La nuova architettura nazionale di cybersicurezza

9 marzo 2023

CONTESTO DELLA RIFORMA

CISR

CISR Tecnico

CIC

PCM

MIMIT

DIS

AGENZIA PER LA CYBERSICUREZZA NAZIONALE — ACN — SAPIENTIA ADIUVAT

Autorità competenti NIS

AGID

Decreto-legge 14 giugno 2021, n. 82

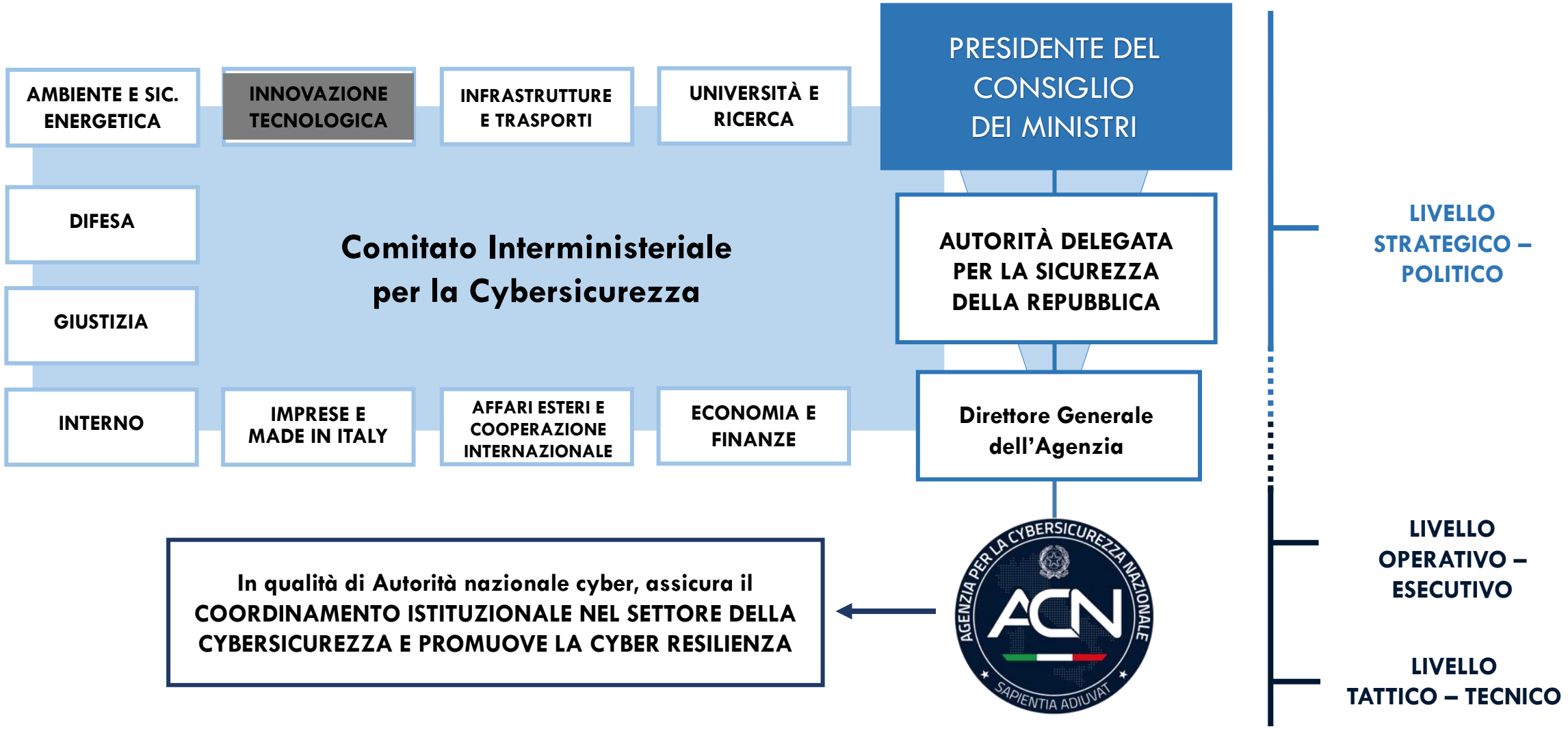
Autorità co… …ber > 20

Riordino

Razionalizzazione

Approccio olistico

QUADRO DI GOVERNANCE (1/2)



