

**MANUALE OPERATIVO
IMPLEMENTAZIONE MISURA #82
PIANO DI IMPLEMENTAZIONE
STRATEGIA NAZIONALE DI CYBERSICUREZZA
2022 – 2026**



Indice

1	Overview	4
1.1	Scopo del documento	4
1.2	Metodologia di lavoro	4
1.3	Versioni del documento	12
2	Misure da implementare e indicatori proposti	13
2.1	Misure di protezione	13
2.1.1	Scrutinio tecnologico	13
2.1.2	Definizione e mantenimento di un quadro giuridico nazionale aggiornato e coerente	18
2.1.3	Conoscenza approfondita del quadro della minaccia cibernetica	25
2.1.4	Potenziamento capacità cyber della Pubblica Amministrazione	27
2.1.5	Sviluppo di capacità di protezione per le infrastrutture nazionali	29
2.1.6	Promozione dell'uso della crittografia	35
2.1.7	Definizione e implementazione di un piano di contrasto alla disinformazione online	37
2.2	Misure di risposta	38
2.2.1	Sistema di gestione crisi nazionale e transnazionale	38
2.2.2	Servizi cyber nazionali	42
2.2.3	Esercitazioni di cybersicurezza	49
2.2.4	Definizione del posizionamento e della procedura nazionale in materia di attribuzione	51
2.2.5	Contrasto al cybercrime	52
2.2.6	Capacità di deterrenza in ambito cibernetico	55
2.3	Misure di Sviluppo	56
2.3.1	Centro nazionale di coordinamento	56
2.3.2	Sviluppo di tecnologia nazionale ed europea	58
2.3.3	Realizzazione di un "parco nazionale della cybersicurezza"	59
2.3.4	L'impulso all'innovazione tecnologica e alla digitalizzazione	60
2.3.5	Sviluppo industriale, tecnologico e della ricerca	64
2.4	Fattori abilitanti	71
2.4.1	Formazione	71
2.4.2	Promozione della cultura della sicurezza cibernetica	94
2.4.3	Cooperazione	98
2.4.4	Metriche e Key Performance Indicators	103



Figura 1 - Agenda sessione di approfondimento 5 Settembre 2022	5
Figura 2 - Agenda sessione di approfondimento 12 Settembre 2022	6
Figura 3 - Agenda sessione di approfondimento 19 Settembre 2022	6
Figura 4 - Agenda sessione di approfondimento 26 Settembre 2022	7
Figura 5 - Agenda sessione di approfondimento 3 Ottobre 2022	7
Figura 6 - Agenda sessione di approfondimento 10 Ottobre 2022	8
Figura 7 - Prioritizzazione delle misure da implementare	9
Figura 8 - Cronoprogramma per l'implementazione delle misure "quick win"	10
Figura 9 - Cronoprogramma relativo alla raccolta dei KPI per tutte le misure	11



1. Overview

1.1 Scopo del documento

Il presente documento costituisce una versione operativa del Piano di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026. Il suo scopo è quello di declinare, per ogni misura, le metriche e gli indicatori di misurazione individuati, l'anno di prevalente implementazione delle stesse, oltre alle relative linee guida.

La misurazione dei progressi registrati nelle attività di attuazione delle misure richiede, infatti, la definizione di specifici indicatori, i quali:

- sono specifici per ogni misura del piano di implementazione. Per ognuna di esse sono stati infatti individuati uno o più indicatori;
- sono misurabili in modalità quantitativa, secondo diversi livelli di affidabilità;
- non hanno, allo stato, un target prestabilito, che sarà definito a partire dal secondo anno di esercizio della misurazione, ossia dal 2023.

Ogni indicatore ha un livello di affidabilità ed esso associato che misura il livello di precisione con cui può essere misurato:

- Alta affidabilità: l'indicatore è misurabile in modo quantitativo in quanto collegato a metriche specifiche e univoche;
- Media affidabilità: l'indicatore è misurabile in modo quantitativo ma legato a metriche in parte soggettive;
- Bassa affidabilità: l'indicatore è misurabile in modo quantitativo ma legato a metriche soggettive. Gli indicatori a bassa affidabilità non sono stati presi in considerazione ai fini del presente Manuale.

L'impianto degli indicatori, unitamente ai target specifici definiti per ciascuno di essi, espressi in termini numerici, consentirà di calcolare, per ciascuna misura, il relativo KPI. I KPI indicheranno, pertanto, il grado di attuazione delle misure, espresso in termini percentuali, sulla base di una media ponderata dei valori dei singoli indicatori alla data di effettuazione della rilevazione.

Ciò è funzionale alla predisposizione della relazione che il Presidente del Consiglio dei Ministri è tenuto a trasmettere al Parlamento, entro il 30 aprile di ogni anno, sull'attività svolta dall'Agenzia nell'anno precedente in materia di cybersicurezza nazionale, oltre che dei periodici aggiornamenti che saranno forniti dall'ACN al Comitato Interministeriale per la Cybersicurezza (CIC), il quale esercita l'alta sorveglianza sullo stato di attuazione della Strategia Nazionale di Cybersicurezza.

Il presente Manuale intende costituire un "living document", soggetto a periodici aggiornamenti e revisioni, nel quale riportare – come in una sorta di "diario di bordo" – le linee guida elaborate per la concreta implementazione delle singole misure, mano a mano che le stesse saranno implementate.

1.2 Metodologia di lavoro

In seguito all'adozione, il 17 maggio u.s., da parte del Presidente del Consiglio dei Ministri, della Strategia Nazionale di Cybersicurezza 2022-2026 e dell'annesso Piano di implementazione, sono state poste in essere una serie di attività prodromiche all'attuazione delle misure di cui a quest'ultimo documento, a partire dall'ultima misura, la n° 82, concernente la definizione di metriche e di Key Performance Indicator (KPI).

In particolare, è stato definito un modello ed un piano di lavoro per l'elaborazione degli indicatori di misurazione che consentiranno di elaborare, a partire dal secondo anno di implementazione, dei KPI che permetteranno di registrare i progressi effettivi rispetto agli obiettivi della Strategia e di identificare i trend delle prestazioni. Tali dati saranno visualizzabili grazie ad un apposito "cruscotto" che consentirà di automatizzarne l'elaborazione per le successive attività di reporting dei risultati conseguiti previste dal DL 82/2021.



Al fine di illustrare la metodologia adottata, il 12 luglio 2022 si è tenuto un kick-off meeting con i referenti delle Amministrazioni individuate come attori responsabili per l'attuazione delle misure, ossia, segnatamente, oltre a quelle che compongono il CIC, Presidenza del Consiglio dei Ministri, Ufficio del Consigliere Militare del Presidente del Consiglio, Ministero dell'Istruzione, Consorzio Interuniversitario Nazionale per l'Informatica e Atenei.

Successivamente, tra settembre e ottobre, si sono tenuti cinque incontri con le citate Amministrazioni (Figure 1-5), suddivise per gruppi sulla base di una clusterizzazione delle misure, con l'obiettivo di:

- definire le metriche e gli indicatori di misurazione proposti da ACN. Sul punto si evidenzia che gli indicatori elaborati mirano a misurare l'effettivo grado di implementazione delle diverse misure e non l'efficacia delle attività poste in essere in attuazione delle stesse. Con riguardo a quest'ultimo aspetto, infatti, è buona prassi assicurarne l'efficacia e rilevare la stessa con le più opportune modalità a seconda del tipo di iniziativa posta in essere;
- identificare le misure di prioritaria attuazione, anche in considerazione delle propedeuticità tra le stesse, individuando l'anno di prevalente implementazione, riportato a fianco di ogni misura. L'anno indicato è utile ai fini della pianificazione delle attività e non si riferisce all'anno di rilevazione degli indicatori della misura, in quanto vi sono indicatori misurabili fin dall'avvio delle attività e altri che sono quantificabili solo in un momento successivo.

Sessione di approfondimento del 5 Settembre 2022

	- ID Misure -	- Ambito -	- Enti responsabile della misura -	
	9.00 – 9.30	Introduzione		
Slot 1 9.30 – 11.00	2	Certificazione di sicurezza	- Ministero dell'Interno - Ministero della Difesa	
	4	Attività ispettiva	- Ministero dell'Interno - Ministero della Difesa	
	9	Normativa di sicurezza	- ACN - Ministero dell'Interno - Ministero della Giustizia	
	12	Analisi di contesto	- ACN - Ministero dell'Interno - Ministero della Difesa - DIS - AISE - AISI	
	68	Formazione e awareness	- Ministero dell'Interno - Ministero della Giustizia	
		- ID Misure -	- Ambito -	- Enti responsabile della misura -
Slot 2 11.30 – 13.00	75	Cooperazione	- MAECI - ACN - Ministero dell'Interno - Ministero della Giustizia - Ministero della Difesa - MISE	
	79	Cooperazione	- MAECI - ACN - Ministero dell'Interno - Ministero della Giustizia - Ministero della Difesa	
	41	Contrasto al cybercrime	- Ministero dell'Interno - Ministero della Giustizia - MEF	
	42	Contrasto al cybercrime	- Ministero dell'Interno - Ministero della Giustizia - DIS	
	43	Contrasto al cybercrime	- MAECI - Ministero dell'Interno - Ministero della Giustizia	
		44	Contrasto al cybercrime	- Ministero dell'Interno - Ministero della Giustizia

Figura_1 - Agenda sessione di approfondimento 5 Settembre 2022

Sessione di approfondimento del 12 Settembre 2022

	- ID Misure -	- Ambito -	- Enti responsabile della misura -		- ID Misure -	- Ambito -	- Enti responsabile della misura -
9.00 – 9.30	Introduzione						
Slot 1 9.30 – 11.00	20	Implementazioni di cyberdefense	- ACN - Ministero degli Interni	Slot 2 11.30 – 13.00	7	Normativa di sicurezza	- MITD - MEF - ACN
	71	Formazione e awareness	- ACN - Ministero degli Interni - MUR - MITD - PCM		48	Ricerca tecnologica	- ACN - MITD - Ministero della Difesa
	73	Formazione e awareness	- Ministero degli Interni - PCM		49	Ricerca tecnologica	- ACN - Ministero della Difesa - MITD - MEF - MiSE
	28	Gestione incidenti e crisi	- PCM - ACN-NCS		54	Ricerca tecnologica	- ACN - MITD - MEF - MiSE - MUR - Ministero della Difesa
	8	Normativa di sicurezza	- PCM - ACN		47	Servizi cyber nazionali	- MiSE - MITD - ACN

Figura 2 - Agenda sessione di approfondimento 12 Settembre 2022

Sessione di approfondimento del 19 Settembre 2022

	- ID Misure -	- Ambito -	- Enti responsabile della misura -		- ID Misure -	- Ambito -	- Enti responsabile della misura -
9.00 – 9.30	Introduzione						
Slot 1 9.30 – 11.00	40	Normativa di sicurezza	- DIS - AISE - AISI - MAECI	Slot 2 11.30 – 13.00	59	Formazione e awareness	- Ministero dell'istruzione - MUR - Atenei - ACN - Ministero della Difesa
	45	Deterrenza	- DIS - AISE - AISI - MAECI - Ministero della Difesa		60	Formazione e awareness	- Ministero dell'istruzione - MUR - Atenei - ACN
	76	Cooperazione	- MAECI - ACN		61	Formazione e awareness	- ACN - Atenei - Ministero dell'istruzione - MUR
	77	Cooperazione	- MACEI - ACN - Ministero della Difesa		65	Formazione e awareness	- PCM - Ministero dell'istruzione - MUR - Atenei - CINI - ACN
	33	Servizi cyber nazionali	- ACN - Amministrazioni NCS		67	Formazione e awareness	- MUR - MITD - MAECI - CINI - Ministero della Difesa
					72	Formazione e awareness	- Ministero dell'istruzione - MUR - Atenei - ACN

Figura 3 - Agenda sessione di approfondimento 19 Settembre 2022



Sessione di approfondimento del 26 Settembre 2022

	- ID Misure -	- Ambito -	- Enti responsabile della misura -		- ID Misure -	- Ambito -	- Enti responsabile della misura -
9.00 – 9.30	Introduzione						
Slot 1 9.30 – 11.00	5	Certificazione di sicurezza	- ACN - MITD	Slot 2 11.30 – 13.00	53	Innovazione tecnologica	- ACN - MITD - MiSE - MUR - Ministero della Difesa
	6	Normativa di sicurezza	- MITD - ACN		56	Innovazione tecnologica	- MITD - MiSE - ACN
	16	Implementazioni di cloud security	- MITD - ACN		51	Sviluppo industriale	- MiSE - MITD - MAECI - ACN
	55	Innovazione tecnologica	- MITD - ACN		63	Formazione e awareness	- MITD - MEF
	58	Innovazione tecnologica	- MITD		70	Formazione e awareness	- MiSE - MITD - ACN

Figura 4 - Agenda sessione di approfondimento 26 Settembre 2022

Sessione di approfondimento del 3 Ottobre 2022

	- ID Misure -	- Ambito -	- Enti responsabile della misura -
9.00 – 9.30	Introduzione		
Slot 1 9.30 – 11.00	64	Formazione e awareness	- MEF - MiSE - MITD
	66	Formazione e awareness	- MiSE - MUR - Ministero dell'istruzione - MITD - MEF
	81	Cooperazione	- ACN - MITD - MiSE
	50	Sviluppo industriale	- MAECI - MiSE - ACN
	52	Sviluppo industriale	- ACN - MiSE
	24	Formazione e awareness	- PCM-DIE* - DIS
	69	Formazione e awareness	- ACN - MAECI
	78	Cooperazione	- ACN - MAECI

*Dipartimento per l'Informazione e l'Editoria

Figura 5 - Agenda sessione di approfondimento 3 Ottobre 2022



Sessione di approfondimento del 10 ottobre – Misure di competenza ACN

- ID Misure -	- Ambito -	- ID Misure -	- Ambito -	- ID Misure -	- Ambito -
1	Certificazione di sicurezza	22	Crittografia	36	Servizi cyber nazionali
3	Attività ispettiva	23	Crittografia	37	Servizi cyber nazionali
10	Normativa di sicurezza	25	Gestione incidenti e crisi	38	Esercitazioni di cybersicurezza
11	Normativa di sicurezza	26	Gestione incidenti e crisi	39	Esercitazioni di cybersicurezza
13	Analisi di contesto	27	Gestione incidenti e crisi	46	Servizi cyber nazionali
14	Implementazioni di cyberdefense	29	Gestione incidenti e crisi	57	Innovazione tecnologica
15	Implementazioni di cloud security	30	Servizi cyber nazionali	62	Formazione
17	Implementazioni di cyberdefense	31	Servizi cyber nazionali	74	Cooperazione
18	Implementazioni di cyberdefense	32	Servizi cyber nazionali	80	Cooperazione
19	Implementazioni di cyberdefense	34	Servizi cyber nazionali		
21	Implementazioni di data security	35	Servizi cyber nazionali		

Figura 6 - Agenda sessione di approfondimento 10 Ottobre 2022

Parallelamente, sono state coinvolte anche le diverse articolazioni di questa Agenzia per la validazione di tali elementi (Figura 6), che sono stati riversati nell’annesso Manuale operativo, il quale è stato poi sottoposto alla validazione del Comitato Tecnico Scientifico, che si è riunito il 29 novembre 2022. Il Manuale operativo è stato quindi successivamente condiviso con tutte le Amministrazioni interessate.

Ad esito del processo sopra descritto, si è provveduto a prioritizzare le misure come da Figura 7.

FOCALIZZAZIONE PREVALENTE DEGLI INVESTIMENTI PER ANNO FISCALE

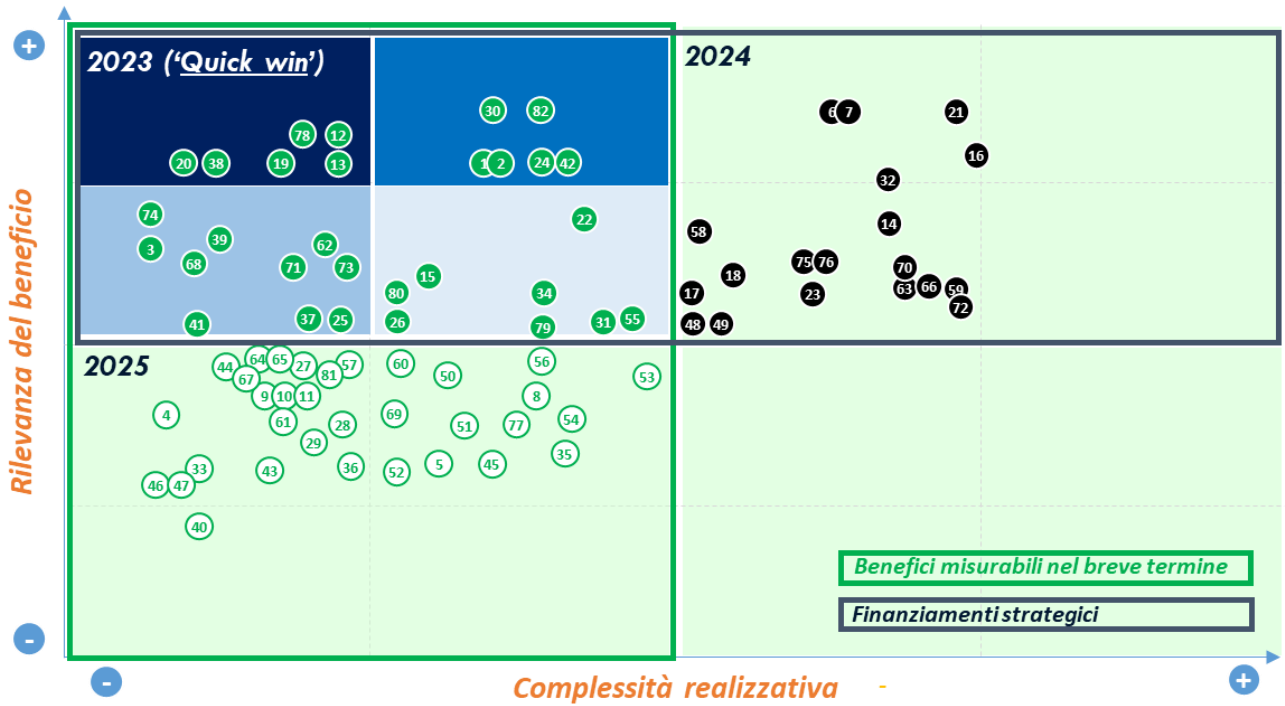


Figura 7 - Prioritizzazione delle misure da implementare

Sulla base delle misure identificate come “quick win”, di prevalente attuazione nel 2023, a partire dal mese di dicembre 2022, sono stati pianificati una serie di incontri con le Amministrazioni responsabili, calendarizzate sulla base del cronoprogramma che rappresenta il periodo di implementazione di cui al Gantt in Figura 8.



