

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

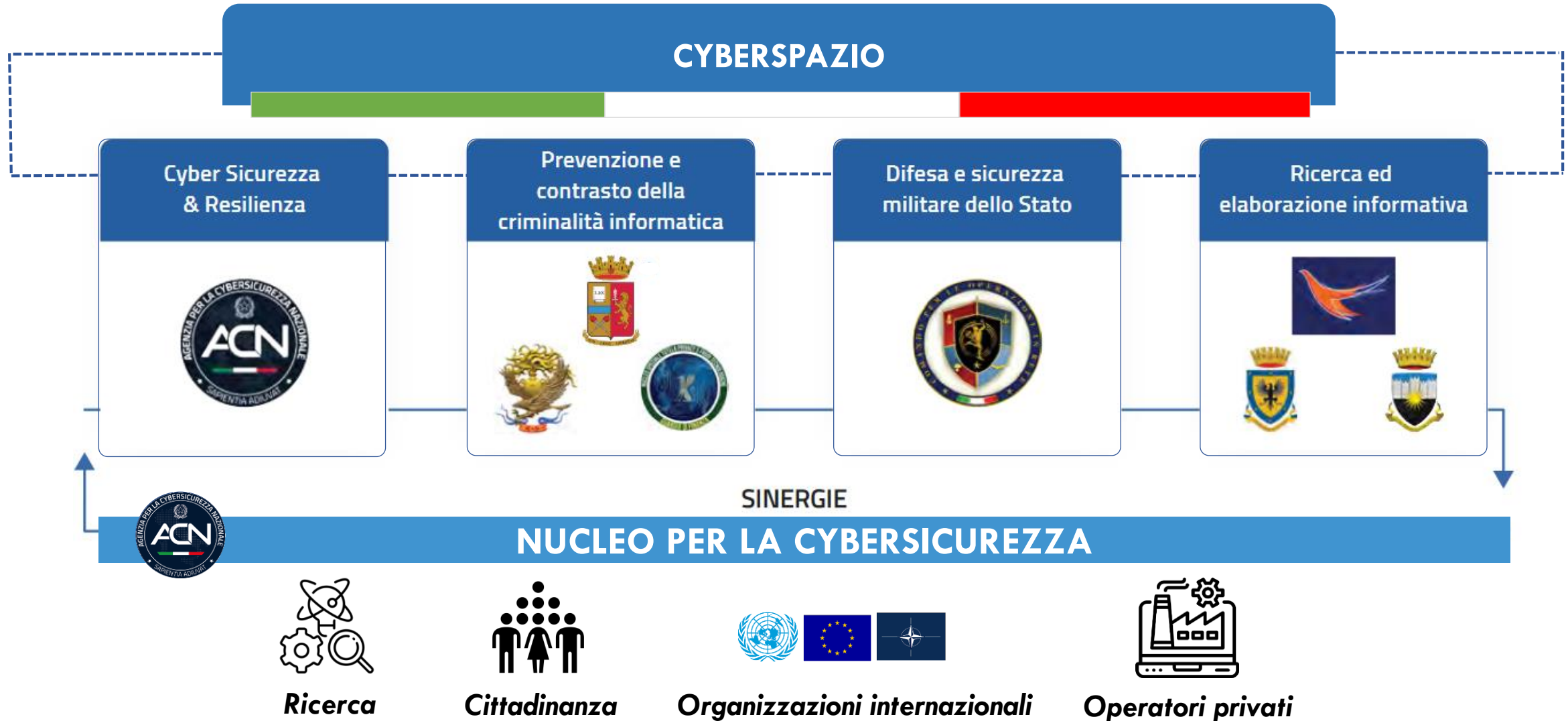
*Servizio Programmi Industriali,
Tecnologici, di Ricerca e Formazione*



Architettura Nazionale Cybersicurezza



Gli Organi a difesa dell'architettura nazionale cyber



Autorità Nazionale per la Cybersicurezza



Strategia di Cybersicurezza Nazionale



Overview Strategia

Tra i principali compiti dell'Agencia c'è l'attuazione della **Strategia Nazionale di Cybersicurezza 2022 - 2026**, adottata dal Presidente del Consiglio con DPCM del 17 Maggio 2022. La Strategia mira ad affrontare le sfide inerenti al rafforzamento della resilienza nella transizione digitale del sistema Paese.

LE SFIDE DA AFFRONTARE

Rafforzamento della resilienza nella transizione digitale del sistema Paese

Conseguimento dell'autonomia strategica nella dimensione cibernetica

Anticipazione dell'evoluzione della minaccia cyber

Gestione di crisi cibernetiche in scenari geopolitici complessi

Contrasto alla disinformazione online

GLI OBIETTIVI DELLA STRATEGIA



Documenti a supporto della Strategia



Strategia Nazionale di Cybersicurezza 2022-2026

Volta a pianificare, coordinare e attuare misure tese a rendere il Paese più sicuro e resiliente.



Piano di implementazione della Strategia 2022-2026

Descrizione dettagliata delle 82 misure da realizzare, suddivise per aree tematiche e con indicazione degli attori responsabili per la loro attuazione e tutti gli altri soggetti a vario titolo interessati.




Manuale operativo implementazione misure 2022-2026

Descrizione, per ogni misura, delle metriche e degli indicatori di misurazione individuati, l'anno di prevalente implementazione delle stesse, oltre alle relative linee guida.