QUADRO DI GOVERNANCE (2/2)

LIVELLO INTERNAZIONALE MULTILATERALE (1/2)

Consiglio dell'UE

Horizontal Working Group on Cyber Issues

Commissione UE

ENISA

European Union Agency for Cybersecurity

ECCC

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca

Nazioni Unite

Open-ended working group on security of and in the use of ICT

NATO

G7

OSCE

Informal Working Group (Confidence Building Measures)

LIVELLO INTERNAZIONALE MULTILATERALE (2/2)

Commissione UE

DG CONNECT-Reti di comunicazione, dei contenuti e delle tecnologie

- elabora e attua politiche in ambito digitale e promuove un mercato interno che favorisca lo sviluppo di nuove tecnologie
- tramite finanziamenti, norme e iniziative politiche, contribuisce a garantire la leadership e l'indipendenza dell'UE nell'ambito delle tecnologie digitali critiche
- Strategia europea di cibersicurezza

ENISA

European Union Agency for Cybersecurity

- supporta istituzioni UE e Stati membri nell'elaborazione e attuazione di politiche, nello sviluppo di capacità e nella revisione normativa
- promuove l'uso della certificazione europea di cibersicurezza
- promuove la cooperazione e lo sviluppo della consapevolezza cyber

Consiglio dell'UE

Horizontal Working Party on Cyber Issues (HWPCI)

- coordina i lavori del Consiglio sulle questioni relative alla cibersicurezza, in particolare la politica e le attività legislative in materia
- garantisce una piattaforma di lavoro orizzontale per l'armonizzazione e l'approccio unificato
- facilita lo scambio di informazioni tra i paesi dell'UE
- definisce le priorità e gli obiettivi strategici dell'UE

Gruppi settoriali tematici (es. NISCG, ECCG, CSIRT Network, CyCLONe)

L'Agenzia per la cybersicurezza nazionale

L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE

- È istituita a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, proteggendo dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche e assicurandone la sicurezza e la resilienza.
- L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria.
- Il Presidente del Consiglio dei ministri e l'Autorità delegata si avvalgono dell'Agenzia per l'esercizio delle competenze in materia di cybersicurezza.

L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE. QUADRO NORMATIVO DI RIFERIMENTO

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 162° - Numero 140

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

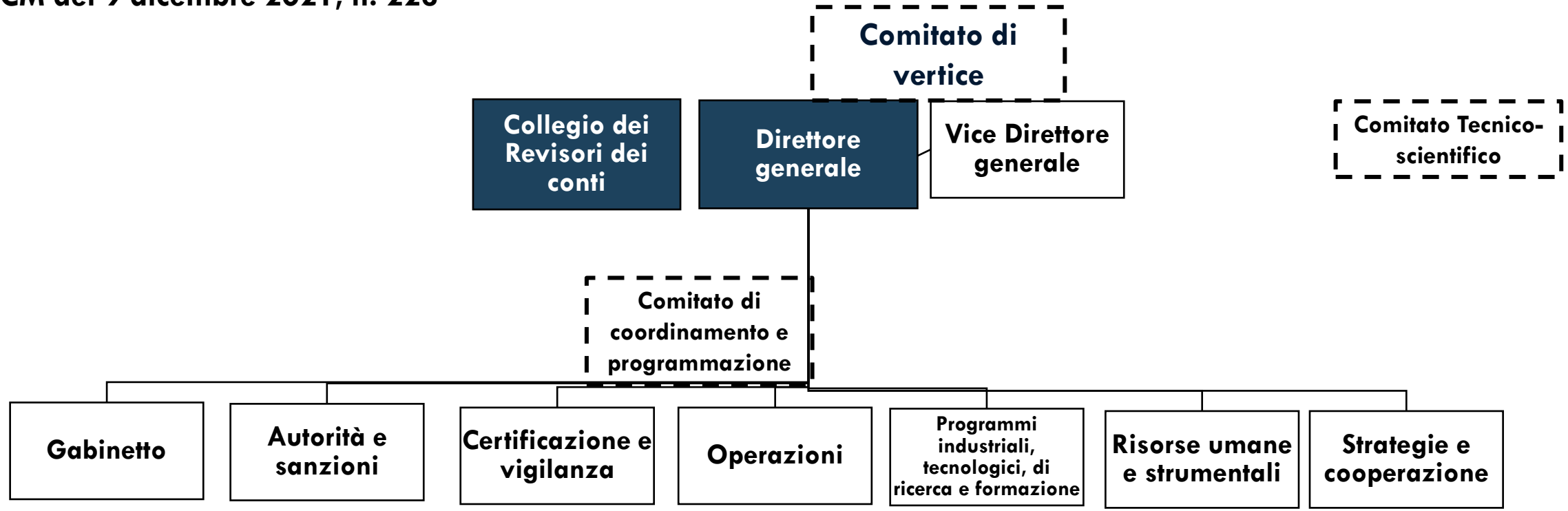
PARTE PRIMA — Roma - Lunedì, 14 giugno 2021 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