GANNT 2023

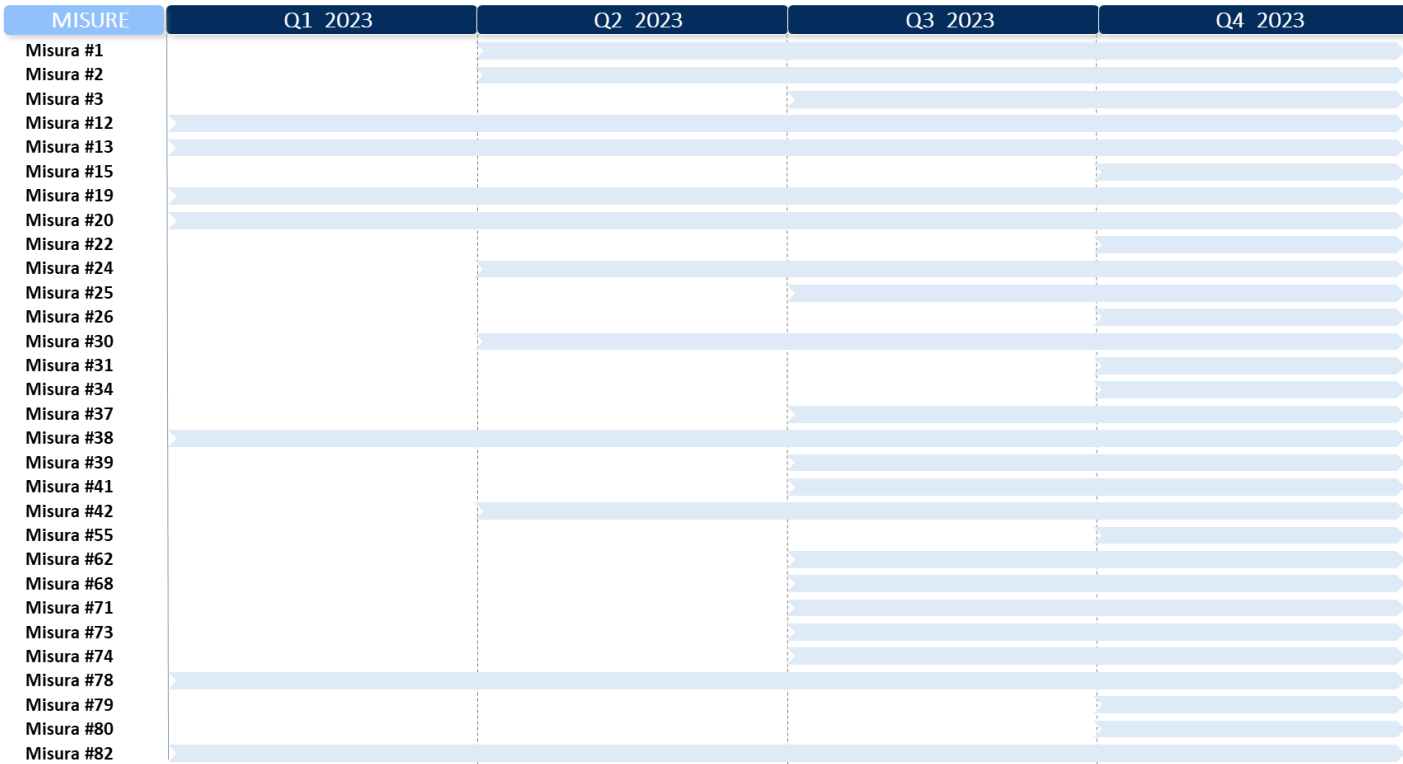


Figura 8 - Cronoprogramma per l'implementazione delle misure "quick win"

Nel corso dei citati incontri si provvederà alla definizione del piano di lavoro, con conseguente identificazione delle attività da porre in essere per la concreta attuazione delle misure, oltre all'individuazione dei target da conseguire per ciascun indicatore, in base ai quali calcolare il KPI di ogni misura.

Successivamente, saranno calendarizzati gli incontri per le altre misure, a partire da gennaio 2023, come da cronoprogramma in Figura 9 che rappresenta l'arco temporale di misurazione dei KPI per le singole misure.



PIANO DI IMPLEMENTAZIONE DELLA STRATEGIA NAZIONALE DI CYBERSICUREZZA 2022-2026

MISURE	2023	2024	2025	2026
Misura #1				
Misura #2				
Misura #3				
Misura #4				
Misura #5				
Misura #6				
Misura #7				
Misura #8				
Misura #9				
Misura #10				
Misura #11				
Misura #12				
Misura #13				
Misura #14				
Misura #15				
Misura #16				
Misura #17				
Misura #18				
Misura #19				
Misura #20				
Misura #21				
Misura #22				
Misura #23				
Misura #24				
Misura #25				
Misura #26				
Misura #27				
Misura #28				
Misura #29				
Misura #30				
Misura #31				
Misura #32				
Misura #33				
Misura #34				
Misura #35				
Misura #36				
Misura #37				
Misura #38				
Misura #39				
Misura #40				
Misura #41				
Misura #42				
Misura #43				
Misura #44				
Misura #45				
Misura #46				
Misura #47				
Misura #48				
Misura #49				
Misura #50				
Misura #51				
Misura #52				
Misura #53				
Misura #54				
Misura #55				
Misura #56				
Misura #57				
Misura #58				
Misura #59				
Misura #60				
Misura #61				
Misura #62				
Misura #63				
Misura #64				
Misura #65				
Misura #66				
Misura #67				
Misura #68				
Misura #69				
Misura #70				
Misura #71				
Misura #72				
Misura #73				
Misura #74				
Misura #75				
Misura #76				
Misura #77				
Misura #78				
Misura #79				
Misura #80				
Misura #81				
Misura #82				

Figura 9 - Cronoprogramma relativo alla raccolta dei KPI per tutte le misure



1.3 Versioni del documento

a tabella sottostante elenca le versioni del documento, la data di pubblicazione e i dettagli di ogni aggiornamento.

Versione	Data	Descrizione
1.0	09/11/2022	Prima bozza per revisione CTS
2.0	05/12/2022	Bozza validata dal CTS
3.0	08/03/2023	Nuova versione con aggiornamento parziale degli indicatori

2. Misure da implementare e indicatori proposti

2.1 Misure di protezione

2.1.1 Scrutinio tecnologico

Misura #1

Rafforzare il sistema di scrutinio tecnologico nazionale a supporto della sicurezza della supply chain delle particolari categorie di asset rientranti nel Perimetro e per l'adozione di schemi di certificazione europea di cybersecurity, anche mediante l'accreditamento di laboratori di valutazione pubblico/privati.



Attori responsabili

ACN



Altri soggetti interessati

Min. Interno, Min. Difesa,
Operatori privati



Anno di implementazione

2023



METRICA

1a
Beni, sistemi e servizi ICT oggetto di valutazione da parte del CVCN e dei CV.



INDICATORE

1a
Numero di beni, sistemi e servizi ICT oggetto di valutazione ai sensi dell'art. 1 comma 6, lettera a) del DL 105/2019, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

Il target verrà definito in base al numero di beni, sistemi e servizi ICT per i quali viene richiesta una valutazione ai sensi dell'art. 1 comma 6, lettera a) del DL 105/2019. Dovrà essere altresì calcolato il numero di procedimenti, la cui fase di verifiche preliminari si sia conclusa entro i 45 giorni, senza ricorrere ai 15 giorni di proroga.



METRICA

1b
Beni, sistemi e servizi ICT oggetto di scrutinio tecnologico da parte del CVCN, dei CV e dei Laboratori Accreditati di Prova.



INDICATORE

1b
Numero di beni, sistemi e servizi ICT oggetto di scrutinio tecnologico da parte del CVCN, dei CV e dei Laboratori Accreditati di Prova nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

Il target verrà definito in base al numero di beni, sistemi e servizi ICT per i quali viene richiesta una valutazione ai sensi dell'art. 1 comma 6, lettera a) del DL 105/2019. Dovrà essere altresì calcolato il numero di procedimenti, la cui fase di verifiche preliminari si sia conclusa entro i 45 giorni, senza ricorrere ai 15 giorni di proroga.



METRICA

1c
Schemi di certificazione europea supportati.



INDICATORE

1c
Numero di attività ed eventi volti a supportare l'adozione di schemi di certificazione europea (Work Stream, EUCC, ENISA, etc.) ai quali ACN ha partecipato nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere incluse tutte le attività e gli eventi in cui vengono discussi o negoziati gli schemi di certificazione o eventi relativi ad altre attività prodromiche alla predisposizione degli schemi che verranno successivamente negoziati.

 METRICA

1d
Laboratori accreditati.

 INDICATORE

1d
Numero di laboratori accreditati nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere inclusi tutti i laboratori (intesi come pool di esperti) che includono dipendenti pubblici e istituti privati accreditati.

Misura #2

Sviluppare le capacità dei Centri di Valutazione del Ministero dell'Interno e del Ministero della Difesa accreditati dall'ACN, quali organismi di valutazione della conformità, per i sistemi di rispettiva competenza.



Attori responsabili
Min. Interno, Min. Difesa



Altri soggetti interessati
ACN



Anno di implementazione
2023

 METRICA

2a
Addetti dei Centri di Valutazione.

 INDICATORE

2a
Numero di addetti dei Centri di Valutazione alla data di misurazione.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere conteggiati sia i dipendenti pubblici interamente dedicati ai Centri di valutazione che i dipendenti pubblici che svolgono, anche, altre mansioni.

 METRICA

2b
Ore di formazione specialistica su tematiche di cybersecurity erogate per gli addetti dei Centri di Valutazione .

 INDICATORE

2b
Numero di ore di formazione specialistica su tematiche di cybersecurity erogate per gli addetti dei Centri di Valutazione nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

Tra i corsi di formazione specialistica sono compresi:

- Tutti i corsi di laurea magistrale o magistrale a ciclo unico in ambito cybersecurity;
- Master in ambito cybersecurity;
- Certificazioni esterne di enti riconosciuti (e.g. a titolo esemplificativo e non esaustivo la ISO/IEC 27001, CISM, CISP, CRISC);
- Certificazioni interne erogate dalla PA (e.g. da ente ACN).

 METRICA

2c
Ore di formazione specialistica relative alle certificazioni erogate per gli addetti dei Centri di Valutazione.

 INDICATORE

2c
Numero di ore di formazione specialistica relative alle certificazioni erogate per gli addetti dei Centri di Valutazione nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA


2d
Formazione specialistica relativa alla certificazione di prodotti, processi e servizi ICT erogata per gli addetti dei Centri di Valutazione.

 INDICATORE

2d
Numero di ore di formazione specialistica relativa alla certificazione di prodotti, processi e servizi ICT erogate per gli addetti dei Centri di Valutazione nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

2e
Formazione specialistica relativa alle Certificazioni.

 INDICATORE

2e
Numero di ore di formazione specialistica relativa alle certificazioni erogate per gli addetti dei Centri di Valutazione nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #3

Attivazione di un nucleo ispettivo centrale presso l'Agencia a supporto delle attività ispettive in relazione agli obblighi derivanti dalle normative cyber vigenti.



Attori responsabili

ACN



Anno di implementazione

2023

METRICA

INDICATORE

AFFIDABILITA'

3a
Addetti del nucleo ispettivo centrale.

3a
Numero di addetti del nucleo ispettivo centrale alla data di misurazione.

Alta

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere conteggiati sia i dipendenti pubblici interamente dedicati al nucleo ispettivo centrale che i dipendenti pubblici che svolgono, anche, altre mansioni.

METRICA

INDICATORE

AFFIDABILITA'

3b
Attività ispettive condotte.

3b
Numero di attività ispettive condotte nel periodo di riferimento.

Alta

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere conteggiate le attività di assessment e gap analysis in relazione alla normativa Cyber vigente.

 METRICA

 INDICATORE

AFFIDABILITA'

3c
Enti oggetto di attività ispettive.

3c
Numero di Enti oggetto di attività ispettive nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #4

Attivazione di omologhe unità ispettive presso i Ministeri dell'Interno e della Difesa, a supporto delle attività ispettive in relazione agli obblighi derivanti dalle normative cyber vigenti.



Attori responsabili

Min. Interno, Min. Difesa



Altri soggetti interessati

ACN



Anno di implementazione

2025

 METRICA

 INDICATORE

AFFIDABILITA'

4a
Addetti delle unità ispettive.

4a
Numero di addetti delle unità ispettive alla data di misurazione.


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere conteggiati sia i dipendenti pubblici interamente dedicati alle unità ispettive presso o i Ministeri dell'Interno e della Difesa che i dipendenti pubblici che svolgono, anche, altre mansioni.

 METRICA

 INDICATORE

AFFIDABILITA'

4b
Attività ispettive completate.

4b
Numero di attività ispettive completate nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere conteggiate le attività di assessment e gap analysis in relazione alla normativa Cyber vigente.

 METRICA

 INDICATORE

AFFIDABILITA'

4c
Enti coinvolti nelle attività ispettive completate.

4c
Numero di Enti coinvolti nelle attività ispettive completate nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE


N/A




2.1.2 Definizione e mantenimento di un quadro giuridico nazionale aggiornato e coerente

Misura #5

Supportare lo sviluppo, valutandone l'adeguatezza in termini di sicurezza nazionale, degli schemi di certificazione in materia di cybersicurezza e, in collaborazione con il settore privato, promuoverne l'adozione e l'utilizzo da parte dei fornitori di servizi e delle imprese italiane, favorendo lo sviluppo del tessuto imprenditoriale nazionale specializzato al fine di conseguire un vantaggio competitivo sul mercato

 **Attori responsabili**
ACN, DTD

 **Altri soggetti interessati**
MIMIT, Associazioni di categoria

 **Anno di implementazione**
2025

METRICA

5a
Iniziative volte a supportare lo sviluppo di schemi di certificazione in materia di cybersicurezza.

INDICATORE

5a
Numero di iniziative volte a supportare lo sviluppo di schemi di certificazione in materia di cybersicurezza, portate a termine nel periodo di riferimento.

AFFIDABILITA'


Alta

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere conteggiate tutte le iniziative progettuali/o spot, che concorrono alla definizione/revisione di schemi di certificazione in ambito cybersecurity, che sono state portate a termine nel periodo di riferimento.

METRICA

5b
Schemi di certificazione in materia di cybersicurezza oggetto di analisi.

INDICATORE

5b
Numero di schemi di certificazione in materia di cybersicurezza oggetto di analisi nel periodo di riferimento.

AFFIDABILITA'


Alta

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere conteggiate tutti gli schemi di certificazione finalizzati e sottoposti ad analisi nel periodo di riferimento.

METRICA

5c
Iniziative volte a promuovere l'adozione e l'utilizzo degli schemi di certificazione da parte dei fornitori di servizi e delle imprese italiane.

INDICATORE

5c
Numero di iniziative volte a promuovere l'adozione e l'utilizzo degli schemi di certificazione da parte dei fornitori di servizi e delle imprese italiane, portate a termine nel periodo di riferimento.

AFFIDABILITA'


Alta

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere incluse tutte le attività/iniziative di awareness, sensibilizzazione e promozione degli schemi dei quali è richiesta l'adozione, che sono state portate a termine.

 METRICA

 INDICATORE

AFFIDABILITA'

5d
PMI italiane che hanno adottato schemi di certificazione in materia di cybersicurezza.

5d
Numero di PMI italiane che hanno adottato schemi di certificazione in materia di cybersicurezza nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

5e
Grandi aziende italiane che hanno adottato schemi di certificazione in materia di cybersicurezza.

5e
Numero di grandi aziende italiane che hanno adottato schemi di certificazione in materia di cybersicurezza nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

5f
Fornitori di servizi che hanno adottato schemi di certificazione in materia di cybersicurezza.

5f
Numero di fornitori di servizi che hanno adottato schemi di certificazione in materia di cybersicurezza nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #6

Introdurre norme giuridiche che valorizzino l'inclusione di elementi di sicurezza cibernetica nelle attività di procurement ICT della Pubblica Amministrazione, fornendo indicazioni sia a quest'ultima che agli operatori di mercato per garantire che i beni e i servizi informatici, acquistati dai soggetti pubblici nell'ambito di gare d'appalto o di specifici accordi quadro, rispondano ad adeguati livelli di cybersicurezza. Ciò, compatibilmente con la celere definizione delle relative procedure di aggiudicazione.



Attori responsabili

MITD, ACN



Altri soggetti interessati

MEF, Min. Giustizia, MPA, altre Amministrazioni NCS



Anno di implementazione

2024

METRICA

6a
Atti normativi e regolatori che prevedono l'inclusione di requisiti di sicurezza con rilevanza valutativa.

INDICATORE

6a
Numero di atti normativi e regolatori che prevedono l'inclusione di requisiti di sicurezza con rilevanza valutativa emessi nel periodo di riferimento.

AFFIDABILITA'



Media

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere inclusi tutti i tipi di atti normativi e regolatori, compresi i provvedimenti amministrativi, che includono requisiti di sicurezza.

Misura #7

Promuovere la realizzazione, a livello nazionale ed europeo, di un sistema di gare pubbliche impostato su criteri che garantiscano soluzioni di qualità sotto il profilo della cybersicurezza.



Attori responsabili

DTD, MEF, ACN



Altri soggetti interessati

MPA, altre Amministrazioni NCS



Anno di implementazione

2024

METRICA

7a
Requisiti di sicurezza definiti nell'ambito di linee guida emesse per procurement ICT della Pubblica Amministrazione.

INDICATORE

7a
Numero di requisiti di sicurezza definiti nell'ambito di linee guida emesse per procurement ICT della Pubblica Amministrazione nel periodo di riferimento.

AFFIDABILITA'



Alta

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere inclusi sia i requisiti di sicurezza di cui gli enti si sono già dotati in passato, approvati da ACN, sia nuovi requisiti emergenti purché non si tratti di requisiti equivalenti rispetto a quelli già in essere.

In considerazione dei rilevanti profili giuridici che presenta la tematica, è previsto il coinvolgimento della competente articolazione dell'ACN.

 METRICA

 INDICATORE

AFFIDABILITA'

7b
Enti che hanno introdotto requisiti di sicurezza con rilevanza valutativa in gare di appalto pubbliche.

7b
Numero di Enti che hanno introdotto requisiti di sicurezza con rilevanza valutativa in gare di appalto pubbliche nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere inclusi gli Enti della PA che hanno adottato il modello di requisiti di sicurezza di cui al punto precedente sia in relazione alla gestione di gare d'appalto, sia in relazione ad altre modalità di ingaggio.

 METRICA

 INDICATORE

AFFIDABILITA'

7c
Procedure di affidamento pubbliche che hanno previsto requisiti di sicurezza con rilevanza valutativa.

7c
Numero di procedure di affidamento che hanno previsto requisiti di sicurezza con rilevanza valutativa nel periodo di riferimento.



Alta


 LINEE GUIDA PER LA MISURAZIONE


Nel calcolo dovranno essere conteggiate tutte le gare d'appalto ed eventuali altre modalità di ingaggio che includono i requisiti di sicurezza definiti.

Misura #8

Introdurre norme giuridiche volte a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale

 **Attori responsabili**
PCM, ACN

 **Altri soggetti interessati**
Amministrazioni NCS

 **Anno di implementazione**
2025

 METRICA

 INDICATORE

AFFIDABILITA'

8a
Interventi normativi e regolatori volti a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale.

8a
Numero di interventi normativi e regolatori volti a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale, emesse nel periodo di riferimento.


Media

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere inclusi tutti i tipi di atti normativi e regolatori, compresi i provvedimenti amministrativi, volti a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale.
Per l'implementazione della misura 8, in aggiunta ai soggetti responsabili e interessati già indicati dal piano di implementazione, si ritiene necessario coinvolgere il DICA.

 METRICA

 INDICATORE

AFFIDABILITA'

8b
Componenti (tecnologie / processi) oggetto di norme giuridiche volte a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale.

8b
Numero di componenti (tecnologie / processi) oggetto di norme giuridiche volte a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale., acquisiti nel periodo di riferimento.


Media


 LINEE GUIDA PER LA MISURAZIONE


Per componenti si intendono soluzioni software/ hardware/appliance che introducono funzionalità di sicurezza su:

- sistemi operativi;
- apparati di rete;
- basi dati;
- middleware;
- applicazioni informatiche.

Misura #9

Definire una politica nazionale sulla divulgazione coordinata di vulnerabilità (coordinated vulnerability disclosure).

 **Attori responsabili**
ACN, Min. Interno, Min. Giustizia

 **Anno di implementazione**
2025

 METRICA

 INDICATORE

AFFIDABILITA'

9a
Enti che sono stati coinvolti nel percorso di definizione della politica nazionale sulla divulgazione coordinata di vulnerabilità.