Risorse finanziarie per la Strategia di Cybersicurezza Nazionale

 **LEGGE DI BILANCIO 2023 – Ambito Cybersecurity** 

 **PNRR**
Obiettivo 1.5 (ACN soggetto attuatore)

 **FONDI DL 82/2021 Istituzione ACN**

 **Eventuali FONDI EU**



AMMINISTRAZIONI RESPONSABILI DELL'ATTUAZIONE DELLE MISURE

- Amministrazioni CIC
 - MAECI
 - Min. Interno
 - Min. Giustizia
 - Min. Difesa
 - MEF
 - MIMIT
 - MASE
 - MUR
 - MIT
- Presidenza del Consiglio dei Ministri (DAGL, DIE e DTD)
- Ufficio del Consigliere Militare del Presidente del Consiglio
- Ministero dell'Istruzione e del Merito
- CINI
- Atenei



Legge di Bilancio 2023

Al fine di dare attuazione alla **Strategia Nazionale di Cybersicurezza** e di rendere effettivo il relativo piano di implementazione, sono stati istituiti nello stato di previsione del Ministero dell'economia e finanze, secondo l'articolo 1 della legge 29 dicembre 2022 n. 197 (Legge di Bilancio 2023), i Fondi riportati di seguito.

L'Agenzia coordina e monitora l'attuazione degli interventi.

	2023	2024	2025	2026-2037
Attuazione	70 M€	90 M€	110€ M	150 M€ ANNUI
Gestione	10 M€	50 M€	70€ M	70 M€ ANNUI



FONDO PER L'ATTUAZIONE: destinato a finanziare, anche ad integrazione delle risorse già assegnate a tale fine, gli investimenti volti al conseguimento dell'autonomia tecnologica in ambito digitale, nonché l'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali.



FONDO PER LA GESTIONE: destinato a finanziare le attività di gestione operativa.

I Fondi per l'**attuazione** e per la **gestione** della Strategia sono assegnati alle **amministrazioni individuate dal piano di implementazione** con uno o più decreti del Presidente del Consiglio dei ministri*, adottati su proposta dell'Agenzia per la cybersicurezza nazionale e d'intesa con il Ministero dell'economia e delle finanze.



*La prima assegnazione è avvenuta con Decreto del Presidente del Consiglio dei Ministri del 9 agosto 2023 (G.U. Serie Generale n. 230 del 2 ottobre 2023) per **MEF, Interno, MAECI, MUR, Giustizia, PCM – DIE, Presidenza della Repubblica, Camera dei deputati, Corte Costituzionale.**

Ricerca e MUR nella Strategia Nazionale: un ruolo chiave



Misure con coinvolgimento MUR
11



Soggetto Responsabile
10



Soggetto Interessato
1



300k€ triennio 2023-2025 per la misura #71



Avviare iniziative e campagne di sensibilizzazione volte a promuovere le competenze degli utenti e i comportamenti responsabili nello spazio cibernetico

Misure

#71, #72



Favorire la ricerca e lo sviluppo, specialmente nelle nuove tecnologie, promuovendo l'inclusione dei principi di cybersicurezza

#54, #61, #67



Favorire l'organizzazione di iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica

#59, #60, #65, #66

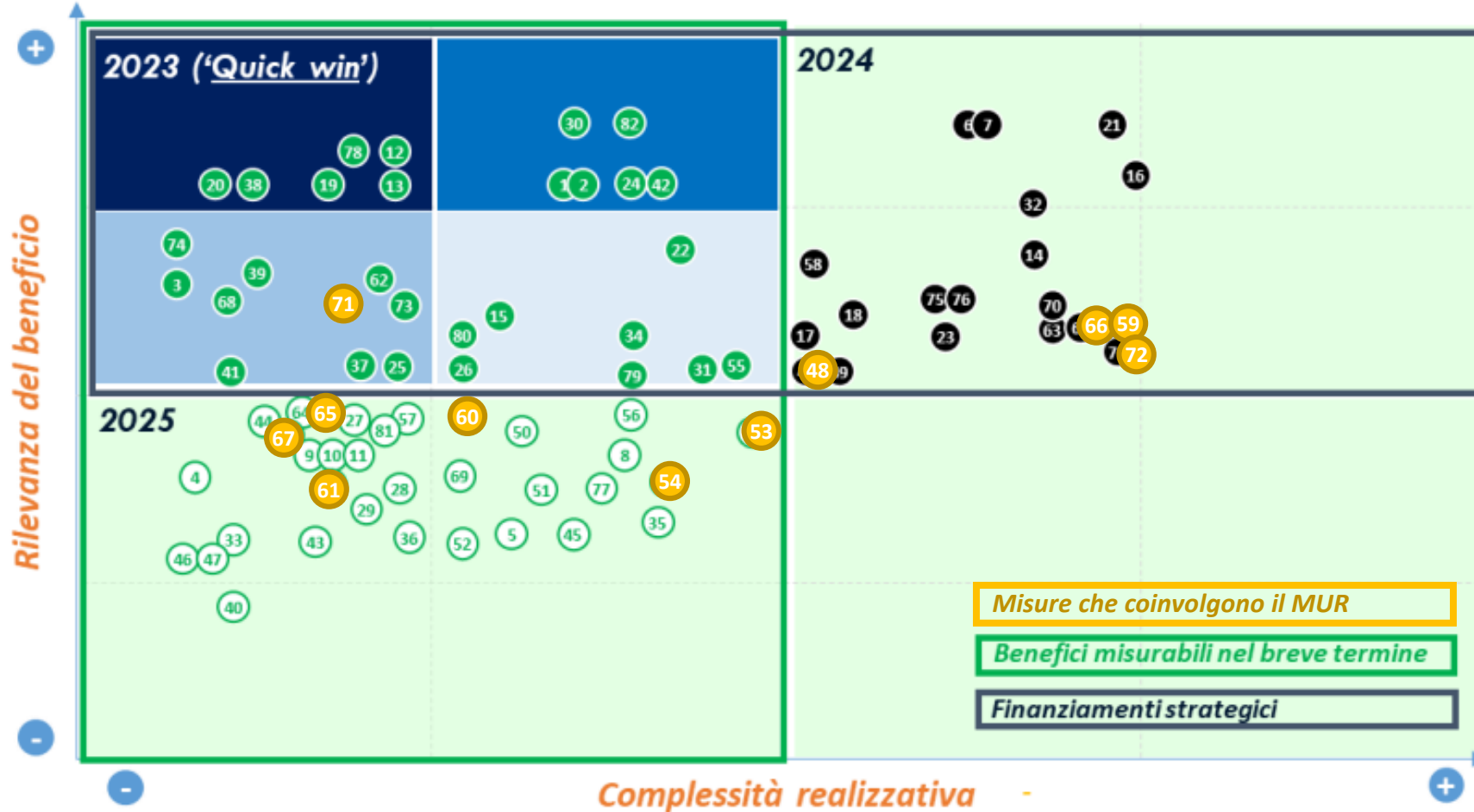


Promuovere ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia

#53

Prioritizzazione delle misure

Come riportato nel Manuale Operativo, sono state individuate le **misure di prioritaria attuazione** sulla base della **rilevanza del beneficio** e la **complessità realizzativa**, considerando anche le **propedeuticità** tra le diverse misure. Per ogni misura viene riportato l'anno di prevalente implementazione, utile ai fini della pianificazione delle attività dei singoli interventi.



Per eventuali richieste informative scrivere a strategia-cybersecurity@acn.gov.it

Gli obiettivi della Strategia

Il Piano di implementazione riporta, per ciascuno degli **obiettivi** della Strategia Nazionale di Cybersicurezza – **Protezione, risposta e sviluppo** – le **misure** da porre in essere per il loro conseguimento, suddivise per aree tematiche:

PROTEZIONE



24 misure

volte alla **protezione degli asset strategici nazionali**. Di particolare importanza è lo **sviluppo di strategie innovative per la verifica e la valutazione della sicurezza delle infrastrutture ICT**

RISPOSTA



21 misure

volte alla **risposta alle minacce, agli incidenti e alle crisi cyber nazionali**, attraverso l'impiego di elevate capacità nazionali di monitoraggio, rilevamento, analisi

SVILUPPO



13 misure


volte allo **sviluppo consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale**

FATTORI ABILITANTI



23 misure

volte alla realizzazione dei **fattori abilitanti**, quali la formazione, la promozione della cultura della sicurezza cibernetica e cooperazione.



**Obiettivo di protezione: PNRR -
Investimento 1.5 «Cybersecurity»**

Contesto di riferimento

L'Investimento 1.5 “Cybersecurity” della Missione 1 – Componente 1 – Asse 1 del PNRR, per cui l’Agenzia è stata individuata quale Soggetto attuatore tramite un accordo di collaborazione con il Dipartimento per la trasformazione digitale (DTD) della Presidenza del Consiglio dei ministri, ha come fulcro il **rafforzamento dell’ecosistema digitale nazionale**, il relativo **potenziamento dei servizi di gestione della minaccia cyber e lo sviluppo dell’autonomia tecnologica nazionale**, nonché il **supporto all’avvio e all’incremento delle capacità dell’ACN**.

Stream Progettuali

SERVIZI CYBER NAZIONALI



Attivazione e supporto alla piena operatività dei servizi dell’Agenzia per il potenziamento delle capacità nazionali di prevenzione, monitoraggio, risposta e mitigazione di minacce cyber, in linea con la legislazione nazionale del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e con la Direttiva europea NIS

INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER PER LA PA



Potenziamento delle capacità cyber della Pubblica Amministrazione per il miglioramento della resilienza e della relativa postura di sicurezza

LABORATORI DI SCRUTINIO E CERTIFICAZIONE TECNOLOGICA



Potenziamento delle competenze e capacità nazionali di scrutinio, valutazione e certificazione tecnologica a supporto dell’implementazione del PSNC, per un’adozione consapevole e ponderata di nuove tecnologie digitali

Interventi di potenziamento della resilienza cyber per la PA: panoramica Avvisi e Accordi

Per la realizzazione dell'Investimento, l'Agenzia sta prevedendo due modalità attuative:

- **Interventi a Titolarità** – in cui ACN opera direttamente in veste di Soggetto attuatore del progetto a favore di Soggetti beneficiari
- **Interventi a Regia** – in cui ACN finanzia progetti rientranti nella titolarità di altri soggetti pubblici o privati

Panoramica

DOTAZIONE FINANZIARIA

623 M€

Totale dei fondi destinati all'Investimento 1.5 "Cybersecurity" nell'ambito del PNRR

AVVISI PUBBLICATI E ACCORDI STIPULATI

13

Totale degli Avvisi Pubblici «a titolarità» e «a regia» pubblicati e degli Accordi stipulati con altre PA in ambito Cyber Defence

IMPORTI FINANZIATI

289.03 M€

Totale degli importi destinati ai Soggetti finanziati nell'ambito degli Avvisi Pubblici conclusi e degli Accordi Cyber Defence stipulati