CONTABILITÀ (art. 11, c. 3)	**ORGANIZZAZIONE E FUNZIONAMENTO** (art. 6)	**PERSONALE** (art. 12)	**APPALTI IN DEROGA** (art. 11, c. 4)
DPCM, di concerto con MEF, previo parere COPASIR, sentito il CIC	DPCM, di concerto con MEF, previo parere Commissioni parlamentari competenti e COPASIR, sentito il CIC	DPCM, previo parere Commissioni parlamentari competenti e COPASIR, sentito il CIC	DPCM, previo parere COPASIR e sentito il CIC
1 **9 DICEMBRE 2021**	2 **9 DICEMBRE 2021**	3 **9 DICEMBRE 2021**	4 **1 SETTEMBRE 2022**

STRUTTURAZIONE DELL'AGENZIA. REGOLAMENTO DI ORGANIZZAZIONE E FUNZIONAMENTO

L'organizzazione e il funzionamento dell'Agenzia sono definiti da un apposito regolamento che ne prevede, in particolare, l'articolazione in uffici di livello dirigenziale generale, nonché in articolazioni di livello dirigenziale non generale.
Sono organi dell'Agenzia il Direttore generale e il Collegio dei revisori dei conti.
Con il regolamento sono disciplinati altresì:
a) le funzioni del Direttore generale e del Vice Direttore generale dell'Agenzia;
b) la composizione e il funzionamento del Collegio dei revisori dei conti;
c) l'istituzione di eventuali sedi secondarie. (art. 6 del d.l. n. 82/2021)