9a
Numero di Enti che sono stati coinvolti nel percorso di definizione della politica nazionale sulla divulgazione coordinata di vulnerabilità nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere inclusi tutti gli enti della PA che hanno partecipato attivamente alla definizione della politica nazionale sulla divulgazione coordinata di vulnerabilità. Per «divulgazione coordinata di vulnerabilità» (CVD) si intende il processo mediante il quale i rilevatori di vulnerabilità lavorano insieme e condividono le informazioni con le parti interessate come fornitori e proprietari di infrastrutture ICT. Tale processo garantisce che le vulnerabilità del software vengano divulgate al pubblico una volta che il fornitore è stato in grado di sviluppare una correzione, una patch o ha trovato una soluzione diversa.

La relativa politica nazionale è un insieme di regole e accordi progettati al fine di garantire che: i ricercatori contattino le parti giuste per rivelare la vulnerabilità; i fornitori possano sviluppare una correzione o una patch in modo tempestivo; i ricercatori ottengano il riconoscimento dal loro lavoro e siano protetti dall'azione penale. In tal senso sarà necessario individuare un istituto giuridico che escluda la responsabilità penale di coloro che hanno scoperto la vulnerabilità.

In considerazione dei rilevanti profili giuridici che presenta la tematica, è previsto il coinvolgimento della competente articolazione dell'ACN.

 METRICA

 INDICATORE

AFFIDABILITA'

9b
Processi e strumenti di attuazione della normativa che disciplina la Coordinated Vulnerability Disclosure.

9b
Numero di processi e strumenti di attuazione della normativa che disciplina la Coordinated Vulnerability Disclosure alla data di misurazione


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

9c
Vulnerabilità gestite e divulgate secondo la politica nazionale definita.

9c
Numero di vulnerabilità gestite e divulgate secondo la politica nazionale definita nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere incluse il totale delle segnalazioni che concernono le vulnerabilità gestite e divulgate a livello nazionale (cfr. articolo 12 direttiva NIS 2). Vengono incluse quindi, sia le segnalazioni di nuove vulnerabilità, che eventuali comunicazioni relative ad update inerenti a vulnerabilità già segnalate.

Misura #10

Pubblicare linee guida sulla cybersecurity per le Amministrazioni Pubbliche, con differenti gradi di coerenza (con riguardo, ad es., a MFA, registrazione e conservazione dei log, ecc.), anche in riferimento alla transizione al cloud e favorendo una gestione continuativa e automatizzata del rischio cyber, secondo un approccio "zero trust".



Attori responsabili
ACN



Altri soggetti interessati
Amministrazioni NCS



Anno di implementazione
2025

 METRICA

 INDICATORE

AFFIDABILITA'

10a
Componenti di sicurezza (tecnologie / processi) trattati dalle linee guida emesse, anche in riferimento alla transizione al cloud.

10a
Numero di componenti di sicurezza (tecnologie / processi) trattati dalle linee guida emesse, anche in riferimento alla transizione al cloud, alla data di misurazione.


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere conteggiate tutte le tecnologie/processi di sicurezza emessi (e.g. MFA, log collection, Identity Management, Agent per il monitoraggio di sicurezza per le postazioni di lavoro, Agent per la classificazione dei dati e delle informazioni).

Misura #11

Porre in essere iniziative di sensibilizzazione per favorire l'applicazione del "Framework Nazionale per la Cybersecurity e la Data Protection" e dei "Controlli essenziali di cybersecurity", opportunamente aggiornati in linea con il quadro della minaccia, da parte della PA, delle imprese e delle PMI.



Attori responsabili

ACN



Altri soggetti interessati

DTD, Associazioni di categoria



Anno di implementazione

2025



METRICA

11a

Iniziative di sensibilizzazione (campagne) sviluppate per favorire l'applicazione del "Framework Nazionale per la Cybersecurity e la Data Protection" e dei "Controlli essenziali di cybersecurity" ad uso delle PA, delle imprese e delle PMI.



INDICATORE

11a

Numero di iniziative di sensibilizzazione (campagne) sviluppate per favorire l'applicazione del "Framework Nazionale per la Cybersecurity e la Data Protection" e dei "Controlli essenziali di cybersecurity" ad uso delle PA, delle imprese e delle PMI, sviluppate nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere incluse tutte le iniziative di sensibilizzazione, awareness e promozione del "Framework Nazionale per la Cybersecurity e la Data Protection" e dei "Controlli essenziali di cybersecurity", portate a termine.



METRICA

11b

Enti della PA, delle imprese e delle PMI, coinvolti in iniziative di sensibilizzazione (campagne) sviluppate per favorire l'applicazione del "Framework Nazionale per la Cybersecurity e la Data Protection" e dei "Controlli essenziali di cybersecurity".



INDICATORE

11b

Numero di Enti della PA, delle imprese e delle PMI, coinvolti in iniziative di sensibilizzazione (campagne) sviluppate per favorire l'applicazione del "Framework Nazionale per la Cybersecurity e la Data Protection" e dei "Controlli essenziali di cybersecurity", coinvolte nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

2.1.3 Conoscenza approfondita del quadro della minaccia cibernetica

Misura #12

Continuare ad accrescere le capacità nazionali di difesa, resilienza, contrasto al crimine e cyber intelligence, rafforzando ulteriormente la situational awareness mediante il monitoraggio continuo e l'analisi di minacce, vulnerabilità e attacchi, secondo gli specifici ambiti di competenza.



Attori responsabili

ACN, Min. Interno, Min. Difesa, DIS, AISE, AISI



Anno di implementazione

2023



METRICA



INDICATORE

AFFIDABILITA'

12a

Addetti coinvolti nei processi di monitoraggio e situational awareness ivi inclusa l'analisi di minacce, vulnerabilità e attacchi.

12a

Numero di addetti coinvolti nei processi di monitoraggio e situational awareness ivi inclusa l'analisi di minacce, vulnerabilità e attacchi, alla data di misurazione.



Alta



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere inclusi tutti i dipendenti pubblici dedicati o che svolgono, anche, altre mansioni coinvolti, nei processi di situational awareness.

Per l'implementazione della misura 12, in aggiunta ai soggetti responsabili e interessati già indicati dal piano di implementazione, si ritiene necessario coinvolgere il MAECI (Per il contributo delle Ambasciate) e il MEF.



METRICA



INDICATORE

AFFIDABILITA'

12b

Eventi oggetto di monitoraggio continuo nell'ambito dei processi di situational awareness ivi incluso l'analisi di minacce, vulnerabilità e attacchi.

12b

Numero di eventi oggetto di monitoraggio continuo nell'ambito dei processi di situational awareness ivi incluso l'analisi di minacce, vulnerabilità e attacchi, nel periodo di riferimento.



Media



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere inclusi eventi di sicurezza che possono tradursi in incidenti, minacce, attacchi e nuove vulnerabilità, sottoposti a monitoraggio continuo.



METRICA



INDICATORE

AFFIDABILITA'

12c

Affidabilità ed efficacia dei dati condivisi tramite gli strumenti sviluppati e rilasciati per l'esecuzione dei processi di situational awareness ivi incluso l'analisi di minacce, vulnerabilità e attacchi.

12c

Numero di riscontri relativi ad incidenti, eventi di sicurezza rilevanti ricevuti dai soggetti accreditati nel periodo di riferimento.







Media



LINEE GUIDA PER LA MISURAZIONE


N/A


 METRICA	 INDICATORE	AFFIDABILITA'
12d Effort effettivo erogato per l'accrescimento delle capacità nazionali di difesa, resilienza, contrasto al crimine e cyber intelligence.	12d Numero di giornate uomo erogate da ciascun Ente per l'erogazione dei processi di situational awareness nel periodo di riferimento.	 Media


 **LINEE GUIDA PER LA MISURAZIONE**




Il conteggio fa riferimento al totale cumulato delle giornate lavorate da dipendenti pubblici dedicati o che svolgono, anche, altre mansioni.


Misura #13
 Realizzare un servizio di monitoraggio del rischio cyber nazionale a favore delle organizzazioni e del pubblico in generale, al fine di comunicare l'effettivo livello della minaccia, nonché di informare adeguatamente i processi decisionali.

 **Attori responsabili**
ACN




 **Altri soggetti interessati**
Amministrazioni NCS, Operatori privati, Atenei, Ricerca


 **Anno di implementazione**
2023

 METRICA	 INDICATORE	AFFIDABILITA'
13a Iniziative che mirano a comunicare l'effettivo livello della minaccia cyber.	13a Numero di iniziative che mirano a comunicare l'effettivo livello della minaccia cyber poste in essere nel periodo di riferimento.	 Media

 **LINEE GUIDA PER LA MISURAZIONE**

N/A

 METRICA	 INDICATORE	AFFIDABILITA'
13b Accessi al cruscotto di monitoraggio del rischio Cyber nazionale.	13b Numero di accessi al cruscotto di monitoraggio del rischio Cyber nazionale alla data di misurazione.	 Alta

 **LINEE GUIDA PER LA MISURAZIONE**

Il numero di accessi verrà monitorato periodicamente in modo da verificare che sia costante o in crescita.

2.1.4 Potenziamento capacità cyber della Pubblica Amministrazione

Misura #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.



Attori responsabili
ACN



Altri soggetti interessati
DTD, MPA



Anno di implementazione
2024



METRICA

14a
Iniziativa volte a facilitare il potenziamento delle capacità cyber della PA.



INDICATORE

14a
Numero di iniziative volte a facilitare il potenziamento delle capacità cyber della PA portate a termine nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #15

Provvedere alla qualificazione dei servizi cloud per la Pubblica Amministrazione, in attuazione della Strategia Cloud Italia, al fine di assicurare adeguati livelli di sicurezza per i servizi e i dati della PA.



Attori responsabili
ACN



Altri soggetti interessati
DTD



Anno di implementazione
2023



METRICA

15a
Servizi cloud qualificati per la PA.



INDICATORE

15a
Numero di servizi Cloud qualificati per la PA alla data di misurazione.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #16

Facilitare la migrazione sicura dei servizi e dei dati della Pubblica Amministrazione sul cloud, ovvero PSN o Public Cloud, in linea con le attività di classificazione dei dati e dei servizi come da Strategia Cloud Italia.



Attori responsabili

DTD, ACN



Anno di implementazione

2024



METRICA

16a

Iniziative volte alla definizione di requisiti specifici per garantire la migrazione sicura dei servizi e dei dati della Pubblica Amministrazione sul cloud.



INDICATORE

16a

Numero di iniziative volte alla definizione di requisiti specifici per garantire la migrazione sicura dei servizi e dei dati della Pubblica Amministrazione sul cloud portate a termine nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

Con requisiti specifici si fa riferimento ai requisiti che devono essere adottati in accordo con la strategia Cloud Italia che presuppone un percorso di qualificazione dei Cloud provider e dei loro servizi per garantire che le caratteristiche e i livelli di servizio dichiarati siano in linea con i requisiti necessari di sicurezza, affidabilità e rispetto delle normative rilevanti.



METRICA

16b

Requisiti definiti per la migrazione sicura dei servizi e dei dati della Pubblica Amministrazione sul cloud.



INDICATORE

16b

Grado di copertura dei requisiti definiti nelle due determinazioni adottate da ACN per la migrazione sicura dei servizi e dei dati della Pubblica Amministrazione sul cloud, alla data di misurazione.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

I requisiti citati includono quelli di cui a standard relativi alla cloud security, quali ad esempio ISO27017 e CSA.



METRICA

16c

Servizi e dati della Pubblica Amministrazione migrati in modalità sicura sul cloud, ovvero PSN o Public Cloud.



INDICATORE

16c

Numerosità di servizi e dati della Pubblica Amministrazione migrati in modalità sicura sul cloud, ovvero PSN o Public Cloud, alla data di misurazione.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A

2.1.5 Sviluppo di capacità di protezione per le infrastrutture nazionali

Misura #17

Promuovere lo sviluppo di procedure, processi e sistemi di monitoraggio e controllo delle configurazioni BGP nazionali in cooperazione con gli operatori IXP nazionali.



Attori responsabili
ACN



Altri soggetti interessati
Operatori privati



Anno di implementazione
2024



METRICA

17a
IXP italiani coinvolti nella definizione di Best Practice e nel monitoraggio della rispettiva applicazione.



INDICATORE

17a
Numero di IXP italiani coinvolti nella definizione di Best Practice e nel monitoraggio della rispettiva applicazione alla data di misurazione.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

17b
Attività di sensibilizzazione rivolte agli operatori di AS volta a promuovere l'implementazione di un framework di best practice tecniche.



INDICATORE

17b
Numero di attività di sensibilizzazione rivolte agli operatori di AS volte a promuovere l'implementazione di un framework di best practice tecniche, effettuate nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

17c
IP nazionale gestito dagli operatori che hanno preso parte alle attività di sensibilizzazione.



INDICATORE

17c
Percentuale dell'indirizzamento IP nazionale gestito dagli operatori che hanno preso parte alle attività di sensibilizzazione nel periodo di riferimento.

AFFIDABILITA'






Alta






LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA	 INDICATORE	AFFIDABILITA'
17d Controlli eseguiti sulle procedure, processi e sistemi di monitoraggio e controllo delle configurazioni BGP contenute nel framework di best practice.	17d Numero di controlli eseguiti sulle procedure, processi e sistemi di monitoraggio e controllo delle configurazioni BGP contenute nel framework di best practice nel periodo di riferimento	 Alta


 LINEE GUIDA PER LA MISURAZIONE
N/A


 METRICA	 INDICATORE	AFFIDABILITA'
17e Eventi di BGP Hijacking rilevati ai danni di AS nazionali.	17e Numero di eventi anomali rilevati ai danni di AS italiani o che originano da AS italiani.	 Media


 LINEE GUIDA PER LA MISURAZIONE
N/A




Misura #18


Promuovere l'implementazione di una infrastruttura di risoluzione DNS nazionale al servizio degli operatori pubblici e privati, sostenendo l'applicazione di controlli di sicurezza sulla navigazione e protezione contro attività malevole condotte anche tramite il DNS.

 **Attori responsabili**
ACN

 **Altri soggetti interessati**
Amministrazioni centrali, Regioni e Province autonome, CNR, Operatori privati

 **Anno di implementazione**
2024

 METRICA	 INDICATORE	AFFIDABILITA'
18a Iniziative attuate per promuovere l'implementazione di una infrastruttura di risoluzione DNS.	18a Numero di iniziative attuate per promuovere l'implementazione di una infrastruttura di risoluzione DNS nel periodo di riferimento.	 Media

 LINEE GUIDA PER LA MISURAZIONE
N/A

 METRICA

18b
Controlli di sicurezza sulla navigazione e protezione contro attività malevole condotte anche tramite il DNS.

 INDICATORE

18b
Numero di controlli di sicurezza sulla navigazione e protezione contro attività malevole condotte anche tramite il DNS definiti alla data di misurazione.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

18c
Utenti che fanno uso della infrastruttura nazionale di risoluzione DNS.

 INDICATORE

18c
Numero di utenti che fanno uso della infrastruttura nazionale di risoluzione DNS alla data di misurazione.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #19

Implementare servizi di monitoraggio di vulnerabilità e configurazioni erranee dei servizi digitali esposti su Internet di interesse della Pubblica Amministrazione, attuando politiche di early warning.



Attori responsabili

ACN



Anno di implementazione

2023

 METRICA

19a
Pubbliche amministrazioni oggetto di monitoraggio.

 INDICATORE

19a
Numero delle Pubbliche amministrazioni oggetto di monitoraggio alla data di misurazione.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

19b
Iniziative promosse per l'implementazione di servizi di monitoraggio di vulnerabilità e configurazioni erranee dei servizi digitali esposti su internet di interesse della Pubblica Amministrazione.

 INDICATORE

19b
Numero di iniziative promosse per l'implementazione di servizi di monitoraggio di vulnerabilità e configurazioni erranee dei servizi digitali esposti su internet di interesse della Pubblica Amministrazione, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A



 METRICA

19c
Eventi di vulnerabilità e configurazioni erranee dei servizi digitali esposti su internet comunicati a Pubbliche Amministrazioni.

 INDICATORE

19c
Numero di eventi di vulnerabilità e configurazioni erranee dei servizi digitali esposti su internet comunicati a Pubbliche Amministrazioni nel periodo di riferimento.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #20

Promuovere l'utilizzo delle migliori pratiche di gestione dei domini di posta elettronica della Pubblica Amministrazione, implementando un servizio di monitoraggio e protezione contro campagne di phishing o abusi.



Attori responsabili

ACN, Min. Interno



Altri soggetti interessati

Amministrazioni centrali, Regioni e Province autonome



Anno di implementazione

2023

 METRICA

20a
Nomi di dominio di posta elettronica della Pubblica Amministrazione che usufruiscono di servizi di monitoraggio e protezione contro campagne di phishing o abusi.

 INDICATORE

20a
Numero di nomi di dominio di posta elettronica della Pubblica Amministrazione che usufruiscono di servizi di monitoraggio e protezione contro campagne di phishing o abusi alla data di misurazione.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

20b
Eventi rilevanti e nomi di dominio identificati nell'ambito di campagne di phishing o abusi.

 INDICATORE

20b
Numero di eventi rilevanti e di nomi di dominio identificati, nell'ambito di campagne di phishing o abusi, nel periodo di riferimento.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo verranno escluse eventuali segnalazioni che a seguito di analisi dovessero risultare falsi positivi.

 METRICA

 INDICATORE

AFFIDABILITA'

20c
Nomi di dominio disattivati nell'ambito di campagne di phishing o abusi.

20c
Numero di nomi di dominio disattivati, nell'ambito di campagne di phishing o abusi, nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

20d
Early warning relativi ad eventi rilevati e nomi di dominio identificati, nell'ambito di campagne di phishing, per successiva disattivazione.

20d
Numero Early warning relativi ad eventi rilevati e di domini identificati, nell'ambito di campagne di phishing, per successiva disattivazione, alla data di misurazione.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #21

Promuovere lo sviluppo e l'implementazione di un servizio nazionale di gestione delle copie dei backup "a freddo", al fine di offrire, alle Pubbliche Amministrazioni e operatori privati, un'infrastruttura con alti livelli di resilienza a supporto di una pronta riattivazione di sistemi e servizi a seguito di guasti o incidenti.



Attori responsabili
ACN



Altri soggetti interessati
DTD, Operatori privati



Anno di implementazione
2024

 METRICA

 INDICATORE

AFFIDABILITA'

21a
Pubbliche Amministrazioni e operatori privati che adottano il servizio nazionale di gestione delle copie dei backup "a freddo".

21a
Numero di Pubbliche Amministrazioni e operatori privati che adottano il servizio nazionale di gestione delle copie dei backup "a freddo", alla data di misurazione.


Alta

 LINEE GUIDA PER LA MISURAZIONE

Il target verrà definito in base al numero delle Pubbliche Amministrazioni e degli operatori privati che saranno individuati in fase di pianificazione della misura (verrà adottata una differenziazione per cluster).

 METRICA	 INDICATORE	AFFIDABILITA'
--	--	---------------

21b
 Pubbliche Amministrazioni e operatori privati che hanno eseguito test di ripristino tramite il servizio nazionale di gestione delle copie dei backup "a freddo".

21b
 Numero di Pubbliche Amministrazioni e operatori privati che hanno eseguito test di ripristino tramite il servizio nazionale di gestione delle copie dei backup "a freddo" alla data di misurazione.


 Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA	 INDICATORE	AFFIDABILITA'
--	--	---------------

21c
 Dati gestiti dal servizio nazionale di gestione delle copie dei backup "a freddo".

21c
 Quantità di dati gestiti dal servizio nazionale di gestione delle copie dei backup "a freddo", alla data di misurazione.


 Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

2.1.6 Promozione dell'uso della crittografia

Misura #22

Promuovere l'uso della crittografia in ambito non classificato, quale impostazione predefinita e comunque fin dalla fase di progettazione di reti, applicazioni e servizi, in conformità ai principi della sicurezza e della tutela della vita privata, nel rispetto dei principi stabiliti dalla normativa nazionale ed europea.