Avanzamento

187 interventi

52 Amministrazioni coinvolte
19 soggetti privati

23 Chiusi

137 In corso

27 In attivazione

PROSSIME INIZIATIVE

Ricevute le candidature da parte di regioni e province autonome nell'ambito dell'Avviso dedicato **all'attivazione e potenziamento di CSIRT regionali**

Ulteriori Avvisi Pubblici destinati alle Pubbliche Amministrazioni Centrali e Locali

Misure di riferimento

	Misura	Anno avvio implementazione	Attori Responsabili	Altri Soggetti Interessati
55	Promuovere la digitalizzazione e l'innovazione, nonché rafforzare la sicurezza nella Pubblica Amministrazione , anche mediante l'impiego delle risorse del PNRR.	2023	ACN, DTD	MPA, Altre Amministrazioni centrali, Regioni e Province autonome
14	Coordinare interventi di potenziamento delle capacità di identificazione, monitoraggio e controllo del rischio cyber nella Pubblica Amministrazione per la messa in sicurezza dei dati e dei servizi dei cittadini .	2024	ACN	DTD, MPA

Panoramica Avvisi e Accordi

Soggetti finanziati

12 **Avviso 1 PAC a ristoro**

15,5 Mln/€

Interventi di potenziamento della resilienza cyber

Organi Costituzionali e di rilievo Costituzionale, Agenzie Fiscali e Amministrazioni del nucleo per la Cybersicurezza

Soggetti finanziati

12 **Avviso 2 PAC a servizio**

7,85 Mln/€

Interventi di potenziamento della resilienza cyber

Organi Costituzionali e di rilievo Costituzionale, Agenzie Fiscali e Amministrazioni del nucleo per la Cybersicurezza

Soggetti finanziati

35 **Avviso 3 PAL a ristoro**

63,69 Mln/€

Interventi di potenziamento della resilienza cyber

Regioni, Comuni capoluogo facenti parte di Città metropolitane e Province autonome

Soggetto finanziato

1 **Avviso 4 PAC a ristoro**

1,16 Mln/€

Interventi di potenziamento delle capacità di analisi e scrutinio software nella PAC

Amministrazioni Pubbliche Centrali individuate nella Presidenza del Consiglio dei Ministri, nei Ministeri e nelle Agenzie Fiscali

Soggetti finanziati

27 **Avviso 5 Pubblici/Privati a ristoro**

4,33 Mln/€

Erogazione di contributi per l'attivazione di laboratori di prova per l'area di accreditamento Software e Network

Soggetti destinatari

21 **Avviso 6 PAL a ristoro**

28 Mln/€

Erogazione di interventi finalizzati all'attivazione o al potenziamento di CSIRT Regionali

Regioni e Province autonome

Soggetti coinvolti

49 **Avviso 7 PAC a servizio**

15 Mln/€

Interventi di potenziamento della resilienza cyber

Organi costituzionali e a rilevanza costituzionale, Ministeri, Agenzie fiscali, Enti di regolazione dell'attività economica, Autorità amministrative indipendenti, Enti a struttura associativa

168,5 Mln/€

Accordi Cyber-defence


Interventi di potenziamento della resilienza cyber

MINISTERO DELLA DIFESA, MINISTERO DELL'INTERNO, Carabinieri, Ministero della Giustizia, CONSIGLIO DI STATO


Obiettivo di risposta: Servizi Cyber Nazionali



Verso una rete di CSIRT nazionale

SERVIZI CYBER NAZIONALI 



Attivazione e supporto alla piena operatività dei servizi dell’Agenzia per il potenziamento delle capacità nazionali di prevenzione, monitoraggio, risposta e mitigazione di minacce cyber, in linea con la legislazione nazionale del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e con la Direttiva europea NIS

INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER PER LA PA 

Potenziamento delle capacità cyber della Pubblica Amministrazione per il miglioramento della resilienza e della relativa postura di sicurezza

LABORATORI DI SCRUTINIO E CERTIFICAZIONE TECNOLOGICA 

Potenziamento delle competenze e capacità nazionali di scrutinio, valutazione e certificazione tecnologica a supporto dell’implementazione del PSNC, per un’adozione consapevole e ponderata di nuove tecnologie digitali

- HyperSOC
- ISAC
- Servizi PSNC / NIS
- Agenzia Cybersicurezza Nazionale
- **HPC & AI/ML** 
- **Ispezioni PSNC / NIS**
- **WP7-CERTs** 

MICI – 20
Dispiego integrale dei servizi nazionali di cybersecurity
 **T4 2024**

Misura	Avvio	Attori Responsabili	Altri Soggetti Interessati
<p>33</p> <p>Accrescere le capacità di risposta e ripristino a seguito di crisi cibernetiche implementando una rete di CERT settoriali integrata con lo CSIRT Italia, nonché un piano nazionale di gestione crisi che definisca procedure, processi e strumenti da utilizzare in coordinamento con gli operatori pubblici e privati, con l’obiettivo di assicurare la continuità operativa delle reti, dei sistemi informativi e dei servizi informatici.</p>	2025	ACN, Amministrazioni NCS	Operatori Privati

HPC & AI-ML: Convenzione CINECA - MUR



Firmato, in data 11 settembre 2023, il **protocollo d'intesa tra ACN e il consorzio Cineca**, nell'ambito dell'evento inaugurativo dell'ampliamento della sede di CINECA a Napoli con la realizzazione di un data center ad alta efficienza energetica. Gli **investimenti** per la realizzazione del centro di calcolo, l'acquisizione dei sistemi HPC e i costi operativi e di gestione saranno dell'**ordine di circa 50 milioni di euro, di cui oltre 20 messi a disposizione dall'ACN**.



