1: creare nuovi prodotti e servizi. Per mettere in comune i rischi e incoraggiare le vittime di incidenti informatici digitali a chiedere l'aiuto di esperti per gestire l'incidente e ripristinare un sistema colpito da un atto malevolo, le compagnie di assicurazione saranno invitate a creare prodotti specifici per il settore dell'assicurazione contro i rischi informatici».

I feedback degli intervistati sono stati piuttosto eterogenei su questo argomento: alcuni Stati membri hanno dichiarato che il tema dell'assicurazione contro i rischi informatici è recentemente diventato un argomento di discussione, mentre altri hanno affermato che, sebbene l'argomento sia promettente, il settore non è ancora sufficientemente maturo. Un numero elevato di intervistati ha tuttavia dichiarato che l'argomento non viene affrontato nell'ambito della NCSS, perché ritenuto troppo specifico o perché non rientra nell'ambito della NCSS.

TP-02-21-253-IT-N

Informazioni sull'Agenzia dell'Unione europea per la cibersicurezza

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento dell'UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza contribuisce alla politica dell'UE in materia di sicurezza informatica, migliora l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche del futuro. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Per maggiori informazioni, visitare il sito www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-482-4
DOI: 10.2824/144346