Attori responsabili

ACN



Altri soggetti interessati

DIS (UCSe), Min. Giustizia, Min. Difesa, MIMIT, DTD, Atenei, Ricerca, Operatori privati



Anno di implementazione

2023

METRICA

22a

Linee guida, attività ed eventi finalizzati a promuovere l'uso della crittografia in ambito non classificato.

INDICATORE

22a

Numero di linee guida, attività ed eventi finalizzati a promuovere l'uso della crittografia in ambito non classificato alla data di misurazione.

AFFIDABILITA'



Media

LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #23

Sviluppo di tecnologie/sistemi di cifratura nazionale in ambito non classificato. A sostegno di tale iniziativa è prevista la creazione di un ecosistema nazionale per il suo mantenimento ed evoluzione.



Attori responsabili

ACN



Altri soggetti interessati

DIS (UCSe), Min. Difesa, Atenei, Ricerca



Anno di implementazione

2024

METRICA

23a

Elaborati tecnici prodotti relativamente allo studio, analisi e sviluppo di tecnologie/sistemi di cifratura per la creazione, il mantenimento e l'evoluzione di un ecosistema nazionale in ambito non classificato.

INDICATORE

23a

Numero di elaborati tecnici prodotti relativamente allo studio, analisi e sviluppo di tecnologie/sistemi di cifratura per la creazione, il mantenimento e l'evoluzione di un ecosistema nazionale in ambito non classificato, alla data di misurazione.

AFFIDABILITA'



Alta

LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

23b

Addetti che contribuiscono allo studio, analisi e sviluppo di tecnologie/sistemi di cifratura per la creazione, il mantenimento e l'evoluzione di un ecosistema nazionale in ambito non classificato.

23b

Numero di addetti che contribuiscono allo studio, analisi e sviluppo di tecnologie/sistemi di cifratura per la creazione, il mantenimento e l'evoluzione di un ecosistema nazionale in ambito non classificato, alla data di misurazione.



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

2.1.7 Definizione e implementazione di un piano di contrasto alla disinformazione online

Misura #24

Implementare un'azione di coordinamento nazionale, coerente con le iniziative adottate a livello europeo e in sinergia con i Paesi like-minded, per prevenire e contrastare – anche attraverso campagne informative – la disinformazione online che, sfruttando le caratteristiche del dominio cibernetico, mira a condizionare/influenzare processi politici, economici e sociali del Paese.



Attori responsabili

PCM-DIE¹, DIS



Altri soggetti interessati

AISE, AISI, MAECI, Min. Interno, Min. Difesa, ACN, AGCOM



Anno di implementazione

2023

METRICA

24a
Iniziative volte a porre in essere un'azione di coordinamento nazionale per prevenire e contrastare la disinformazione online portate a termine.

INDICATORE

24a
Numero di iniziative volte a porre in essere un'azione di coordinamento nazionale per prevenire e contrastare la disinformazione online portate a termine nel periodo di riferimento.

AFFIDABILITA'



Media

LINEE GUIDA PER LA MISURAZIONE

N/A

METRICA

24b
Campagne informative condotte in merito alla disinformazione online.

INDICATORE

24b
Numero di campagne informative condotte in merito alla disinformazione online, nel periodo di riferimento.

AFFIDABILITA'



Alta

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere incluse tutte le attività di natura progettuale/singole iniziative portate a termine che concorrono in modo concreto alla realizzazione delle campagne informative in ambito cyber (e.g. creazione di concept note, contributi alla stesura di documenti, convocazione di una serie di meeting su tematica specifica).

METRICA

24c
Soggetti target delle campagne informative condotte in merito alla disinformazione online.

INDICATORE

24c
Numero di soggetti target delle campagne informative condotte in merito alla disinformazione online, nel periodo di riferimento.

AFFIDABILITA'



Alta

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo si dovrà fare riferimento ai cluster di soggetti destinatari delle campagne informative e.g. insegnanti, genitori, studenti, ecc.

¹ Dipartimento per l'Informazione e l'Editoria



2.2 Misure di risposta

2.2.1 Sistema di gestione crisi nazionale e transnazionale

Misura #25

Sviluppare un sistema di coordinamento continuativo di tutte le Amministrazioni che compongono il NCS, che garantisca una tempestiva e sinergica gestione dei vari possibili scenari di crisi cibernetica, nonché una immediata implementazione delle misure di risposta.



Attori responsabili
ACN-NCS²



Altri soggetti interessati
Altre Amministrazioni NCS



Anno di implementazione
2023



METRICA



INDICATORE

AFFIDABILITA'

25a

Iniziative per lo sviluppo di un sistema di coordinamento continuativo di tutte le Amministrazioni NCS.

25a

Numero di iniziative per lo sviluppo di un sistema di coordinamento continuativo di tutte le Amministrazioni NCS portate a termine nel periodo di riferimento.



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA



INDICATORE

AFFIDABILITA'

25b

Incontri per il coordinamento continuativo in merito ai possibili scenari di crisi cibernetica con le Amministrazioni che compongono il NCS.

25b

Numero di incontri per il coordinamento continuativo in merito ai possibili scenari di crisi cibernetica con le Amministrazioni che compongono il NCS nel periodo di riferimento.



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA



INDICATORE

AFFIDABILITA'

25c

Esercitazioni table-top di incident response effettuate.

25c

Numero di esercitazioni table-top di incident response effettuate nel periodo di riferimento.



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

²Il Nucleo per la Cybersicurezza è istituito presso l'ACN, che svolge ogni necessaria attività di supporto al suo funzionamento

Misura #26

Contribuire alla fattiva ed efficace attivazione dei meccanismi europei di risposta coordinata agli incidenti e alle crisi cibernetiche transnazionali su larga scala.



Attori responsabili

ACN-NCS²



Altri soggetti interessati

MAECI, altre Amministrazioni NCS



Anno di implementazione

2023

METRICA

INDICATORE

AFFIDABILITA'

26a

Iniziativa condotta per una fattiva attivazione dei meccanismi europei di risposta coordinata agli incidenti e alle crisi cibernetiche transnazionali su larga scala.

26a

Numero di iniziative condotte per una fattiva attivazione dei meccanismi europei di risposta coordinata agli incidenti e alle crisi cibernetiche transnazionali su larga scala nel periodo di riferimento.



Media

LINEE GUIDA PER LA MISURAZIONE

N/A

METRICA

INDICATORE

AFFIDABILITA'

26b

Enti coinvolti nella risposta coordinata agli incidenti e alle crisi cibernetiche transnazionali su larga scala.

26b

Numero di Enti coinvolti nella risposta coordinata agli incidenti e alle crisi cibernetiche transnazionali su larga scala, alla data di misurazione.



Alta

LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #27

Assicurare e facilitare modalità di notifica unitaria degli incidenti di sicurezza cibernetica allo CSIRT per rendere più efficace la capacità di risposta e allarme tempestivo.



Attori responsabili

ACN



Altri soggetti interessati

Min. Interno



Anno di implementazione

2025

METRICA

INDICATORE

AFFIDABILITA'

27a

Iniziativa condotta per assicurare e facilitare la notifica unitaria degli incidenti di sicurezza cibernetica allo CSIRT.

27a

Numero di iniziative condotte per assicurare e facilitare la notifica unitaria degli incidenti di sicurezza cibernetica allo CSIRT nel periodo di riferimento.



Alta

LINEE GUIDA PER LA MISURAZIONE

N/A

²Il Nucleo per la Cybersicurezza è istituito presso l'ACN, che svolge ogni necessaria attività di supporto al suo funzionamento

Misura #28

Sviluppare ulteriormente le capacità per assicurare una pronta attività di comunicazione istituzionale in caso di incidenti cyber rilevanti o di crisi cibernetica, nonché ogni qual volta si renda necessario svolgere azioni di sensibilizzazione nei confronti della popolazione civile.



Attori responsabili

PCM, ACN-NCS²



Altri soggetti interessati

Altre Amministrazioni NCS, Operatori privati



Anno di implementazione

2025



METRICA

28a

Iniziativa condotta per sviluppare le capacità per assicurare una pronta ed efficace attività di comunicazione istituzionale in caso di incidenti cyber rilevanti o di crisi cibernetica.



INDICATORE

28a

Numero di iniziative condotte per sviluppare le capacità per assicurare una pronta ed efficace attività di comunicazione istituzionale in caso di incidenti cyber rilevanti o di crisi cibernetica nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere incluse tutte le attività di natura progettuale/singole iniziative relative:

- setup del processo di comunicazione istituzionale in caso di incidenti o crisi cibernetica;
- identificazione dei soggetti coinvolti nelle segnalazioni e nelle comunicazioni, con particolare riferimento agli aspetti di continuità operativa (Emergency contact list);
- Definizione delle procedure standard di risposta ad eventi pre-classificati.

Misura #29

Assicurare il periodico aggiornamento delle procedure operative relative alle misure di risposta connesse ai vari scenari della minaccia cyber per le determinazioni del Presidente del Consiglio, ai sensi della vigente normativa nazionale, e per la conseguente corretta implementazione da parte dei soggetti interessati.



Attori responsabili

ACN-NCS²



Altri soggetti interessati

DIS, AISE, AISI, Min. Interno, Min. Difesa



Anno di implementazione

2025



METRICA

29a

Scenari di minaccia cyber per cui siano state definite le procedure operative relative alle misure di risposta.



INDICATORE

29a

Numero di scenari di minaccia cyber per cui siano state definite le procedure operative relative alle misure di risposta nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

²Il Nucleo per la Cybersicurezza è istituito presso l'ACN, che svolge ogni necessaria attività di supporto al suo funzionamento



 METRICA

 INDICATORE

AFFIDABILITA'

29b
Procedure operative aggiornate.

29b
Numero di procedure operative aggiornate nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

2.2.2 Servizi cyber nazionali

Misura #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.



Attori responsabili

ACN



Altri soggetti interessati

Atenei, Ricerca, Amministrazioni centrali, Operatori privati, Regioni e Province autonome



Anno di implementazione

2023

METRICA

INDICATORE

AFFIDABILITA'

30a
Organizzazioni collegate con l'HyperSOC.

30a
Numero di organizzazioni collegate con l'HyperSOC alla data di misurazione.



Alta

LINEE GUIDA PER LA MISURAZIONE

N/A

METRICA

INDICATORE

AFFIDABILITA'

30b
Scenari di monitoraggio implementati al fine di individuare precocemente eventuali “pattern” di attacco complessi.

30b
Numero di scenari di monitoraggio implementati al fine di individuare precocemente eventuali “pattern” di attacco complessi nel periodo di riferimento.



Alta

LINEE GUIDA PER LA MISURAZIONE

Si tratta di scenari di monitoraggio in generale, alcuni dei quali supportati da HPC.

METRICA

INDICATORE

AFFIDABILITA'

30c
Iniziative di analisi e condivisione di potenziali fattori di rischio.

30c
Numero di iniziative di analisi e condivisione di potenziali fattori di rischio portante a termine nel periodo di riferimento.




Alta

LINEE GUIDA PER LA MISURAZIONE




N/A




 METRICA	 INDICATORE	AFFIDABILITA'
30d Use Case implementati su infrastrutture di High Performance Computing.	30d Numero di Use Case implementati su infrastrutture di High Performance Computing nel periodo di riferimento.	 Media


 LINEE GUIDA PER LA MISURAZIONE
N/A




Misura #31

Stipulare apposite convenzioni con gli Internet Service Provider (ISP), al fine di condividere eventi di interesse, così da supportare sia il raggiungimento della misura 30, sia l'individuazione precoce di eventuali minacce emergenti e la mitigazione di attacchi al nostro Paese.

-  **Attori responsabili**
ACN
-  **Altri soggetti interessati**
DIS, ISP
-  **Anno di implementazione**
2023

 METRICA	 INDICATORE	AFFIDABILITA'
31a Convenzioni stipulate con gli Internet Service Provider (ISP) per condividere eventi di interesse e abilitare l'individuazione precoce di eventuali minacce emergenti e la mitigazione di attacchi al nostro Paese.	31a Numero di convenzioni stipulate con gli Internet Service Provider (ISP) per condividere eventi di interesse e abilitare l'individuazione precoce di eventuali minacce emergenti e la mitigazione di attacchi al nostro Paese alla data di misurazione.	 Alta

 LINEE GUIDA PER LA MISURAZIONE
N/A

 METRICA	 INDICATORE	AFFIDABILITA'
31b Scenari monitorati sulla base degli eventi di interesse condivisi dagli Internet Service Provider.	31b Numero di scenari monitorati sulla base degli eventi di interesse condivisi dagli Internet Service Provider alla data di misurazione.	 Media

 LINEE GUIDA PER LA MISURAZIONE
N/A

Misura #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.



Attori responsabili
ACN



Altri soggetti interessati
Amministrazioni NCS, Atenei, Ricerca, Operatori privati



Anno di implementazione
2024

METRICA

32a
Infrastruttura di High Performance Computing dedicata alla cybersecurity nazionale.

INDICATORE

32a
Capacità elaborativa dell'infrastruttura di High Performance Computing dedicata alla cybersecurity nazionale disponibile alla data di misurazione.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

L'unità di misura che verrà utilizzata per misurare la capacità elaborativa dell'infrastruttura sarà indicata con il target.

METRICA

32b
Strumenti di simulazione, basati sull'Intelligenza Artificiale e il machine learning.

INDICATORE

32b
Numero di strumenti di simulazione, basati sull'Intelligenza Artificiale e il machine learning disponibili alla data di misurazione.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #33

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.



Attori responsabili
ACN, Amministrazioni NCS



Altri soggetti interessati
Operatori privati



Anno di implementazione
2025

METRICA

33a
CERT, rappresentativi di settori di interesse, formalmente integrati con lo CSIRT Italia.

INDICATORE


33a
Numero di CERT, rappresentativi di settori di interesse, formalmente integrati con lo CSIRT Italia alla data di misurazione.


AFFIDABILITA'




LINEE GUIDA PER LA MISURAZIONE


Nel conteggio dovranno essere inclusi i CERT territoriali rappresentativi di settori di interesse. In continuità con il PNRR, dove si vuole creare e finanziare una rete di CERT regionali che lavorino in sinergia con lo CSIRT Italia, si è immaginato di incentivare la creazione/potenziamento di CERT settoriali, anche con il coinvolgimento delle Amministrazioni NCS per il loro settore di competenza.

METRICA	INDICATORE	AFFIDABILITA'
33b Procedure, processi e strumenti definiti 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.	33b Numero di procedure, processi e strumenti definiti 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 nel periodo di riferimento.	 Media

 LINEE GUIDA PER LA MISURAZIONE

N/A




METRICA	INDICATORE	AFFIDABILITA'
33c Operatori pubblici e privati che hanno adottato procedure, processi e strumenti definiti con l'obiettivo di assicurare la continuità operativa delle reti, dei sistemi informativi e dei servizi informatici.	33c Numero di operatori pubblici e privati che hanno adottato procedure, processi e strumenti definiti con l'obiettivo di assicurare la continuità operativa delle reti, dei sistemi informativi e dei servizi informatici alla data di misurazione.	 Media


 LINEE GUIDA PER LA MISURAZIONE


N/A

Misura #34


Creare un ISAC presso l'ACN, con il compito di coordinare la collazione e l'analisi di informazioni operazionali e strategiche a maggior valor aggiunto prodotte dai vari servizi cyber nazionali. La struttura sarà collegata alla rete europea degli ISAC contribuendo alla realizzazione dello "European CyberShield", previsto dalla Strategia di cybersecurity dell'UE.


-  **Attori responsabili**
ACN
-  **Altri soggetti interessati**
Amministrazioni NCS
-  **Anno di implementazione**
2023

METRICA	INDICATORE	AFFIDABILITA'
34a Destinatari dei servizi dell'ISAC istituito presso l'ACN.	34a Numero di destinatari dei servizi dell'ISAC istituito presso l'ACN alla data di misurazione.	 Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

METRICA	INDICATORE	AFFIDABILITA'
34b Analisi condotte congiuntamente alla rete europea degli ISAC.	34b Numero di analisi condotte congiuntamente alla rete europea degli ISAC nel periodo di riferimento.	 Media

 LINEE GUIDA PER LA MISURAZIONE

N/A



Misura #35

Promuovere la creazione di ISAC settoriali integrati con l'ISAC dell'ACN, anche mediante iniziative pubblico-private, così da favorire il potenziamento dello scambio informativo e di best-practice a servizio delle Pubbliche Amministrazioni e dell'industria nazionale.



Attori responsabili
ACN



Altri soggetti interessati
Amministrazioni centrali,
Regioni e Province autonome,
Operatori privati



Anno di implementazione
2025



METRICA

35a
ISAC settoriali integrati con l'ISAC dell'ACN.



INDICATORE

35a
Numero di ISAC settoriali integrati con l'ISAC dell'ACN alla data di misurazione.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

35b
Analisi condotte congiuntamente agli ISAC settoriali.



INDICATORE

35b
Numero di analisi condotte congiuntamente agli ISAC settoriali nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #36

Realizzare un programma di qualificazione in materia di incident response dei SOC/CERT/CSIRT di un gruppo di aziende selezionate, in grado di fornire supporto allo CSIRT Italia nel caso in cui dovesse verificarsi una moltitudine di incidenti cyber di natura sistemica



Attori responsabili
ACN



Altri soggetti interessati
Operatori privati



Anno di implementazione
2025



METRICA

36a
Procedure in materia di incident response emesse nel periodo di riferimento.



INDICATORE

36a
Numero di procedure in materia di incident response emesse nel periodo di riferimento.

AFFIDABILITA'




Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA	INDICATORE	AFFIDABILITA'
36b Aziende qualificate.	36b Numero di aziende qualificate alla data di misurazione.	 Alta

LINEE GUIDA PER LA MISURAZIONE
N/A

Misura #37

Promuovere la creazione di una gestione integrata e continuativa del rischio cyber nazionale, facilitata da attività di analisi della postura di sicurezza della Pubblica Amministrazione, nonché da strumenti di controllo e monitoraggio della supply chain.



Attori responsabili

ACN




Altri soggetti interessati

Amministrazioni NCS




Anno di implementazione


2023

METRICA	INDICATORE	AFFIDABILITA'
37a Procedure per la gestione integrata e continuativa del rischio cyber nazionale, in relazione agli ambiti identificati come prioritari.	37a Numero di procedure per la gestione integrata e continuativa del rischio cyber nazionale, in relazione agli ambiti identificati come prioritari, alla data di misurazione.	 Alta

LINEE GUIDA PER LA MISURAZIONE
N/A

METRICA	INDICATORE	AFFIDABILITA'
37b Ambiti coperti dal monitoraggio della supply chain.	37b Numero di ambiti coperti dal monitoraggio della supply chain alla data di misurazione.	 Media

LINEE GUIDA PER LA MISURAZIONE
Gli ambiti oggetto della presente metrica e del relativo indicatore riguardano sia componenti hardware che software da definire (ad es. router, ecc.).

METRICA	INDICATORE	AFFIDABILITA'
37c Enti della Pubblica Amministrazione oggetto di attività di analisi della postura di sicurezza.	37c Numero di Enti della Pubblica Amministrazione oggetto di attività di analisi della postura di sicurezza nel periodo di riferimento.	 Alta

LINEE GUIDA PER LA MISURAZIONE
N/A



 METRICA

 INDICATORE

AFFIDABILITA'

37d
Strumenti di controllo e monitoraggio della supply chain.

37d
Numero di strumenti di controllo e monitoraggio della supply chain disponibili alla data di misurazione.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

37e
Riscontri in fase ispettiva sulle misure di sicurezza PSNC specifiche per la supply chain.

37e
Numero di riscontri in fase ispettiva sulle misure di sicurezza PSNC specifiche per la supply chain alla data di misurazione.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

37f
ambiti coperti dal monitoraggio della supply chain.

37f
Numero di ambiti coperti dal monitoraggio della supply chain, nel periodo di riferimento.