L'accordo prevede l'acquisizione del sistema High Performance Computing (HPC) dell'Agenzia da collocare presso il nuovo centro di Napoli. Il sistema sarà dedicato al monitoraggio della minaccia cyber centrale, l'**HyperSOC**, anche attraverso l'utilizzo di strumenti di **intelligenza artificiale e machine learning**.



L'ecosistema nazionale per la cybersecurity, coordinato da ACN, avrà accesso alle risorse del sistema HPC di Napoli per lo **sviluppo dei metodi di prevenzione e di salvaguardia della sicurezza informatica del nostro Paese**. Questa azione di coordinamento di un ecosistema nazionale, incentrato sulla realizzazione di una infrastruttura HPC per la cybersecurity rappresenta, inoltre, **un'azione di rilevanza strategica per lo sviluppo di una rete europea di infrastrutture HPC per la cybersecurity**, rispetto alla quale l'Italia assume una posizione di rilievo per la salvaguardia della sovranità europea relativa alla sicurezza informatica dei dati, della loro riservatezza e della privacy delle istituzioni e delle persone.



L'infrastruttura di calcolo nazionale si arricchisce di un importante nodo HPC, **integrato nel sistema europeo di supercalcolo**. Il sistema farà parte di una rete di sistemi complementari del supercomputer Leonardo, e consentirà di **supportare non solo le applicazioni consolidate della fisica, della chimica, delle scienze ambientali e dell'ingegneria, ma soprattutto le applicazioni di apprendimento automatico e di intelligenza artificiale sia classica che generativa**.

Misure di riferimento

	Misura	Anno avvio implementazione	Attori Responsabili	Altri Soggetti Interessati
30	Realizzare un sistema di raccolta e analisi HyperSOC per aggregare, correlare ed analizzare eventi di sicurezza di interesse al fine di individuare precocemente eventuali “pattern” di attacco complessi, nonché abilitare una gestione del rischio cyber in chiave preventiva e integrata tra molteplici sorgenti dati, sfruttando anche infrastrutture di High Performance Computing e tecnologie di Intelligenza Artificiale e il machine learning.	2023	ACN	Atenei, Ricerca, Amministrazioni centrali, Operatori privati, Regioni e Province autonome
32	Creare un’infrastruttura di High Performance Computing dedicata alla cybersecurity nazionale per il potenziamento dei servizi cyber nazionali dell’Agenzia , nonché lo sviluppo di strumenti di simulazione, basati sull’Intelligenza Artificiale e il machine learning, per supportare le fasi di prevenzione, scoperta, risposta e predizione degli impatti di attacchi cyber di natura sistemica.	2024	ACN	Amministrazioni NCS, Atenei, Ricerca, Operatori privati

Obiettivi di sviluppo: Cyber Innovation Network



Struttura del programma «Cyber Innovation Network»



AREA DI INTERVENTO 1

[Progettualità avviata]

Sviluppo di **nuova imprenditorialità innovativa (startup e spin-off)** in collaborazione con primari **programmi di incubazione ed accelerazione**

Obiettivi

- ❑ Costruire una **rete stabile con l'ecosistema dell'innovazione**, per programmi congiunti con l'Agenzia.
- ❑ Creare e sviluppare **nuove realtà imprenditoriali (startup e spin-off)** ad alto contenuto di innovazione nelle aree tecnologiche dell'Agenzia.
- ❑ Supportare la **validazione e lo sviluppo di tecnologie emergenti**, per favorire innovazione e discontinuità tecnologiche.

Benefici alle startup

- ❑ Opportunità di **validare tecnologie e soluzioni** nei contesti di impiego dell'Agenzia.
- ❑ **Contributo a fondo perduto*** per progetti di validazione (fino a 50.000 €) e per progetti di sviluppo (fino a 150.000 €).

*Il contributo complessivo per startup non potrà superare 200.000 € nel rispetto della disciplina degli aiuti di Stato.



AREA DI INTERVENTO 2

[Progettualità pianificata]

Valorizzazione dei risultati della ricerca pubblica in collaborazione con i *Technology Transfer Offices* di Università ed Enti Pubblici di Ricerca

Obiettivi

- ❑ **Ampliare l'Innovation Network** con il coinvolgimento dei TTOs.
- ❑ **Favorire i processi di trasferimento tecnologico**, innalzando il TRL dei risultati della ricerca.
- ❑ Creare una vera e propria **filiera integrata di sostegno all'innovazione**, partendo dalle fasi più a monte della ricerca.

Benefici ai gruppi di ricerca

- ❑ Opportunità di **validare i risultati della ricerca incrementandone il TRL** su filoni tecnologici ed impiego ad alto impatto.
- ❑ **Contributo a fondo perduto** erogato ai **gruppi di ricerca** attraverso il coinvolgimento dei TTOs



Arete tecnologie di cybersecurity presidiate

- Robotica
- Blockchain
- Data Science
- AI
- Quantum
- Computing
- Crittografia

Misure di riferimento (1/2)