Media

 LINEE GUIDA PER LA MISURAZIONE

N/A

2.2.3 Esercitazioni di cybersicurezza

Misura #38

Prevedere l'organizzazione di periodiche esercitazioni interministeriali, anche in ambito Perimetro, che riguardano aspetti tecnici e operativi di gestione di eventi o crisi con profili di cybersicurezza.



Attori responsabili
ACN



Altri soggetti interessati
Amministrazioni NCS,
Operatori privati



Anno di implementazione
2023



METRICA

38a

Esercitazioni interministeriali, anche in ambito Perimetro, che riguardano aspetti tecnici e operativi di gestione di eventi o crisi con profili di cybersicurezza.



INDICATORE

38a

Numero di esercitazioni interministeriali, anche in ambito Perimetro, che riguardano aspetti tecnici e operativi di gestione di eventi o crisi con profili di cybersicurezza condotte nel periodo di riferimento.



Alta

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

38b

Enti coinvolti nell'esecuzione di esercitazioni interministeriali, anche in ambito Perimetro, che riguardano aspetti tecnici e operativi di gestione di eventi o crisi con profili di cybersicurezza.



INDICATORE

38b

Numero di Enti coinvolti nell'esecuzione di esercitazioni interministeriali, anche in ambito Perimetro, che riguardano aspetti tecnici e operativi di gestione di eventi o crisi con profili di cybersicurezza condotte nel periodo di riferimento.



Alta

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #39

Promuovere e coordinare la partecipazione a esercitazioni europee e internazionali che riguardano la simulazione di eventi di natura cibernetica, al fine di innalzare la resilienza del Paese.



Attori responsabili

ACN-NCS²



Altri soggetti interessati

ACN, MAECI, Min. Interno, Min. Giustizia, Min. Difesa, MEF



Anno di implementazione

2023



METRICA

39a

Partecipazione a esercitazioni europee e internazionali che riguardano la simulazione di eventi di natura cibernetica, al fine di innalzare la resilienza del Paese.



INDICATORE

39a

Numero di esercitazioni europee e internazionali che riguardano la simulazione di eventi di natura cibernetica, al fine di innalzare la resilienza del Paese, cui si è partecipato nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

39b

Enti partecipanti a esercitazioni europee e internazionali che riguardano la simulazione di eventi di natura cibernetica, al fine di innalzare la resilienza del Paese.



INDICATORE

39b

Numero di enti che hanno partecipato a esercitazioni europee e internazionali che riguardano la simulazione di eventi di natura cibernetica, al fine di innalzare la resilienza del Paese, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo deve essere fatto riferimento sia agli enti pubblici che agli enti privati.

²Il Nucleo per la Cybersicurezza è istituito presso l'ACN, che svolge ogni necessaria attività di supporto al suo funzionamento



2.2.4 Definizione del posizionamento e della procedura nazionale in materia di attribuzione

Misura #40

Rafforzare i meccanismi nazionali volti all'applicazione degli strumenti di deterrenza definiti a livello europeo e internazionale per la risposta ad attacchi cyber. In tale contesto, si pone l'esigenza di definire un documento sul posizionamento e sulla procedura nazionale in materia di attribuzione.



Attori responsabili

DIS, AISE, AISI, MAECI



Altri soggetti interessati

ACN, Min. Difesa, Min. Interno, Altre Amministrazioni CISR



Anno di implementazione

2025



METRICA

40a

Iniziative e attività volte all'elaborazione del documento sul posizionamento e sulla procedura nazionale in materia di attribuzione.



INDICATORE

40a

Numero di iniziative e attività volte all'elaborazione del documento sul posizionamento e sulla procedura nazionale in materia di attribuzione portate a termine nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

40b

Iniziative e attività volte all'attuazione del documento sul posizionamento e sulla procedura nazionale in materia di attribuzione.



INDICATORE

40b

Numero di iniziative e attività volte all'attuazione del documento sul posizionamento e sulla procedura nazionale in materia di attribuzione, portate a termine nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere incluse tutte le attività di natura progettuale/singole iniziative portate a termine, volte all'applicazione delle misure/requisiti/attività definiti all'interno del documento sul posizionamento. Data la dipendenza dal documento di posizionamento questo indice verrà calcolato a partire dalla finalizzazione del documento stesso.

2.2.5 Contrasto al cybercrime

Misura #41

Potenziare ulteriormente le capacità di prevenzione e contrasto al crimine informatico da parte della Polizia Postale e delle comunicazioni e delle Forze di polizia, prevedendo anche specifiche attività di addestramento.



Attori responsabili

Min. Interno, Min. Giustizia, MEF



Anno di implementazione

2023

METRICA

41a
Attività di addestramento condotte da parte della Polizia Postale e delle comunicazioni e delle Forze di polizia in generale.

INDICATORE

41a
Numero di attività di addestramento condotte da parte della Polizia Postale e delle comunicazioni e delle Forze di polizia in generale nel periodo di riferimento.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere incluse tutte le attività di addestramento che consentono di sviluppare conoscenze e capacità strumentali al contrasto del crimine informatico e in ambito cyber.

METRICA

41b
Addetti della Polizia Postale e delle comunicazioni e delle Forze di polizia in generale coinvolti in attività di addestramento.

INDICATORE

41b
Numero di addetti della Polizia Postale e delle comunicazioni e delle Forze di polizia in generale coinvolti in attività di addestramento nel periodo di riferimento.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #42

Potenziare le competenze nel contrasto di attività volte a diffondere contenuti di odio, violenza e discriminazione online.



Attori responsabili

Min. Interno, Min. Giustizia, DIS



Altri soggetti interessati

MIM



Anno di implementazione

2023

METRICA

42a
Iniziative di formazione volte a potenziare le competenze nel contrasto di attività volte a diffondere contenuti di odio, violenza e discriminazione online.

INDICATORE

42a
Numero di iniziative di formazione volte a potenziare le competenze nel contrasto di attività volte a diffondere contenuti di odio, violenza e discriminazione online, nel periodo di riferimento.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere incluse tutte le attività, sia di natura progettuale che singole iniziative di qualsiasi durata temporale, che abbiano l'obiettivo di sensibilizzare i soggetti coinvolti rispetto alle tematiche indicate nella misura.



 METRICA

 INDICATORE

AFFIDABILITA'

42b

Soggetti coinvolti in iniziative di formazione volte a potenziare le competenze nel contrasto di attività volte a diffondere contenuti di odio, violenza e discriminazione online.

42b

Numeri di soggetti coinvolti in iniziative di formazione volte a potenziare le competenze nel contrasto di attività volte a diffondere contenuti di odio, violenza e discriminazione online, nel periodo di riferimento.



Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere inclusi tutti i soggetti sia pubblici che privati, sia persone fisiche che persone giuridiche.

Misura #43

Rafforzare ulteriormente la cooperazione internazionale e lo scambio informativo in materia di contrasto al crimine informatico con gli analoghi organismi europei, internazionali e degli altri Stati.



Attori responsabili

MAECI, Min. Interno, Min. Giustizia



Altri soggetti interessati

ACN



Anno di implementazione

2025

 METRICA

 INDICATORE

AFFIDABILITA'

43a

Iniziative sviluppate per la cooperazione internazionale e lo scambio informativo in materia di contrasto al crimine informatico con gli analoghi organismi europei, internazionali e degli altri Stati.

43a

Numero di iniziative sviluppate per la cooperazione internazionale e lo scambio informativo in materia di contrasto al crimine informatico con gli analoghi organismi europei, internazionali e degli altri Stati, nel periodo di riferimento.



Media

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #44

Assicurare una puntuale rilevazione statistica dei dati relativi ai reati informatici e quelli favoriti dall'informatica, acquisiti dalle Forze di polizia e dall'Autorità giudiziaria, per agevolarne l'analisi, anche al fine di eventuali integrazioni normative.



Attori responsabili

Min. Interno, Min. Giustizia



Altri soggetti interessati

ACN



Anno di implementazione

2025

 METRICA

 INDICATORE

AFFIDABILITA'

44a

Rendicontazioni statistiche in merito a dati relativi ai reati informatici e quelli favoriti dall'informatica.

44a

Numero di rendicontazioni statistiche in merito a dati relativi ai reati informatici e quelli favoriti dall'informatica effettuate nel periodo di riferimento.



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A



 METRICA

 INDICATORE

AFFIDABILITA'

44b

Enti che hanno contribuito a fornire dati relativi ai reati informatici e quelli favoriti dall'informatica alle Forze di polizia e all'Autorità giudiziaria.

44b

Numero di Enti che hanno contribuito a fornire dati relativi ai reati informatici e quelli favoriti dall'informatica alle Forze di polizia e all'Autorità giudiziaria nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

2.2.6 Capacità di deterrenza in ambito cibernetico

Misura #45

Rafforzare le capacità di deterrenza in ambito cibernetico, in ragione degli scenari in atto.



Attori responsabili

DIS, AISE, AISI, MAECI, Min. Difesa



Altri soggetti interessati

ACN



Anno di implementazione

2025



METRICA

45a

Iniziative promosse per rafforzare le capacità di deterrenza in ambito cibernetico, in ragione degli scenari in atto.



INDICATORE

45a

Numero di iniziative promosse per rafforzare le capacità di deterrenza in ambito cibernetico, in ragione degli scenari in atto nel periodo di riferimento.



Media



LINEE GUIDA PER LA MISURAZIONE

N/A

2.3 Misure di sviluppo

2.3.1 Centro nazionale di coordinamento

Misura #46

Realizzare e promuovere la partecipazione a progetti volti a supportare lo sviluppo di capacità, tecnologie e infrastrutture di cybersicurezza, mediante l'accesso ai pertinenti programmi di finanziamento dell'UE, assicurando il coinvolgimento del mondo industriale, accademico, della ricerca e della società civile, nonché favorendo sinergie con analoghe progettualità attive a livello nazionale.



Attori responsabili

ACN-NCC



Altri soggetti interessati

Amministrazioni centrali, Ricerca, Regioni e Province autonome, Operatori privati, Atenei



Anno di implementazione

2025



METRICA

46a

Progetti realizzati o promossi per supportare lo sviluppo di capacità, tecnologie e infrastrutture di cybersicurezza, mediante l'accesso ai pertinenti programmi di finanziamento dell'UE.



INDICATORE

46a

Numero di progetti realizzati o promossi per supportare lo sviluppo di capacità, tecnologie e infrastrutture di cybersicurezza, mediante l'accesso ai pertinenti programmi di finanziamento dell'UE, nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

46b

Fondi UE ottenuti per realizzare o promuovere progetti per supportare lo sviluppo di capacità, tecnologie e infrastrutture di cybersicurezza.



INDICATORE

46b

Ammontare di fondi UE ottenuti per realizzare o promuovere progetti per supportare lo sviluppo di capacità, tecnologie e infrastrutture di cybersicurezza, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

46c

Fondi UE utilizzati per realizzare o promuovere progetti per supportare lo sviluppo di capacità, tecnologie e infrastrutture di cybersicurezza.



INDICATORE

46c

Ammontare di fondi UE utilizzati per realizzare o promuovere progetti per supportare lo sviluppo di capacità, tecnologie e infrastrutture di cybersicurezza, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

Il target che verrà adottato sarà l'ammontare dei fondi UE ottenuti per realizzare o promuovere progetti per supportare lo sviluppo di capacità, tecnologie e infrastrutture di cybersicurezza.



 METRICA

 INDICATORE

AFFIDABILITA'

46d
Soggetti coinvolti (industria, accademia, società civile).

46d
Numero di soggetti coinvolti (industria, accademia, società civile) alla data di misurazione.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #47

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.



Attori responsabili

MIMIT, DTD, ACN



Altri soggetti interessati

Associazioni di categoria, Atenei, Ricerca



Anno di implementazione

2025

 METRICA

 INDICATORE

AFFIDABILITA'

47a
Iniziativa intraprese a supporto delle PMI coinvolte nelle attività del Digital Innovation Hub.

47a
Numero di iniziative intraprese a supporto delle PMI coinvolte nelle attività del Digital Innovation Hub nel periodo di riferimento.


Media

 LINEE GUIDA PER LA MISURAZIONE

Si fa qui riferimento sia ai DIH di Confindustria, sia ai 30 DIH recentemente nati su iniziativa del MIMIT, selezionati nell'ambito di una call europea afferente al Programma Europa digitale, di cui 13 finanziati al 100% (50% dall'Europa e 50% dall'Italia) e 17 per i quali si prevede il finanziamento del MIMIT al 50%.

Il MIMIT è altresì coinvolto in relazione ai centri di competenza ad alta specializzazione, di cui due dedicati alla cybersecurity (START 4.0 e CYBER 4.0). Per l'implementazione della misura 47, in aggiunta ai soggetti responsabili e interessati già indicati dal piano di implementazione, si ritiene necessario coinvolgere Confcommercio - Confagricoltura – Confartigianato.

 METRICA

 INDICATORE

AFFIDABILITA'

47b
PMI coinvolte nelle attività del Digital Innovation Hub.

47b
Numero di PMI coinvolte nelle attività del Digital Innovation Hub nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

«La categoria delle microimprese, delle piccole imprese e delle medie imprese (PMI) è costituita da imprese con meno di 250 occupati, il cui fatturato annuo non supera i 50 milioni di euro oppure il cui totale di bilancio annuo non supera i 43 milioni di euro». (Estratto dell'articolo 2 dell'allegato della raccomandazione 2003/361/CE).



2.3.2 Sviluppo di tecnologia nazionale ed europea

Misura #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.



Attori responsabili

ACN, MIMIT (Autorità delegata alle Politiche dello Spazio e dell'Aerospazio), Min. Difesa (ricerca militare)



Altri soggetti interessati

MUR e altre Amministrazioni NCS, Operatori Privati, Atenei, Ricerca



Anno di implementazione

2024



METRICA

48a

Progettualità avviate per sviluppare tecnologia nazionale ed europea nei segmenti più innovativi e sensibili (ad es. cloud ed edge computing, tecnologie basate su blockchain, spazio, ecc.).



INDICATORE

48a

Numero di progettualità avviate per sviluppare tecnologia nazionale ed europea nei segmenti più innovativi e sensibili (ad es. cloud ed edge computing, tecnologie basate su blockchain, spazio, ecc.) nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere conteggiate tutte le progettualità o iniziative volte a sviluppare, sia a livello nazionale che europeo, tecnologia relativa ai segmenti più innovativi e sensibili. Devono essere ricomprese anche le tecnologie parzialmente composte con componenti estere.

2.3.3 Realizzazione di un “parco nazionale della cybersicurezza”

Misura #49

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.



Attori responsabili

ACN, DTD, MEF, MIMIT, Min. Difesa (ricerca militare)



Altri soggetti interessati

Regioni e Province autonome, Atenei, Ricerca, Operatori privati



Anno di implementazione

2024



METRICA



INDICATORE

AFFIDABILITA'

49a

Soggetti che costituiscono o contribuiscono al “parco nazionale della cybersicurezza”.

49a

Numero di soggetti che costituiscono o contribuiscono al “parco nazionale della cybersicurezza” alla data di misurazione.



Alta



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere ricompresi i soggetti che pur non costituendo "il parco nazionale della cybersicurezza" apportano per la sua realizzazione un contributo di tipo materiale (e.g. supporto finanziario, operativo, di know-how ecc.).



METRICA



INDICATORE

AFFIDABILITA'

49b

Addetti che operano nell'ambito del “parco nazionale della cybersicurezza”.

49b

Numero di addetti che operano nell'ambito del “parco nazionale della cybersicurezza” alla data di misurazione.



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

2.3.4 L'impulso all'innovazione tecnologica e alla digitalizzazione

Misura #50

Promuovere l'internazionalizzazione delle imprese italiane che offrono prodotti e servizi di cybersecurity mediante il supporto agli investimenti, all'innovazione e alle esportazioni.



Attori responsabili

MAECI, MIMIT, ACN



Anno di implementazione

2025



METRICA



INDICATORE

AFFIDABILITA'

50a

Imprese italiane che offrono prodotti e servizi di cybersecurity supportate nel processo di internazionalizzazione.

50a

Numero di imprese italiane che offrono prodotti e servizi di cybersecurity supportate nel processo di internazionalizzazione, nel periodo di riferimento.



Alta



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere ricomprese le imprese italiane che godono di finanziamenti o incentivi di qualunque genere finalizzati a supportare ed incrementare l'internazionalizzazione dell'impresa stessa.



METRICA



INDICATORE

AFFIDABILITA'

50b

Investimenti volti a potenziare le capacità di export internazionale effettuati dalle imprese italiane che offrono prodotti e servizi di cybersecurity.

50b

Ammontare degli investimenti volti a potenziare le capacità di export internazionale effettuati dalle imprese italiane che offrono prodotti e servizi di cybersecurity, nel periodo di riferimento.



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA



INDICATORE

AFFIDABILITA'

50c

Iniziative volte a promuovere l'innovazione delle imprese al fine di potenziare le capacità di export internazionale poste in essere dalle imprese italiane che offrono prodotti e servizi di cybersecurity.

50c

Numero di iniziative volte a promuovere l'innovazione delle imprese al fine di potenziare le capacità di export internazionale poste in essere dalle imprese italiane che offrono prodotti e servizi di cybersecurity, nel periodo di riferimento.



Media



LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

50d

Esportazioni effettuate dalle imprese italiane che offrono prodotti e servizi di cybersecurity.

50d

Ammontare delle esportazioni effettuate dalle imprese italiane che offrono prodotti e servizi di cybersecurity nel periodo di riferimento.



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #51

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.



Attori responsabili

MIMIT, DTD, MAECI, ACN



Altri soggetti interessati

Regioni e Province autonome, Min. Difesa (ricerca militare)



Anno di implementazione

2025

 METRICA

 INDICATORE

AFFIDABILITA'

51a

Iniziative volte a 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.

51a

Numero di iniziative volte a 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, portate a termine nel periodo di riferimento.



Media

 LINEE GUIDA PER LA MISURAZIONE

Per prodotti/servizi si fa qui riferimento allo sviluppo di software nazionali come antivirus, piuttosto che una app di messaggistica. L'affidabilità viene verificata sia tramite certificazione da parte del CVCN sia assicurando una clean supply chain.

 METRICA

 INDICATORE

AFFIDABILITA'

51b

Imprese e startup sostenute nelle attività di progettazione e realizzazione di prodotti e servizi ad alta affidabilità.

51b

Numero di imprese e startup sostenute nelle attività di progettazione e realizzazione di prodotti e servizi ad alta affidabilità nel periodo di riferimento.




Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A






METRICA	INDICATORE	AFFIDABILITA'
51c Prodotti e servizi ad alta affidabilità (tra cui un'infrastruttura di comunicazione nazionale) sviluppati da imprese e startup italiane.	51c Numero di prodotti e servizi ad alta affidabilità (tra cui un'infrastruttura di comunicazione nazionale) sviluppati da imprese e startup italiane nel periodo di riferimento.	 Alta


LINEE GUIDA PER LA MISURAZIONE

Per prodotti/servizi si fa qui riferimento allo sviluppo di software nazionali come antivirus, piuttosto che una app di messaggistica. L'affidabilità viene verificata sia tramite certificazione da parte del CVCN sia assicurando una clean supply chain.

Misura #52


Incoraggiare la creazione di Product Security Incident Response Team (PSIRT) da parte degli operatori privati, per accrescere le loro capacità di gestire le vulnerabilità di prodotti ICT e per contribuire all'adozione di policy di divulgazione coordinata di vulnerabilità e alla relativa implementazione

-  **Attori responsabili**
ACN, MIMIT
-  **Altri soggetti interessati**
Operatori privati, Associazioni di categoria
-  **Anno di implementazione**
2025

METRICA	INDICATORE	AFFIDABILITA'
52a Iniziative volte a incoraggiare la creazione di Product Security Incident Response Team (PSIRT) da parte degli operatori privati e l'adozione e l'implementazione di policy di divulgazione coordinata di vulnerabilità.	52a Numero di iniziative volte a incoraggiare la creazione di Product Security Incident Response Team (PSIRT) da parte degli operatori privati e l'adozione e l'implementazione di policy di divulgazione coordinata di vulnerabilità nel periodo di riferimento.	 Media

LINEE GUIDA PER LA MISURAZIONE

Verrà effettuata un'attività di sensibilizzazione, associata al dispiegamento di fondi su iniziativa privata.

METRICA	INDICATORE	AFFIDABILITA'
52b Operatori privati che contribuiscono a realizzare Product Security Incident Response Team (PSIRT).	52b Numero di operatori privati che contribuiscono a realizzare Product Security Incident Response Team (PSIRT) alla data di misurazione.	 Alta

LINEE GUIDA PER LA MISURAZIONE

N/A



 METRICA

 INDICATORE

AFFIDABILITA'

52c
Iniziative volte alla definizione di policy (private) di divulgazione coordinata di vulnerabilità.

52c
Numero di Iniziative volte alla definizione di policy (private) di divulgazione coordinata di vulnerabilità poste in essere nel periodo di riferimento.


Media

 LINEE GUIDA PER LA MISURAZIONE

La misura fa riferimento alla possibilità che i privati, in aggiunta e coordinamento con la policy pubblica nazionale, si dotino di Policy private da loro elaborate. Le policy private non devono comunque essere in contrasto rispetto alla normativa nazionale.

 METRICA

 INDICATORE

AFFIDABILITA'

52d
Policy di divulgazione coordinata di vulnerabilità adottate e implementate da operatori privati, in aggiunta alla policy pubblica.

52d
Numero di Policy di divulgazione coordinata di vulnerabilità adottate e implementate da operatori privati, in aggiunta alla policy pubblica, nel periodo di riferimento.


Media

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

52e
Casi in cui sono state applicate le policy private di divulgazione coordinata di vulnerabilità adottate da operatori privati.

52e
Numero di casi in cui sono state applicate le policy di divulgazione coordinata di vulnerabilità adottate da operatori privati, nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel conteggio dovranno essere ricompresi sia i casi di applicazione della policy di divulgazione coordinata di vulnerabilità pubblica sia i casi di applicazione di policy private.

2.3.5 Sviluppo industriale, tecnologico e della ricerca

Misura #53

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.



Attori responsabili

ACN, DTD, MIMIT, MUR, Min. Difesa



Altri soggetti interessati

Atenei, Ricerca, Regioni e Province autonome



Anno di implementazione

2025



METRICA

53a

Iniziative volte 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 che sono state promosse.



INDICATORE

53a

Numero di iniziative volte 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 che sono state promosse nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

Attualmente l'ACN sta sviluppando una Roadmap per la ricerca e l'innovazione, che consta di un'Agenda con delle priorità e di un Piano di incentivazione per ricerca e innovazione sui temi dell'Agenda che prevederà anche dei finanziamenti.



METRICA

53b

Prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore sviluppati a seguito di specifiche iniziative progettuali.



INDICATORE

53b

Numero di prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore sviluppati a seguito di specifiche iniziative progettuali nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

53c

Studio, analisi e sviluppo di algoritmi e tecniche crittografiche nazionali a seguito di specifiche iniziative progettuali.



INDICATORE

53c

Numero di elaborati tecnici prodotti relativi a studio, analisi e sviluppo di algoritmi e tecniche crittografiche nazionali a seguito di specifiche iniziative progettuali, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #54

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.



Attori responsabili

ACN, DTD, MEF, MIMIT, MUR, Min. Difesa



Altri soggetti interessati

Operatori privati, Atenei, Ricerca



Anno di implementazione

2025

METRICA

54a
Iniziative di ricerca e sviluppo relative, totalmente o parzialmente, alla cybersicurezza, con particolare riferimento alle startup e alle PMI innovative.

INDICATORE

54a
Numero di iniziative di ricerca e sviluppo relative, totalmente o parzialmente, alla cybersicurezza, con particolare riferimento alle startup e alle PMI innovative, poste in essere nel periodo di riferimento.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

Attualmente l'ACN sta sviluppando una Roadmap per la ricerca e l'innovazione, che consta di un'Agenda con delle priorità e di un Piano di incentivazione per la ricerca e l'innovazione sui temi dell'Agenda che prevederà anche dei finanziamenti.

METRICA

54b
Finanziamenti erogati per la componente di cybersicurezza, in termini percentuali, per iniziative di ricerca e lo sviluppo, con particolare riferimento alle start-up e alle PMI innovative.

INDICATORE

54b
Ammontare dei finanziamenti erogati per la componente di cybersicurezza, in termini percentuali, per iniziative di ricerca e lo sviluppo, con particolare riferimento alle start-up e alle PMI innovative nel periodo di riferimento.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #55

Promuovere la digitalizzazione e l'innovazione, nonché rafforzare la sicurezza nella Pubblica Amministrazione, anche mediante l'impiego delle risorse del PNRR.



Attori responsabili

DTD, ACN



Altri soggetti interessati

MPA, Altre Amministrazioni centrali, Regioni e Province autonome



Anno di implementazione

2023

METRICA

55a
Iniziative volte a promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione.

INDICATORE

55a
Numero di iniziative volte a promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione, portate a termine nel periodo di riferimento.


AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE


N/A



METRICA	INDICATORE	AFFIDABILITA'
55b Iniziative volte a rafforzare la cybersicurezza nella Pubblica Amministrazione.	55b Numero di iniziative volte a rafforzare la cybersicurezza nella Pubblica Amministrazione, portate a termine nel periodo di riferimento.	 Media


 LINEE GUIDA PER LA MISURAZIONE

N/A

METRICA	INDICATORE	AFFIDABILITA'
55c Fondi ottenuti e utilizzati per promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione.	55c Ammontare dei fondi ottenuti e utilizzati per promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione, nel periodo di riferimento.	 Alta


 LINEE GUIDA PER LA MISURAZIONE

N/A

METRICA	INDICATORE	AFFIDABILITA'
55d Fondi PNRR ottenuti e utilizzati per promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione.	55d Ammontare dei fondi PNRR ottenuti e utilizzati per promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione, nel periodo di riferimento.	 Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

METRICA	INDICATORE	AFFIDABILITA'
55e Fondi ottenuti e utilizzati per rafforzare la cybersicurezza nella Pubblica Amministrazione.	55e Ammontare dei fondi ottenuti e utilizzati per rafforzare la cybersicurezza nella Pubblica Amministrazione, nel periodo di riferimento.	 Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

55f
Fondi PNRR ottenuti e utilizzati per rafforzare la cybersicurezza nella Pubblica Amministrazione.



INDICATORE

55f
Ammontare dei fondi PNRR ottenuti e utilizzati per rafforzare la cybersicurezza nella Pubblica Amministrazione, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

55g
Enti e distribuzione territoriale (a livello di Regione) che hanno ottenuto e utilizzato fondi per promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione.



INDICATORE

55g
Numero di enti e distribuzione territoriale (a livello di Regione) che hanno ottenuto e utilizzato fondi per promuovere la digitalizzazione e l'innovazione nella Pubblica Amministrazione, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

55h
Enti e distribuzione territoriale (a livello di Regione) che hanno ottenuto e utilizzato fondi per rafforzare la cybersicurezza nella Pubblica Amministrazione.



INDICATORE

55h
Numero di enti e distribuzione territoriale (a livello di Regione) che hanno ottenuto e utilizzato fondi per rafforzare la cybersicurezza nella Pubblica Amministrazione, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #56

Promuovere la digitalizzazione e l'innovazione del sistema produttivo nazionale, anche mediante l'impiego delle risorse del PNRR.



Attori responsabili

DTD, MIMIT, ACN



Altri soggetti interessati

Amministrazioni centrali, Regioni e Province autonome



Anno di implementazione

2025



METRICA

56a

Iniziative per la digitalizzazione e l'innovazione del sistema produttivo nazionale promosse, anche mediante l'impiego delle risorse del PNRR.



INDICATORE

56a

Numero di iniziative per la digitalizzazione e l'innovazione del sistema produttivo nazionale promosse, anche mediante l'impiego delle risorse del PNRR, nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

56b

Fondi utilizzati per iniziative per la digitalizzazione e l'innovazione del sistema produttivo nazionale.



INDICATORE

56b

Ammontare dei fondi utilizzati per iniziative per la digitalizzazione e l'innovazione del sistema produttivo nazionale nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

56c

Fondi PNRR utilizzati per iniziative per la digitalizzazione e l'innovazione del sistema produttivo nazionale.



INDICATORE

56c

Ammontare dei fondi PNRR utilizzati per iniziative per la digitalizzazione e l'innovazione del sistema produttivo nazionale nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #57

Promuovere la sicurezza cibernetica degli Internet Exchange Point nazionali, anche al fine di assicurare una rete Internet libera, aperta e trasparente.



Attori responsabili

ACN



Altri soggetti interessati

IXP



Anno di implementazione

2025



METRICA

57a

Iniziative promosse per la sicurezza cibernetica degli Internet Exchange Point nazionali, anche al fine di assicurare una rete Internet libera, aperta e trasparente.



INDICATORE

57a

Numero di iniziative promosse per la sicurezza cibernetica degli Internet Exchange Point nazionali, anche al fine di assicurare una rete Internet libera, aperta e trasparente, nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

57b

Internet Exchange Point nazionali coinvolti in iniziative promosse per la sicurezza cibernetica, anche al fine di assicurare una rete Internet libera, aperta e trasparente.



INDICATORE

57b

Numero di Internet Exchange Point nazionali coinvolti in iniziative promosse per la sicurezza cibernetica, anche al fine di assicurare una rete Internet libera, aperta e trasparente, alla data di misurazione.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #58

Sviluppare servizi pubblici digitali per la Pubblica Amministrazione a livello centrale e locale.



Attori responsabili

DTD



Altri soggetti interessati

ACN



Anno di implementazione

2024



METRICA

58a

Iniziative aventi ad oggetto lo sviluppo di servizi pubblici digitali per la Pubblica Amministrazione a livello centrale e locale.



INDICATORE

58a

Numero di iniziative aventi ad oggetto lo sviluppo di servizi pubblici digitali per la Pubblica Amministrazione a livello centrale e locale, portate a termine nel periodo di riferimento.

AFFIDABILITA'






Alta






LINEE GUIDA PER LA MISURAZIONE


N/A



 METRICA	 INDICATORE	AFFIDABILITA'
58b Servizi pubblici digitali sviluppati per la Pubblica Amministrazione a livello centrale e locale.	58b Numero di servizi pubblici digitali sviluppati per la Pubblica Amministrazione a livello centrale e locale, nel periodo di riferimento.	 Alta

 LINEE GUIDA PER LA MISURAZIONE
N/A

 METRICA	 INDICATORE	AFFIDABILITA'
58c Enti della Pubblica Amministrazione centrale e locale, per cui si è proceduto allo sviluppo di servizi pubblici digitali.	58c Numero di Enti della Pubblica Amministrazione centrale e locale, per cui si è proceduto allo sviluppo di servizi pubblici digitali, nel periodo di riferimento.	 Alta

 LINEE GUIDA PER LA MISURAZIONE
N/A

2.4 Fattori abilitanti

2.4.1 Formazione

Misura #59

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.



Attori responsabili

MIM, MUR, Atenei, ACN, Min. Difesa (alta formazione)



Altri soggetti interessati

PCM, Min. Difesa, Min. Interno, Regioni e Province autonome



Anno di implementazione

2024



METRICA

59a

Percorsi formativi dedicati con diversi livelli di specializzazione in cybersecurity, anche per personale docente.



INDICATORE

59a

Numero di percorsi formativi dedicati con diversi livelli di specializzazione in cybersecurity, anche per personale docente, sviluppati nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

Il calcolo del presente indice verrà eseguito dall'ACN grazie alle singole numeriche fornite per i sottoindicatori (dal 59a.1 al 59a.6) in quanto rappresenta la sommatoria di tutti i percorsi di specializzazione in cybersecurity svolti dai diversi enti e per i diversi livelli di formazione.



METRICA

59a.1

Percorsi formativi di specializzazione in cybersecurity sviluppati per il personale docente.



INDICATORE

59a.1

Numero di percorsi formativi di specializzazione in cybersecurity sviluppati per il personale docente, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

59a.2

Percorsi formativi di specializzazione in cybersecurity sviluppati per la scuola primaria e secondaria.



INDICATORE

59a.2

Numero di percorsi formativi di specializzazione in cybersecurity sviluppati per la scuola primaria e secondaria, nel periodo di riferimento.

AFFIDABILITA'







Alta







LINEE GUIDA PER LA MISURAZIONE




N/A


 METRICA	 INDICATORE	AFFIDABILITA'
59a.3 Corsi post-diploma (ITS) di specializzazione in cybersecurity sviluppati.	59a.3 Numero di corsi post-diploma (ITS) di specializzazione in cybersecurity sviluppati, nel periodo di riferimento.	 Alta




 LINEE GUIDA PER LA MISURAZIONE
N/A


 METRICA	 INDICATORE	AFFIDABILITA'
59a.4 Corsi universitari di laurea e laurea magistrale in cybersecurity sviluppati.	59a.4 Numero di corsi universitari di laurea e laurea magistrale in cybersecurity sviluppati, nel periodo di riferimento.	 Alta

 LINEE GUIDA PER LA MISURAZIONE
N/A

 METRICA	 INDICATORE	AFFIDABILITA'
59a.5 Dottorati di ricerca e master in cybersecurity sviluppati.	59a.5 Numero di dottorati di ricerca e master in cybersecurity sviluppati, nel periodo di riferimento.	 Alta

 LINEE GUIDA PER LA MISURAZIONE
N/A

 METRICA	 INDICATORE	AFFIDABILITA'
59a.6 Percorsi formativi in cybersecurity sviluppati per Scuole di formazione delle Pubbliche Amministrazioni.	59a.6 Numero di percorsi formativi in cybersecurity sviluppati per Scuole di formazione delle Pubbliche Amministrazioni, nel periodo di riferimento.	 Alta

 LINEE GUIDA PER LA MISURAZIONE
N/A

 METRICA

59b
Soggetti coinvolti in percorsi formativi dedicati con diversi livelli di specializzazione in cybersecurity, anche per personale docente.

 INDICATORE

59b
Numero di soggetti coinvolti in percorsi formativi dedicati con diversi livelli di specializzazione in cybersecurity, anche per personale docente, nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

Il calcolo del presente indice verrà eseguito dall'ACN grazie alle singole numeriche fornite per i sottoindicatori (dal 59b.1 al 59b.6) in quanto rappresenta la sommatoria di tutti i soggetti coinvolti in percorsi di specializzazione in cybersecurity svolti dai diversi enti e per i diversi livelli di formazione.

 METRICA

59b.1
Docenti coinvolti in percorsi formativi ad hoc di specializzazione in cybersecurity.

 INDICATORE

59b.1
Numero di docenti coinvolti in percorsi formativi ad hoc di specializzazione in cybersecurity nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59b.2
Soggetti coinvolti in percorsi formativi di specializzazione in cybersecurity sviluppati per la scuola primaria e secondaria.

 INDICATORE

59b.2
Numero di soggetti coinvolti in percorsi formativi di specializzazione in cybersecurity sviluppati per la scuola primaria e secondaria nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59b.3
Soggetti coinvolti in corsi post-diploma (ITS) di specializzazione in cybersecurity.

 INDICATORE

59b.3
Numero di soggetti coinvolti in corsi post-diploma (ITS) di specializzazione in cybersecurity, nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59b.4
Soggetti coinvolti in corsi universitari di laurea e laurea magistrale in cybersecurity.

 INDICATORE

59b.4
Numero di soggetti coinvolti in corsi universitari di laurea e laurea magistrale in cybersecurity, nel periodo di riferimento.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59b.5
Soggetti coinvolti in dottorati di ricerca e master in cybersecurity.

 INDICATORE

59b.5
Numero di soggetti coinvolti in dottorati di ricerca e master in cybersecurity, nel periodo di riferimento.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59b.6
Soggetti coinvolti in percorsi formativi in cybersecurity sviluppati per Scuole di formazione delle Pubbliche Amministrazioni.

 INDICATORE

59b.6
Numero di soggetti coinvolti in percorsi formativi in cybersecurity sviluppati per Scuole di formazione delle Pubbliche Amministrazioni, nel periodo di riferimento.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59c
Fondi utilizzati per finanziare percorsi formativi dedicati con diversi livelli di specializzazione in cybersecurity, anche per personale docente.

 INDICATORE

59c
Ammontare dei fondi utilizzati per finanziare percorsi formativi dedicati con diversi livelli di specializzazione in cybersecurity, anche per personale docente, nel periodo di riferimento.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

Il calcolo del presente indice verrà eseguito dall'ACN grazie alle singole numeriche fornite per i sottoindicatori (dal 59c.1 al 59c.6) in quanto rappresenta la sommatoria di tutti i fondi utilizzati per finanziare percorsi di specializzazione in cybersecurity svolti dai diversi enti e per i diversi livelli di formazione.

 METRICA

59c.1
Fondi utilizzati per finanziare percorsi formativi di specializzazione in cybersecurity sviluppati per il personale docente.

 INDICATORE

59c.1
Ammontare dei fondi utilizzati per finanziare percorsi formativi di specializzazione in cybersecurity sviluppati per il personale docente, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59c.2
Fondi utilizzati per finanziare percorsi formativi di specializzazione in cybersecurity sviluppati per la scuola primaria e secondaria.

 INDICATORE

59c.2
Ammontare dei fondi utilizzati per finanziare percorsi formativi di specializzazione in cybersecurity sviluppati per la scuola primaria e secondaria, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59c.3
Fondi utilizzati per finanziare corsi post-diploma (ITS) di specializzazione in cybersecurity sviluppati.

 INDICATORE

59c.3
Ammontare dei fondi utilizzati per finanziare corsi post-diploma (ITS) di specializzazione in cybersecurity, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59c.4
Fondi utilizzati per finanziare corsi universitari di laurea e laurea magistrale in cybersecurity.

 INDICATORE

59c.4
Ammontare dei fondi utilizzati per finanziare corsi universitari di laurea e laurea magistrale in cybersecurity, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59c.5
Fondi utilizzati per finanziare dottorati di ricerca e master in cybersecurity.

 INDICATORE

59c.5
Ammontare dei fondi utilizzati per finanziare dottorati di ricerca e master in cybersecurity, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59c.6
Fondi utilizzati per finanziare percorsi formativi in cybersecurity sviluppati per Scuole di formazione delle Pubbliche Amministrazioni.

 INDICATORE

59c.6
Ammontare dei fondi utilizzati per finanziare percorsi formativi in cybersecurity sviluppati per Scuole di formazione delle Pubbliche Amministrazioni, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59d
Progetti finanziati relativi a percorsi formativi sviluppati con diversi livelli di specializzazione in cybersecurity, anche per personale docente.

 INDICATORE

59d
Numero di progetti finanziati relativi a percorsi formativi sviluppati con diversi livelli di specializzazione in cybersecurity, anche per personale docente, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

Il calcolo del presente indice verrà eseguito dall'ACN grazie alle singole numeriche fornite per i sottoindicatori (dal 59d.1 al 59d.6) in quanto rappresenta la sommatoria di tutti i progetti finanziati relativi a percorsi di specializzazione in cybersecurity svolti dai diversi enti e per i diversi livelli di formazione.

 METRICA

59d.1
Progetti finanziati relativi a percorsi formativi di specializzazione in cybersecurity sviluppati per il personale docente.

 INDICATORE

59d.1
Numero di progetti finanziati relativi a percorsi formativi di specializzazione in cybersecurity sviluppati per il personale docente, nel periodo di riferimento

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA


59d.2
Progetti finanziati relativi a percorsi formativi di specializzazione in cybersecurity sviluppati per la scuola primaria e secondaria.

 INDICATORE

59d.2
Numero di progetti finanziati relativi a percorsi formativi di specializzazione in cybersecurity sviluppati per la scuola primaria e secondaria, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59d.3
Progetti finanziati relativi a corsi post-diploma (ITS) di specializzazione in cybersecurity.