	Misura	Anno avvio implementazione	Attori Responsabili	Altri Soggetti Interessati
53	<p>Promuovere ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, riguardo a prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore, anche valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali.</p>	2025	ACN, DTD, MIMIT, MUR , Min. Difesa	Atenei, Ricerca, Regioni e Province autonome
54	<p>Favorire la ricerca e lo sviluppo, specialmente nelle nuove tecnologie, promuovendo l'inclusione dei principi di cybersicurezza e supportando, anche mediante finanziamenti, investimenti pubblici e privati e meccanismi di semplificazione, progetti di sicurezza cibernetica da parte del settore privato – con particolare riferimento alle startup e alle PMI innovative – e dei Centri di competenza e di ricerca attivi sul territorio nazionale.</p>	2025	ACN, DTD, MEF, MIMIT, MUR , Min. Difesa	Operatori privati, Atenei, Ricerca
51	<p>Implementare un Piano per l'industria cyber nazionale volto a sostenere imprese e startup per la progettazione e la realizzazione di prodotti e servizi ad alta affidabilità (tra cui un'infrastruttura di comunicazione nazionale), che rispondano agli interessi strategici del Paese e che possano essere promossi presso Stati like-minded.</p>	2025	MIMIT, DTD, MAECI, AC	Regioni e Province autonome, Min. Difesa (ricerca militare)
64	<p>Prevedere incentivi per lo sviluppo di start-up operanti nel settore della cybersecurity e partnership pubblico-privato con aziende di cybersecurity a conduzione femminile.</p>	2025	MEF, MIMIT, DTD	Min. Lavoro, Regioni e Province autonome
47	<p>Supportare l'operatività dei Digital Innovation Hub e favorirne le sinergie con il Centro nazionale di coordinamento, con i Centri di competenza ad alta specializzazione e con i Cluster tecnologici, per agevolare il trasferimento tecnologico verso le PMI</p>	2025	MIMIT, DTD, ACN	Associazioni di categoria, Atenei, Ricerca

Misure di riferimento (2/2)

	Misura	Anno avvio implementazione	Attori Responsabili	Altri Soggetti Interessati
49	<p>Realizzare un “parco nazionale della cybersicurezza” che ospiti le infrastrutture necessarie allo svolgimento di attività di ricerca e sviluppo nell’ambito della cybersecurity e delle tecnologie digitali, dotato di una struttura “diffusa”, con ramificazioni distribuite sull’intero territorio nazionale.</p>	2024	ACN, DTD, MEF, MIMIT, Min. Difesa (ricerca militare)	Regioni e Province autonome, Atenei, Ricerca, Operatori privati
50	<p>Promuovere l’internazionalizzazione delle imprese italiane che offrono prodotti e servizi di cybersecurity mediante il supporto agli investimenti, all’innovazione e alle esportazioni</p>	2025	MAECI, MIMIT, ACN	-
56	<p>Promuovere la digitalizzazione e l’innovazione del sistema produttivo nazionale, anche mediante l’impiego delle risorse del PNRR.</p>	2025	DTD, MIMIT, ACN	Amministrazioni centrali, Regioni e Province autonome

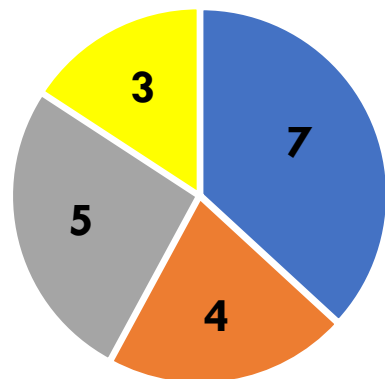
Costruzione del "Cyber Innovation Network"



AREA DI INTERVENTO 1

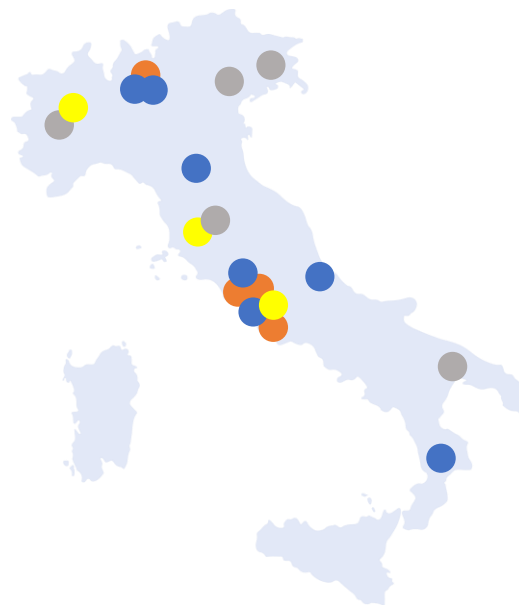
Sviluppo di nuova
imprenditorialità
innovativa

Operatori candidati per categoria



- Venture Capital/Investors
- Corporate/Consulting
- R&D Hub/Incubators with low TRL
- Accelerator pure players

Distribuzione geografica



Accordi sottoscritti



- **Criteri di valutazione: (a) esperienza operatore, (b) qualità del programma proposto, © numero di startup da supportare.**
- **19 operatori selezionati, 63 cybersecurity startups** menzionate nel portafoglio degli operatori.
- Forte focus sulle tematiche di **big data/AI, IoT e Industry 4.0.**
- L'Agenzia è in fase di sottoscrizione degli Accordi di collaborazione con i sei primi Operatori selezionati.

Sviluppo di programmi congiunti su specifici filoni tecnologici

PRINCIPALI ATTIVITÀ



Accordi di Collaborazione **con programmi esistenti e per la definizione di nuovi programmi congiunti** con sei Operatori, mettendo a disposizione un portafoglio di servizi e finanziamenti a supporto dello **sviluppo di imprenditorialità innovativa** (startup e spin-off) su specifici filoni tecnologici.



Attraverso questi programma congiunti, l'Agenzia intende supportare **startup e spin-off** per: **Progetti di validazione** (3-5 mesi), finalizzati a supportare una prima validazione del prototipo e del modello di business.