 INDICATORE

59d.3
Numero di progetti finanziati relativi a corsi post-diploma (ITS) di specializzazione in cybersecurity, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59d.4
Progetti finanziati relativi a corsi universitari di laurea e laurea magistrale in cybersecurity.

 INDICATORE

59d.4
Numero di progetti finanziati relativi a corsi universitari di laurea e laurea magistrale in cybersecurity, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59d.5
Progetti finanziati relativi a dottorati di ricerca e master in cybersecurity.

 INDICATORE

59d.5
Numero di progetti finanziati relativi a dottorati di ricerca e master in cybersecurity, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

59d.6
Progetti finanziati relativi a percorsi formativi in cybersecurity sviluppati per Scuole di formazione delle Pubbliche Amministrazioni.

 INDICATORE

59d.6
Numero di progetti finanziati relativi a percorsi formativi in cybersecurity sviluppati per Scuole di formazione delle Pubbliche Amministrazioni, nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #60

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).



Attori responsabili

MIM, MUR, Atenei, ACN



Altri soggetti interessati

Associazioni di categoria, Enti di formazione accreditati, Operatori privati, Regioni e Province autonome



Anno di implementazione

2025

 METRICA

60a
Istituti Tecnici Superiori (ITS) che hanno avviato percorsi di cybersecurity.

 INDICATORE

60a
Numero di Istituti Tecnici Superiori (ITS) che hanno avviato percorsi di cybersecurity nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

60b
Studenti degli Istituti Tecnici Superiori (ITS) coinvolti in percorsi di cybersecurity.

 INDICATORE

60b
Numero di studenti degli Istituti Tecnici Superiori (ITS) coinvolti in percorsi di cybersecurity, nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

60c
Studenti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, disoccupati o inoccupati) coinvolti in percorsi di cybersecurity.

 INDICATORE

60c
Numero di studenti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, disoccupati o inoccupati) coinvolti in percorsi di cybersecurity alla data di misurazione.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #61

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.



Attori responsabili

ACN, Atenei, MIM, MUR



Altri soggetti interessati

Operatori privati, Regioni e Province autonome



Anno di implementazione

2025

 METRICA

61a
Giornate uomo impiegate per la realizzazione di un sistema nazionale di certificazione in ambito cybersecurity.

 INDICATORE

61a
Numero di giornate uomo impiegate per la realizzazione di un sistema nazionale di certificazione in ambito cybersecurity nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

Il conteggio fa riferimento al totale cumulato delle giornate erogate da dipendenti pubblici dedicati o che svolgono, anche, altre mansioni.

 METRICA

61b
Mappatura dei percorsi di formazione, formativi e professionali, relativi alla cybersecurity.

 INDICATORE

61b
Numero di percorsi di formazione, formativi e professionali, relativi alla cybersecurity mappati nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

61c
Requisiti individuati nell'ambito della realizzazione del sistema nazionale di certificazione in ambito cybersecurity.

 INDICATORE

61c
Numero di requisiti individuati nell'ambito della realizzazione del sistema nazionale di certificazione in ambito cybersecurity nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

61d
Corsi di formazione approvati da ACN che abilitano il conseguimento della certificazione di cybersecurity.

 INDICATORE

61d
Numero di corsi di formazione approvati da ACN che abilitano il conseguimento della certificazione di cybersecurity, nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

61e
Discenti che hanno conseguito la certificazione di cybersecurity.

 INDICATORE

61e
Numero di discenti che hanno conseguito la certificazione di cybersecurity, nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

61f
Discenti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, disoccupati o inoccupati, diversamente abili) che hanno conseguito la certificazione di cybersecurity.

 INDICATORE

61f
Numero di discenti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, disoccupati o inoccupati, diversamente abili) che hanno conseguito la certificazione di cybersecurity alla data di misurazione.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #62

Elaborare uno strumento di formazione e sensibilizzazione online, rivolto alla cittadinanza in generale, che consente, al termine del percorso, di auto-testare le competenze e le sensibilità acquisite e di ottenere un attestato. Lo scopo è quello di creare un primo modulo per avviare una e-Academy dell'Agencia per la Cybersicurezza Nazionale



Attori responsabili

ACN



Anno di implementazione

2023



METRICA

62a

Cittadini che hanno conseguito l'attestato tramite la e-Academy dell'Agencia per la Cybersicurezza Nazionale.



INDICATORE

62a

Numero di cittadini che hanno conseguito l'attestato tramite la e-Academy dell'Agencia per la Cybersicurezza Nazionale, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #63

Dispiegare fondi da dedicare alla formazione professionale nei settori pubblico e privato, al fine di agevolare il passaggio dal mondo scolastico a quello del lavoro e conseguire, così, una sovranità nazionale digitale delle competenze.



Attori responsabili

DTD, MEF



Altri soggetti interessati

ACN, Min. Lavoro, Regioni e Province autonome, Operatori privati



Anno di implementazione

2024



METRICA

63a

Fondi dedicati alla formazione professionale nei settori pubblico e privato in ambito cybersecurity, al fine di agevolare il passaggio dal mondo scolastico a quello del lavoro.



INDICATORE

63a

Ammontare dei fondi dedicati alla formazione professionale nei settori pubblico e privato in ambito cybersecurity, al fine di agevolare il passaggio dal mondo scolastico a quello del lavoro, impiegati nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

63b

Soggetti coinvolti nella formazione professionale nei settori pubblico e privato in ambito cybersecurity, specificamente finanziata.



INDICATORE

63b

Numero di soggetti coinvolti nella formazione professionale nei settori pubblico e privato in ambito cybersecurity, specificamente finanziata, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



 METRICA

 INDICATORE

AFFIDABILITA'

63c

Soggetti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, disoccupati o inoccupati, diversamente abili) coinvolti nella formazione professionale nei settori pubblico e privato in ambito cybersecurity, specificamente finanziata.

63c

Numero di soggetti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, disoccupati o inoccupati, diversamente abili) coinvolti nella formazione professionale nei settori pubblico e privato in ambito cybersecurity, specificamente finanziata, nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #64

Prevedere incentivi per lo sviluppo di start-up operanti nel settore della cybersecurity e partnership pubblico-privato con aziende di cybersecurity a conduzione femminile.



Attori responsabili

MEF, MIMIT, DTD



Altri soggetti interessati

Min. Lavoro, Regioni e Province autonome



Anno di implementazione

2025

 METRICA

 INDICATORE

AFFIDABILITA'

64a

Iniziative per lo sviluppo di start-up operanti nel settore della cybersecurity a conduzione femminile.

64a

Numero di iniziative per lo sviluppo di start-up operanti nel settore della cybersecurity a conduzione femminile, nel periodo di riferimento.


Media

 LINEE GUIDA PER LA MISURAZIONE

Al fine di valutare la fattibilità della misura, sono stati consultati qualificati rappresentanti di CDP Venture Capital SGR SpA (CDO VC), la SGR che gestisce capitali MIMIT da investire in capitale di rischio. CDP VC ha fatto presente la difficoltà a garantire l'attuazione della misura nella parte in cui stabilisce il requisito della conduzione femminile. In sostanza, sarebbe possibile incentivare lo sviluppo del settore industriale della cybersecurity, anche nelle start-up; è invece estremamente difficoltoso che questo sviluppo riguardi le imprese del settore che siano anche a conduzione femminile.

 METRICA

 INDICATORE

AFFIDABILITA'

64b

Iniziative volte ad incentivare partnership pubblico-privato con aziende di cybersecurity a conduzione femminile.

64b

Numero di iniziative volte ad incentivare partnership pubblico-privato con aziende di cybersecurity a conduzione femminile, nel periodo di riferimento.


Media

 LINEE GUIDA PER LA MISURAZIONE

N/A



 METRICA

64c
Start-up operanti nel settore della cybersecurity a conduzione femminile avviate.

 INDICATORE

64c
Numero di start-up operanti nel settore della cybersecurity a conduzione femminile avviate nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

64d
Partnership pubblico-privato attivate con aziende di cybersecurity a conduzione femminile.

 INDICATORE

64d
Numero di partnership pubblico-privato attivate con aziende di cybersecurity a conduzione femminile nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

64e
Aziende coinvolte in iniziative di incentivazione per lo sviluppo di start-up operanti nel settore della cybersecurity a conduzione femminile.

 INDICATORE

64e
Numero di aziende coinvolte in iniziative di incentivazione per lo sviluppo di start-up operanti nel settore della cybersecurity a conduzione femminile, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

64f
Aziende coinvolte in partnership pubblico-privato con aziende di cybersecurity a conduzione femminile.

 INDICATORE

64f
Numero di aziende coinvolte in partnership pubblico-privato con aziende di cybersecurity a conduzione femminile, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #65

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 propizzarne 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



Attori responsabili

PCM, MIM, MUR, Atenei, CINI, ACN



Altri soggetti interessati

Min. Difesa



Anno di implementazione

2025



METRICA

65a

Iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica.



INDICATORE

65a

Numero di iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica promosse nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere considerate tutte le competizioni di interesse nazionale, sia pubbliche che private, con rilevanza almeno regionale.



METRICA

65b

Cittadini coinvolti in iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica.



INDICATORE

65b

Numero di cittadini coinvolti in iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica, nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

65c

Cittadini appartenenti a particolari fasce della popolazione coinvolti in iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica.



INDICATORE

65c

Numero di cittadini appartenenti a particolari fasce della popolazione coinvolti in iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica, nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A

 **METRICA**

 **INDICATORE**

AFFIDABILITA'

65d

Cittadine coinvolte in iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica.

65d

Numero di cittadine coinvolte in iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica, nel periodo di riferimento.



Media

 **LINEE GUIDA PER LA MISURAZIONE**

N/A

 **METRICA**

 **INDICATORE**

AFFIDABILITA'

65e

Enti istituzionali (es. istituti di secondo grado, università) che hanno aderito ad iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica.

65e

Numero di enti istituzionali (es. istituti di secondo grado, università) che hanno aderito ad iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica, alla data di misurazione.



Alta

 **LINEE GUIDA PER LA MISURAZIONE**

N/A

Misura #66

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



Attori responsabili

MIMIT, MUR, MIM, DTD, MEF



Altri soggetti interessati

Min. Lavoro, Associazioni di categoria, Operatori privati, Atenei



Anno di implementazione

2024

 **METRICA**

 **INDICATORE**

AFFIDABILITA'

66a

Progetti di alternanza scuola-lavoro previsti in ambito cybersecurity.

66a

Numero di progetti di alternanza scuola-lavoro in ambito cybersecurity previsti nel periodo di riferimento.



Media

 **LINEE GUIDA PER LA MISURAZIONE**

La misura fa riferimento ai PCTO (Percorsi per le Competenze Trasversali e l'Orientamento) che dovranno essere conteggiati nel KPI.

 METRICA

66b
Fondi utilizzati per programmi di alternanza scuola-lavoro in ambito cybersecurity.

 INDICATORE

66b
Ammontare dei fondi utilizzati per programmi di alternanza scuola-lavoro in ambito cybersecurity, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere considerati tutti i tipi di fondi che finanziano i PCTO (sia fondi nazionali che fondi europei).

 METRICA

66c
Studenti coinvolti in programmi di alternanza scuola-lavoro in ambito cybersecurity.

 INDICATORE

66c
Numero di studenti coinvolti in programmi di alternanza scuola-lavoro in ambito cybersecurity, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

66d
Studenti, appartenenti a particolari categorie (ad es. donne, diversamente abili) coinvolti in programmi di alternanza scuola-lavoro in ambito cybersecurity.

 INDICATORE

66d
Numero di studenti, appartenenti a particolari categorie (ad es. donne, diversamente abili) coinvolti in programmi di alternanza scuola-lavoro in ambito cybersecurity, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

66e
Programmi di inserimento quali stage e apprendistato previsti in ambito cybersecurity.

 INDICATORE

66e
Numero di programmi di inserimento quali stage e apprendistato in ambito cybersecurity previsti nel periodo di riferimento.

AFFIDABILITA'


Media

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere compresi programmi di stage, programmi di apprendistato e qualunque programma assimilabile che dovesse essere normato in futuro.

 METRICA

66f
Fondi utilizzati per programmi di inserimento quali stage e apprendistato in ambito cybersecurity.

 INDICATORE

66f
Ammontare dei fondi utilizzati per programmi di inserimento quali stage e apprendistato in ambito cybersecurity nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

66g
Studenti e neolaureati coinvolti in programmi di inserimento quali stage e apprendistato in ambito cybersecurity.

 INDICATORE

66g
Numero di studenti e neolaureati coinvolti in programmi di inserimento quali stage e apprendistato in ambito cybersecurity, nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

66h
Studenti e neolaureati, appartenenti a particolari categorie (ad es. donne, diversamente abili) coinvolti in programmi di inserimento quali stage e apprendistato in ambito cybersecurity.

 INDICATORE

66h
Numero di studenti e neolaureati, appartenenti a particolari categorie (ad es. donne, diversamente abili) coinvolti in programmi di inserimento quali stage e apprendistato in ambito cybersecurity, nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

66i
Incentivi volti all'assunzione di personale "junior" con competenze in cybersecurity.

 INDICATORE

66i
Numero di incentivi volti all'assunzione di personale "junior" con competenze in cybersecurity previsti nel periodo di riferimento.

AFFIDABILITA'



Alta

 LINEE GUIDA PER LA MISURAZIONE

Per personale "junior" si intende personale la cui esperienza lavorativa in ambito cybersecurity non superi i 5 anni.

 METRICA

 INDICATORE

AFFIDABILITA'

66l
Fondi utilizzati per incentivare l'assunzione di personale "junior" con competenze in cybersecurity.

66l
Ammontare dei fondi utilizzati per incentivare l'assunzione di personale "junior" con competenze in cybersecurity, nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere considerati tutti i tipi di fondi (sia fondi nazionali che fondi europei) che finanziano l'assunzione di personale la cui esperienza lavorativa in ambito cybersecurity non superi i 5 anni.

 METRICA

 INDICATORE

AFFIDABILITA'

66m
Soggetti con competenze in cybersecurity assunti grazie a specifici incentivi relativi al personale "junior".

66m
Numero di soggetti con competenze in cybersecurity assunti grazie a specifici incentivi relativi al personale "junior", nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

66n
Soggetti con competenze in cybersecurity, appartenenti a particolari categorie (ad es. donne, diversamente abili) assunti grazie a specifici incentivi relativi al personale "junior".

66n
Numero di soggetti, appartenenti a particolari categorie (ad es. donne, diversamente abili) assunti grazie a specifici incentivi relativi al personale "junior", nel periodo di riferimento.


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

 INDICATORE

AFFIDABILITA'

66o
Iniziative volte alla riqualificazione e alla ricollocazione professionale.

66o
Numero di iniziative volte alla riqualificazione e alla ricollocazione professionale realizzate nel periodo di riferimento.


Media

 LINEE GUIDA PER LA MISURAZIONE

N/A



 METRICA

66p
Fondi utilizzati per Iniziative volte alla riqualificazione e alla ricollocazione professionale.

 INDICATORE

66p
Ammontare dei fondi utilizzati per Iniziative volte alla riqualificazione e alla ricollocazione professionale, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere considerati tutti i tipi di fondi che finanziano l'assunzione di personale (sia fondi nazionali che fondi europei).

 METRICA

66q
Soggetti coinvolti in iniziative di riqualificazione e ricollocazione.

 INDICATORE

66q
Numero di soggetti coinvolti in iniziative di riqualificazione e ricollocazione, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

66r
Soggetti, appartenenti a particolari categorie (ad es. donne, giovani, over 50, diversamente abili, disoccupati) coinvolti in iniziative di riqualificazione e ricollocazione.

 INDICATORE

66r
Numero di soggetti, appartenenti a particolari categorie (ad es. donne, giovani, over 50, diversamente abili, disoccupati) coinvolti in iniziative di riqualificazione e ricollocazione, nel periodo di riferimento.

AFFIDABILITA'


Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #67

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.



Attori responsabili

MUR, DTD, MAECI, CINI, Min. Difesa



Altri soggetti interessati

ACN, Associazioni di categoria, Operatori privati, Atenei



Anno di implementazione

2025

METRICA

67a
Programmi di scambio e iniziative similari, a livello europeo e internazionale, per attività di istruzione universitaria e in ambito professionale, che promuovano anche una sempre maggiore inclusione della popolazione femminile.

INDICATORE

67a
Numero di programmi di scambio e iniziative similari, a livello europeo e internazionale, per attività di istruzione universitaria e in ambito professionale, che promuovano anche una sempre maggiore inclusione della popolazione femminile, sviluppati nel periodo di riferimento.

AFFIDABILITA'



Media

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere compresi anche i programmi di scambio o iniziative similari relativi a dipendenti pubblici.

METRICA

67b
Soggetti coinvolti in programmi di scambio e iniziative similari, a livello europeo e internazionale, per attività di istruzione universitaria e in ambito professionale.

INDICATORE

67b
Numero di soggetti coinvolti in programmi di scambio e iniziative similari, a livello europeo e internazionale, per attività di istruzione universitaria e in ambito professionale nel periodo di riferimento.

AFFIDABILITA'



Media

LINEE GUIDA PER LA MISURAZIONE

N/A

METRICA

67c
Donne coinvolte in programmi di scambio e iniziative similari, a livello europeo e internazionale, per attività di istruzione universitaria e in ambito professionale.

INDICATORE

67c
Numero di donne coinvolte in programmi di scambio e iniziative similari, a livello europeo e internazionale, per attività di istruzione universitaria e in ambito professionale nel periodo di riferimento.

AFFIDABILITA'



Media

LINEE GUIDA PER LA MISURAZIONE

N/A



Misura #68

Favorire la formazione specialistica di tutte le figure impegnate nel contrasto alla criminalità informatica in ambito giudiziario e investigativo.



Attori responsabili

Min. Interno, Min. Giustizia



Altri soggetti interessati

Atenei, Min. Difesa



Anno di implementazione

2023



METRICA

68a

Iniziative di formazione specialistica per tutte le figure impegnate nel contrasto alla criminalità informatica in ambito giudiziario e investigativo.



INDICATORE

68a

Numero di iniziative di formazione specialistica per tutte le figure impegnate nel contrasto alla criminalità informatica in ambito giudiziario e investigativo, promosse nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere incluse tutte le attività, sia di natura progettuale che singole iniziative, con la finalità indicata nella misura. Per l'implementazione della misura 68, in aggiunta ai soggetti responsabili e interessati già indicati dal piano di implementazione, si ritiene necessario coinvolgere il MEF.



METRICA

68b

Addetti impegnati nel contrasto alla criminalità informatica in ambito giudiziario e investigativo coinvolti in iniziative di formazione specialistica.



INDICATORE

68b

Numero di addetti impegnati nel contrasto alla criminalità informatica in ambito giudiziario e investigativo coinvolti in iniziative di formazione specialistica, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #69

Potenziare la formazione del personale diplomatico così da rafforzare le capacità di cyber diplomacy.



Attori responsabili
ACN, MAECI



Altri soggetti interessati
Atenei



Anno di implementazione
2025



METRICA

69a

Iniziative di formazione del personale diplomatico volte a rafforzare le capacità di cyber diplomacy.



INDICATORE

69a

Numero di iniziative di formazione del personale diplomatico volte a rafforzare le capacità di cyber diplomacy, promosse nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere incluse tutte le attività, sia di natura progettuale che singole iniziative, con la finalità indicata nella misura.



METRICA

69b

Personale diplomatico che ha usufruito di formazione volta a rafforzare le capacità di cyber diplomacy.