Progetti di sviluppo (9-12 mesi), finalizzati a supportare lo sviluppo delle soluzioni innovative, rispetto a contesti di impiego di interesse.

✓ **Contributo a fondo perduto*** per progetti di validazione (fino a 50.000 €) e per progetti di sviluppo (fino a 150.000 €).

* I contributi finanziari dell'Agenzia verranno erogati nell'ambito della disciplina degli aiuti di stato, ed in particolare del de minimis

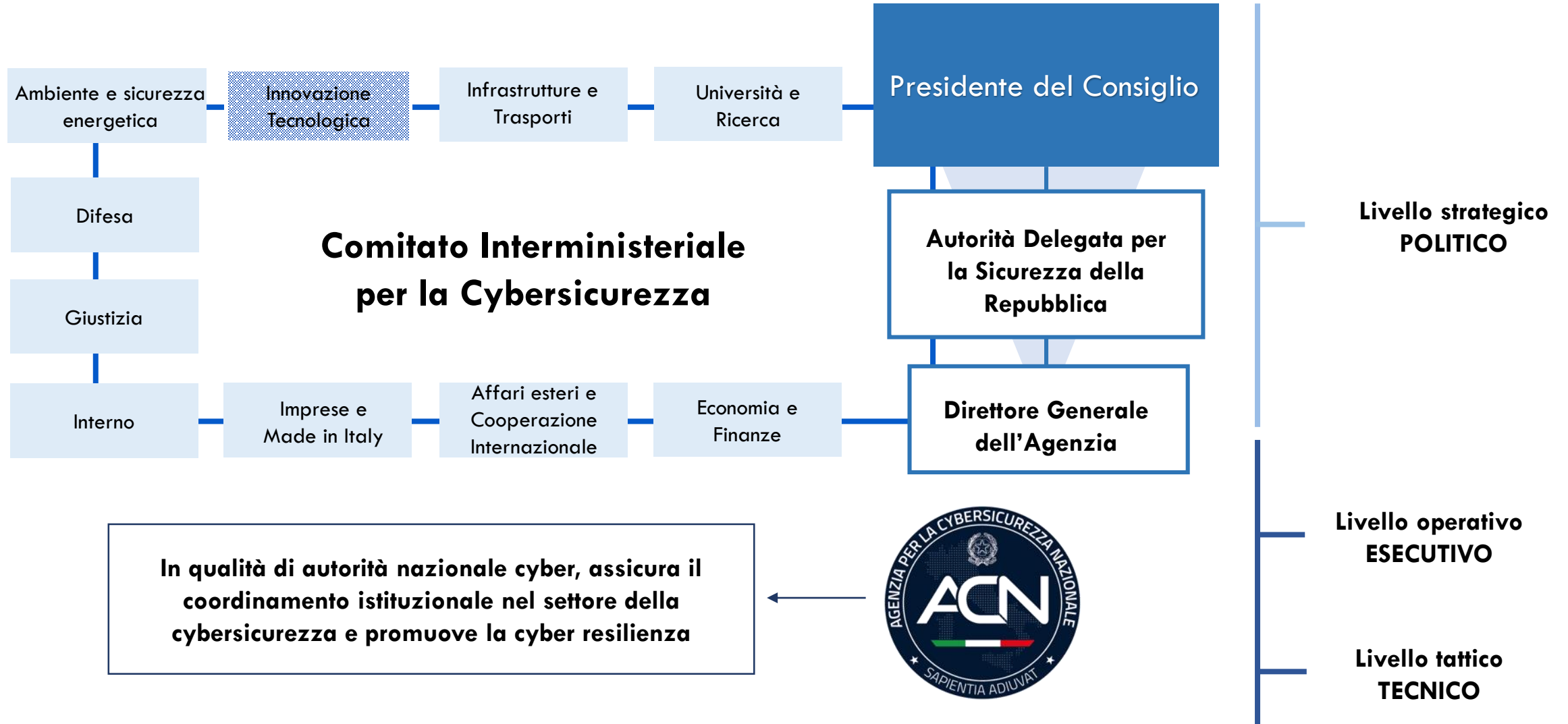
Grazie per l'attenzione



Annex



La Governance della Cybersicurezza



Nucleo per la Cybersicurezza

COMPOSIZIONE

Ordinario

+ altre Amministrazioni, accademia, privati.

Ristretto

Solo amministrazioni e soggetti interessati

Crisi

+ Min. Salute e Dip. VV.FF.
eventualmente + altri soggetti pubblici e privati



FUNZIONI

Proposte di iniziative in materia di cybersicurezza

Pianificazione operativa della risposta a situazioni di crisi cibernetica

Esercitazioni interministeriali

Valutazioni di incidenti rilevanti

Condivisione informazioni

Misure del MUR come Soggetto Responsabile (1/3)