INDICATORE

69b

Numero di personale diplomatico che ha usufruito di formazione volta a rafforzare le capacità di cyber diplomacy nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #70

Promuovere, per tutti i lavoratori pubblici e privati, inclusi quelli di livello apicale, il costante aggiornamento professionale, anche attraverso percorsi di formazione in materia di sicurezza cibernetica, pure nell’ottica di riqualificare la forza lavoro già in organico



Attori responsabili

MIMIT, DTD, ACN



Altri soggetti interessati

PCM, Min. Interno, Min. Difesa, Min. Lavoro, MPA, altre Amministrazioni, Associazioni di categoria



Anno di implementazione

2024



METRICA

70a

Iniziative per il costante aggiornamento professionale in ambito cybersecurity di lavoratori pubblici e privati, inclusi quelli di livello apicale.



INDICATORE

70a

Numero di iniziative per il costante aggiornamento professionale in ambito cybersecurity di lavoratori pubblici e privati, inclusi quelli di livello apicale, promosse nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

70b

Soggetti che hanno usufruito di iniziative per il costante aggiornamento professionale in ambito cybersecurity di lavoratori pubblici e privati, inclusi quelli di livello apicale.



INDICATORE

70b

Numero di soggetti che hanno usufruito di iniziative per il costante aggiornamento professionale in ambito cybersecurity di lavoratori pubblici e privati, inclusi quelli di livello apicale, nel periodo di riferimento.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



METRICA

70c

Soggetti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, diversamente abili) che hanno usufruito di iniziative per il costante aggiornamento professionale in ambito cybersecurity di lavoratori pubblici e privati, inclusi quelli di livello apicale.



INDICATORE

70c

Numero di soggetti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, diversamente abili) che hanno usufruito di iniziative per il costante aggiornamento professionale in ambito cybersecurity di lavoratori pubblici e privati, inclusi quelli di livello apicale, alla data di misurazione.

AFFIDABILITA'



Alta



LINEE GUIDA PER LA MISURAZIONE

N/A



2.4.2 Promozione della cultura della sicurezza cibernetica

Misura #71

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.



Attori responsabili

ACN, Min. Interno, MUR, DTD, PCM-DIE³



Altri soggetti interessati

Associazioni di categoria, Regioni e Province autonome, MPA, Min. Difesa



Anno di implementazione

2023

METRICA

71a
Iniziative e campagne di sensibilizzazione volte a promuovere le competenze degli utenti e i comportamenti responsabili nello spazio cibernetico.

INDICATORE

71a
Numero di iniziative e campagne di sensibilizzazione volte a promuovere le competenze degli utenti e i comportamenti responsabili nello spazio cibernetico in ambito cybersecurity condotte nel periodo di riferimento.

AFFIDABILITA'



Media

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere incluse tutte le attività, sia di natura progettuale che singole iniziative, con la finalità indicata nella misura.

METRICA

71b
Soggetti coinvolti in iniziative e campagne di sensibilizzazione volte a promuovere le competenze degli utenti e i comportamenti responsabili nello spazio cibernetico.

INDICATORE

71b
Numero di soggetti coinvolti in iniziative e campagne di sensibilizzazione volte a promuovere le competenze e i comportamenti responsabili nello spazio cibernetico degli utenti in ambito cybersecurity condotte nel periodo di riferimento.

AFFIDABILITA'



Alta

LINEE GUIDA PER LA MISURAZIONE

N/A

METRICA

71c
Soggetti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, disoccupati o inoccupati, anziani, diversamente abili) coinvolti in iniziative e campagne di sensibilizzazione volte a promuovere le competenze degli utenti e i comportamenti responsabili nello spazio cibernetico.

INDICATORE

71c
Numero di soggetti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, disoccupati o inoccupati, anziani, diversamente abili) coinvolti in iniziative e campagne di sensibilizzazione volte a promuovere le competenze degli utenti e i comportamenti responsabili nello spazio cibernetico in ambito cybersecurity condotte nel periodo di riferimento.

AFFIDABILITA'



Alta

LINEE GUIDA PER LA MISURAZIONE

N/A

³Dipartimento per l'Informazione e l'Editoria



Misura #72

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.



Attori responsabili
MIM, MUR, Atenei, ACN



Anno di implementazione
2024

METRICA

72a
Istituti che hanno sviluppato iniziative per la promozione dell'educazione digitale, comprensiva di aspetti di sicurezza cibernetica.

INDICATORE

72a
Numero di Istituti che hanno sviluppato iniziative per la promozione dell'educazione digitale, comprensiva di aspetti di sicurezza cibernetica, nel periodo di riferimento.

AFFIDABILITA'


Media

LINEE GUIDA PER LA MISURAZIONE

Per l'implementazione della misura 72, in aggiunta ai soggetti responsabili e interessati già indicati dal piano di implementazione, si ritiene necessario coinvolgere le Regioni e il Ministero del Lavoro.

METRICA

72b
Iniziativa volte a promuovere l'educazione digitale anche in raccordo con il mondo accademico, comprensive di aspetti di sicurezza cibernetica.

INDICATORE

72b
Numero di iniziative volte a promuovere l'educazione digitale anche in raccordo con il mondo accademico, comprensive di aspetti di sicurezza cibernetica, portate a termine nel periodo di riferimento.

AFFIDABILITA'


Media

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere incluse tutte le attività, sia di natura progettuale che singole iniziative, con la finalità indicata nella misura. Dovranno essere escluse iniziative ed attività cui non consegua il rilascio di un certificato o che non superino le 8 ore di durata.

METRICA

72c
Soggetti coinvolti in iniziative per la promozione dell'educazione digitale, comprensiva di aspetti di sicurezza cibernetica.

INDICATORE

72c
Numero di soggetti coinvolti in iniziative per la promozione dell'educazione digitale, comprensiva di aspetti di sicurezza cibernetica, nel periodo di riferimento.

AFFIDABILITA'


Media

LINEE GUIDA PER LA MISURAZIONE

N/A

 **METRICA**

 **INDICATORE**

AFFIDABILITA'

72d

Soggetti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, diversamente abili) coinvolti in iniziative per la promozione dell'educazione digitale, comprensive di aspetti di sicurezza cibernetica.

72d

Numero di soggetti appartenenti a particolari fasce della popolazione (ad es. donne, giovani, diversamente abili) coinvolti in iniziative per la promozione dell'educazione digitale, comprensive di aspetti di sicurezza cibernetica, nel periodo di riferimento.



Media

 **LINEE GUIDA PER LA MISURAZIONE**

N/A

 **METRICA**

 **INDICATORE**

AFFIDABILITA'

72e

Soggetti appartenenti a particolari fasce della popolazione (disoccupati o inoccupati) che nell'ambito dell'istruzione professionale sono coinvolti in iniziative per la promozione dell'educazione digitale, comprensive di aspetti di sicurezza cibernetica.

72e

Numero di soggetti appartenenti a particolari fasce della popolazione (disoccupati o inoccupati) che nell'ambito dell'istruzione professionale sono coinvolti in iniziative per la promozione dell'educazione digitale, comprensive di aspetti di sicurezza cibernetica, alla data di misurazione.



Media

 **LINEE GUIDA PER LA MISURAZIONE**

N/A

Misura #73

Predisporre e implementare un'autonoma strategia nazionale, con relativo piano d'azione, dedicata alla protezione online dei minori dai crimini informatici, che contempli iniziative come la realizzazione di campagne di sensibilizzazione indirizzate non solo ai minori, ma anche a genitori, tutori ed educatori.



Attori responsabili

Min. Interno, PCM



Altri soggetti interessati

ACN, MIM, Operatori privati, Atenei



Anno di implementazione

2023

 **METRICA**

 **INDICATORE**

AFFIDABILITA'

73a

Campagne di sensibilizzazione dedicate alla protezione online dei minori dai crimini informatici elaborate nell'ambito dell'autonoma strategia nazionale adottata.

73a

Numero di campagne di sensibilizzazione dedicate alla protezione online dei minori dai crimini informatici elaborate nell'ambito dell'autonoma strategia nazionale adottata e promosse nel periodo di riferimento.



Alta

 **LINEE GUIDA PER LA MISURAZIONE**

N/A



 METRICA

73b
Soggetti coinvolti in campagne di sensibilizzazione dedicate alla protezione online dei minori dai crimini informatici elaborate nell'ambito dell'autonoma strategia nazionale adottata.

 INDICATORE

73b
Numero di soggetti coinvolti in campagne di sensibilizzazione dedicate alla protezione online dei minori dai crimini informatici, elaborate nell'ambito dell'autonoma strategia nazionale e promosse nel periodo di riferimento.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

73c
Minori coinvolti in campagne di sensibilizzazione dedicate alla loro protezione online dai crimini informatici, elaborate nell'ambito dell'autonoma strategia nazionale adottata.

 INDICATORE

73c
Numero di minori coinvolti in campagne di sensibilizzazione dedicate alla loro protezione online dai crimini informatici, elaborate nell'ambito dell'autonoma strategia nazionale adottata e promosse nel periodo di riferimento.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

73d
Genitori/tutori coinvolti in campagne di sensibilizzazione dedicate alla protezione online dei minori dai crimini informatici, elaborate nell'ambito dell'autonoma strategia nazionale adottata.

 INDICATORE

73d
Numero di genitori/tutori coinvolti in campagne di sensibilizzazione dedicate alla protezione online dei minori dai crimini informatici, elaborate nell'ambito dell'autonoma strategia nazionale e promosse nel periodo di riferimento.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

N/A

 METRICA

73e
Educatori coinvolti in campagne di sensibilizzazione dedicate alla protezione online dei minori dai crimini informatici, elaborate nell'ambito dell'autonoma strategia nazionale adottata.

 INDICATORE

73e
Numero di educatori coinvolti in campagne di sensibilizzazione dedicate alla protezione online dei minori dai crimini informatici, elaborate nell'ambito dell'autonoma strategia nazionale e promosse nel periodo di riferimento.

AFFIDABILITA'



 LINEE GUIDA PER LA MISURAZIONE

N/A



2.4.3 Cooperazione

Misura #74

Istituire tavoli operativi permanenti con i soggetti Perimetro, suddivisi per settore, che svolgano a livello operativo specifici compiti in materia di prevenzione, allertamento, risposta agli incidenti e ripristino.



Attori responsabili

ACN



Altri soggetti interessati

Amministrazioni centrali, Regioni e Province autonome, Associazioni di categoria, Operatori privati



Anno di implementazione

2023

METRICA

74a
Tavoli operativi permanenti attivati con i soggetti Perimetro.

INDICATORE

74a
Numero di tavoli operativi permanenti attivati con i soggetti Perimetro nel periodo di riferimento.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

N/A

METRICA

74b
Incontri condotti nell'ambito dei tavoli operativi permanenti attivati con i soggetti Perimetro.

INDICATORE

74b
Numero di incontri condotti nell'ambito dei tavoli operativi permanenti attivati con i soggetti Perimetro nel periodo di riferimento.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #75

Rafforzare il ruolo dell'Italia all'interno dei consessi multilaterali impegnati in ambito di sicurezza cibernetica (quali Unione europea, NATO, G7, OSCE e Consiglio d'Europa) e il posizionamento strategico nazionale in Europa e nel mondo, promuovendo sinergie con i Paesi "like-minded".



Attori responsabili

MAECI, ACN, Min. Interno, Min. Giustizia, Min. Difesa, MIMIT



Anno di implementazione

2024

METRICA

75a
Politiche/atti normativi, sviluppati all'interno di consessi multilaterali, cui è stato apportato un concreto contributo redazionale.

INDICATORE

75a
Numero di politiche/atti normativi, sviluppati all'interno di consessi multilaterali, cui è stato apportato un concreto contributo redazionale nel periodo di riferimento.




AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

N/A









 METRICA	 INDICATORE	AFFIDABILITA'
75b Consessi/gruppi di lavoro a cui si è aderito e a cui sono state presentate fattive proposte di sviluppo.	75b Numero di consessi/gruppi di lavoro a cui si è aderito a cui sono state presentate fattive proposte di sviluppo alla data di misurazione.	 Media


 LINEE GUIDA PER LA MISURAZIONE

N/A




Misura #76
 Assicurare l'implementazione delle Confidence Building Measure (CBM) dell'OSCE in materia di sicurezza cibernetica.


-  **Attori responsabili**
MAECI, ACN
-  **Altri soggetti interessati**
Min. Difesa, altre Amministrazioni NCS, Operatori privati
-  **Anno di implementazione**
2024

 METRICA	 INDICATORE	AFFIDABILITA'
76a Iniziative sviluppate al fine di supportare l'implementazione delle Confidence Building Measure (CBM) dell'OSCE in materia di sicurezza cibernetica.	76a Numero di iniziative sviluppate al fine di supportare l'implementazione delle Confidence Building Measure (CBM) dell'OSCE in materia di sicurezza cibernetica, nel periodo di riferimento.	 Alta

 LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere incluse tutte le attività, sia di natura progettuale che singole iniziative, con la finalità indicata nella misura.

 METRICA	 INDICATORE	AFFIDABILITA'
76b CBM implementate a livello nazionale.	76b Numero di CBM implementate a livello nazionale rispetto al numero complessivo delle CBM alla data di misurazione.	 Alta

 LINEE GUIDA PER LA MISURAZIONE

N/A



Misura #77

Rafforzare la cooperazione con altri Paesi, per contribuire alla stabilità e alla sicurezza dello spazio cibernetico.



Attori responsabili

MAECI, ACN, Min. Difesa



Anno di implementazione

2025

METRICA

INDICATORE

AFFIDABILITA'

77a

Iniziative di cooperazione con altri Paesi, per contribuire alla stabilità e alla sicurezza dello spazio cibernetico.

77a

Numero di iniziative di cooperazione con altri Paesi, per contribuire alla stabilità e alla sicurezza dello spazio cibernetico, sviluppate nel periodo di riferimento.



Media

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo dovranno essere ricomprese sia le iniziative di collaborazione formali che le iniziative di collaborazione informali avviate al fine di dare seguito alla misura.

Verranno escluse dal calcolo le attività di Capacity Building che dovranno essere conteggiate in relazione alla misura #79.

Per l'implementazione della misura 77, in aggiunta ai soggetti responsabili e interessati già indicati dal piano di implementazione, si ritiene necessario coinvolgere il Ministero dell'Interno e il Ministero delle Finanze.

Misura #78

Realizzare un ecosistema nazionale volto a sviluppare capacità di capacity building a favore di Paesi terzi.



Attori responsabili

ACN, MAECI



Altri soggetti interessati

Altre Amministrazioni NCS



Anno di implementazione

2023

METRICA

INDICATORE

AFFIDABILITA'

78a

Iniziative volte alla realizzazione di un ecosistema nazionale.

78a

Numero di iniziative volte alla realizzazione di un ecosistema nazionale attuate, nel periodo di riferimento.



Media

LINEE GUIDA PER LA MISURAZIONE

Nel calcolo devono essere incluse tutte le attività, sia di natura progettuale che singole iniziative, con la finalità indicata nella misura.

Misura #79

Stipulare accordi bilaterali e multilaterali con i Paesi di interesse strategico, prevedendo anche lo sviluppo di attività di capacity building.



Attori responsabili

MAECI, ACN, Min. Interno, Min. Giustizia, Min. Difesa



Altri soggetti interessati

Altre Amministrazioni NCS



Anno di implementazione

2023

METRICA

INDICATORE

AFFIDABILITA'

79a

Individuazione dei Paesi terzi classificabili come prioritari con i quali stipulare accordi bilaterali e multilaterali e/o a cui rivolgere attività di cyber capacity building.

79a

Numero di Paesi terzi individuati come prioritari.



Media

LINEE GUIDA PER LA MISURAZIONE

Per Paesi terzi individuati come prioritari si intendono Paesi con i quali si intende avviare uno scambio informativo volto al mutuo rafforzamento delle capacità di risposta alle minacce e agli attacchi di natura cyber.

METRICA

INDICATORE

AFFIDABILITA'

79b

Accordi bilaterali e multilaterali stipulati con Paesi terzi individuati come prioritari.

79b

Numero di accordi bilaterali e multilaterali stipulati con i Paesi terzi individuati come prioritari.



Media

LINEE GUIDA PER LA MISURAZIONE

Per Paesi terzi individuati come prioritari si intendono Paesi con i quali si intende avviare uno scambio informativo volto al mutuo rafforzamento delle capacità di risposta alle minacce e agli attacchi di natura cyber.

METRICA

INDICATORE

AFFIDABILITA'

79c

Attività di cyber capacity building rivolte ai Paesi terzi individuati come prioritari.

79c

Numero di attività di cyber capacity building rivolte ai Paesi terzi individuati come prioritari.



Media

LINEE GUIDA PER LA MISURAZIONE

Per Paesi terzi individuati come prioritari si intendono i Paesi ai quali si intende proporre attività di sviluppo di capacità cyber e che possono rappresentare un mercato di sbocco per i nostri servizi e prodotti.

Misura #80

Contribuire attivamente, in ambito di Unione europea, alla definizione di policy/regolamentazioni in materia di cybersicurezza.



Attori responsabili

ACN



Altri soggetti interessati

MAECI, DTD, MIMIT



Anno di implementazione

2023



METRICA

80a

Policy/regolamentazioni in materia di cybersicurezza, in ambito UE, cui si è attivamente contribuito.



INDICATORE

80a

Numero di policy/regolamentazioni in materia di cybersicurezza, in ambito UE, cui si è attivamente contribuito alla data di misurazione.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

N/A

Misura #81

Contribuire attivamente, in ambito di Unione europea, all'individuazione delle priorità di ricerca e sviluppo per traggardare l'obiettivo dell'autonomia tecnologica UE in ambito digitale.



Attori responsabili

ACN, DTD, MIMIT



Altri soggetti interessati

MAECI, Min. Difesa (ricerca militare)



Anno di implementazione

2025



METRICA

81a

Iniziativa sviluppate, in ambito di Unione europea, per definire priorità di ricerca e sviluppo e per traggardare l'obiettivo dell'autonomia tecnologica UE in ambito digitale.



INDICATORE

81a

Numero di iniziative sviluppate, in ambito di Unione europea, per definire priorità di ricerca e sviluppo e per traggardare l'obiettivo dell'autonomia tecnologica UE in ambito digitale, nel periodo di riferimento.

AFFIDABILITA'



Media



LINEE GUIDA PER LA MISURAZIONE

L'ambito dell'Unione europea al quale fa riferimento la misura e il relativo indicatore è quello del Governing Board del Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca (ECCC).

2.4.4 Metriche e Key Performance Indicators

Misura #82

Sviluppare, entro 12 mesi dall'adozione della presente strategia, apposite metriche e key performance indicator (KPI) per misurare:

- il livello di implementazione della presente strategia
 - il livello di maturità nel settore della cybersecurity dei diversi OSE/FSD
 - la partecipazione di particolari fasce della popolazione (ad es. donne, giovani e disoccupati o inoccupati) in attività di sensibilizzazione, istruzione e formazione nel campo della sicurezza informatica, e la loro efficacia
- la partecipazione di particolari fasce della popolazione (ad es. donne e giovani) nell'industria della sicurezza informatica iniziative e relativi investimenti, anche da parte dell'industria nazionale, in attività di ricerca e sviluppo nel campo della sicurezza informatica
- il totale degli investimenti in sicurezza informatica da parte di soggetti pubblici e privati
 - il totale delle imprese nazionali coperte da polizza assicurativa contro gli incidenti informatici



Attori responsabili

ACN, altri attori responsabili dell'implementazione della strategia



Altri soggetti interessati

ISTAT, Associazioni di categoria, Operatori privati, Atenei



Anno di implementazione

2023

METRICHE

82a
Metriche e KPI sviluppati per misurare l'attuazione della strategia nazionale di cybersicurezza.

INDICATORE

82a
Numero di metriche e KPI sviluppati per misurare l'attuazione della strategia nazionale di cybersicurezza, definiti alla data di misurazione.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

N/A

METRICHE

82b
Metriche e KPI rendicontati in merito all'attuazione della strategia nazionale di cybersicurezza.

INDICATORE

82b
Numero di metriche e KPI rendicontati in merito all'attuazione della strategia nazionale di cybersicurezza, nel periodo di riferimento.

AFFIDABILITA'



LINEE GUIDA PER LA MISURAZIONE

N/A