	Misura	Anno avvio implementazione	Attori Responsabili	Altri Soggetti Interessati
53	<p>Promuovere ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, riguardo a prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore, anche valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali.</p>	2025	ACN, DTD, MIMIT, MUR , Min. Difesa	Atenei, Ricerca, Regioni e Province autonome
54	<p>Favorire la ricerca e lo sviluppo, specialmente nelle nuove tecnologie, promuovendo l'inclusione dei principi di cybersicurezza e supportando, anche mediante finanziamenti, investimenti pubblici e privati e meccanismi di semplificazione, progetti di sicurezza cibernetica da parte del settore privato – con particolare riferimento alle startup e alle PMI innovative – e dei Centri di competenza e di ricerca attivi sul territorio nazionale.</p>	2025	ACN, DTD, MEF, MIMIT, MUR , Min. Difesa	Operatori privati, Atenei, Ricerca
59	<p>Potenziare lo sviluppo di percorsi formativi dedicati con diversi livelli di specializzazione in cybersecurity (scuola primaria e secondaria, corsi post-diploma - ITS, corsi universitari di laurea e laurea magistrale, dottorati di ricerca e master, Scuole di formazione delle Pubbliche Amministrazioni) – anche investendo nella formazione del personale docente – per allineare l'offerta educativa alla domanda del mercato del lavoro e creare, così, una forza lavoro rispondente alle relative esigenze.</p>	2024	MIM, MUR , Atenei, ACN, Min. Difesa (alta formazione)	PCM, Min. Difesa, Min. Interno, Regioni e Province autonome
60	<p>Attivare Istituti Tecnici Superiori (ITS) con percorsi di cybersecurity, contribuendo a sostenere le specializzazioni produttive della manifattura locale. I programmi e le attività prevederanno, come previsto, una significativa docenza aziendale (50%) e un tirocinio (almeno 30% del tempo).</p>	2025	ACN, Atenei, MIM, MUR	Operatori privati, Regioni e Prov. autonome

Misure del MUR come Soggetto Responsabile (2/3)

	Misura	Anno avvio implementazione	Attori Responsabili	Altri Soggetti Interessati
61	<p>Sviluppare un sistema nazionale di certificazione dell'apprendimento e dell'acquisizione di specifiche professionalità, non solo tecniche, sia a livello di istruzione secondaria di secondo grado, sia a livello universitario e professionale. L'ACN mantiene una lista dei percorsi di formazione, approvati dalla stessa Agenzia, al termine dei quali il discente consegue, oltre al titolo di studio/professionale, la relativa certificazione.</p>	2025	ACN, Atenei, MIM, MUR	Operatori privati, Regioni e Province autonome
65	<p>Favorire l'organizzazione di iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica, che tengano in debita considerazione principi di bilanciamento di genere, mirate all'individuazione di giovani talenti anche al fine di propiziarne l'ulteriore formazione e l'inserimento nel mondo del lavoro. Ciò, anche al fine di promuovere iniziative volte a colmare il "confidence gap" delle studentesse nei confronti di carriere in ambiti scientifici e tecnologici.</p>	2025	PCM, MIM, MUR , Atenei, CINI, ACN	Min. Difesa
66	<p>Prevedere meccanismi per agevolare la transizione di studenti e neolaureati, con competenze in cybersecurity, verso il mondo del lavoro, mediante programmi di alternanza scuola-lavoro e di inserimento quali stage e apprendistato, nonché incentivi all'assunzione di personale "junior", favorendo altresì la riqualificazione e la ricollocazione professionale di coloro che si trovano al di fuori del mercato del lavoro.</p>	2024	MIMIT, MUR , MIM, DTD, MEF	Min. Lavoro, Associazioni di categoria, Operatori privati, Atenei
67	<p>Prevedere programmi di scambio, a livello europeo e internazionale, per attività di istruzione universitaria e in ambito professionale, che promuovano anche una sempre maggiore inclusione della popolazione femminile.</p>	2025	MUR , DTD, MAECI, CINI, Min. Difesa	ACN, Associazioni di categoria, Operatori privati, Atenei

Misure del MUR come Soggetto Responsabile (3/3)

	Misura	Anno avvio implementazione	Attori Responsabili	Altri Soggetti Interessati
71	<p>Avviare iniziative e campagne di sensibilizzazione volte a promuovere le competenze degli utenti e i comportamenti responsabili nello spazio cibernetico, contrastando la disattenzione digitale e accrescendo la consapevolezza sui rischi derivanti dall'uso delle tecnologie informatiche e su come proteggere la propria privacy online, considerando anche le esigenze di particolari fasce della popolazione come le persone anziane e diversamente abili, oltre che di alcune categorie di pubblici dipendenti (come, ad esempio, i magistrati). Ciò, attraverso la diffusione di informazioni facilmente comprensibili dai non addetti ai lavori sulle vulnerabilità di sicurezza di prodotti e servizi ICT di largo impiego.</p>	2023	ACN, Min. Interno, MUR , DTD, PCM-DIE (Dipartimento per l'Informazione e l'Editoria)	Associazioni di categoria, Regioni e Province autonome, MPA, Min. Difesa
72	<p>Promuovere l'educazione digitale, comprensiva di aspetti di sicurezza cibernetica, per tutti i livelli di istruzione scolastica, affinché si diffondano conoscenze tecniche e operative sulla gestione sicura delle informazioni e delle tecnologie di comunicazione, prevedendo anche raccordi con il mondo accademico per massimizzare l'apprendimento degli studenti su tali tematiche.</p>	2024	MIM, MUR , Atenei, ACN	-

Misure del MUR come Soggetto Interessato

	Misura	Anno avvio implementazione	Attori Responsabili	Altri Soggetti Interessati
48	Sviluppare tecnologia nazionale ed europea, specie nei segmenti più innovativi e sensibili (ad es. cloud ed edge computing, tecnologie basate su blockchain, spazio, ecc.), attraverso l'avvio di dedicate progettualità.	2024	ACN, MIMIT (Autorità delegata alle Politiche dello Spazio e dell'Aerospazio), Min. Difesa (ricerca militare)	MUR e altre Amministrazioni NCS, Operatori Privati, Atenei, Ricerca