DPCM del 9 dicembre 2021, n. 223



AGENZIA PER LA CYBERSICUREZZA NAZIONALE. FUNZIONI ISTITUZIONALI

AUTORITÀ NAZIONALE DI CYBERSICUREZZA

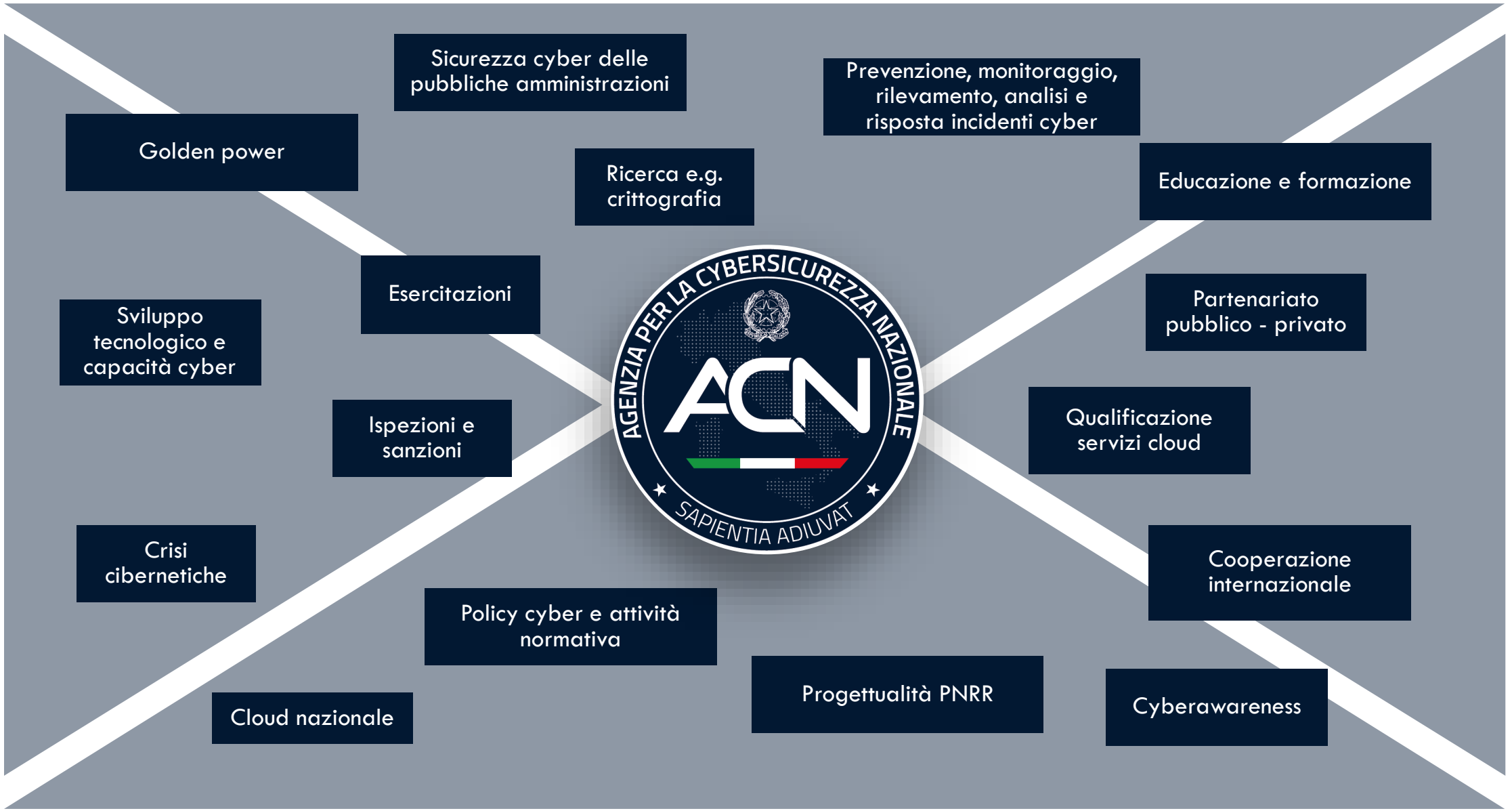
FUNZIONI

- COORDINAMENTO DEI SOGGETTI PUBBLICI COINVOLTI NELLA CYBERSICUREZZA
- AUTORITÀ NAZIONALE COMPETENTE E PUNTO DI CONTATTO UNICO NIS
- CSIRT ITALIA COMPUTER SECURITY INCIDENT RESPONSE TEAM
- SUPERVISIONE DELL'ATTUAZIONE DELLA LEGGE SUL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA
- CVCN
- AUTORITÀ NAZIONALE DI CERTIFICAZIONE DELLA CYBERSICUREZZA
- AUTORITÀ COMPETENTE PER LA SICUREZZA DELLE COMUNICAZIONI ELETTRONICHE
- CENTRO DI COORDINAMENTO NAZIONALE – PoC ECCC

L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE. FUNZIONI

PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA	AUTORITÀ NAZIONALE COMPETENTE E POC NIS	SICUREZZA DELLE COMUNICAZIONI ELETTRONICHE	AUTORITÀ NAZIONALE DI CERTIFICAZIONE DELLA CYBERSICUREZZA	NCC - CENTRO EUROPEO DI COMPETENZA PER LA CYBERSECURITY
• Notifica inserimento elenco soggetti • Elenchi beni ICT • Notifiche di incidenti • Misure di sicurezza • Scrutinio tecnologico con il CVCN • Accreditamento CV e LAP • Ispezioni e sanzioni • Supporto al Presidente del Consiglio nel coordinamento dell'attuazione della normativa perimetro • Tavolo perimetro	• PoC NIS • NIS Cooperation Group • Elenco OSE • Definizione eventuali misure di sicurezza per OSE • Ispezioni e sanzioni • Comitato tecnico di raccordo	• Definizione misure di sicurezza (tecniche e organizzative) per reti pubbliche e servizi di comunicazione elettronica accessibili al pubblico • Definizione soglie di significatività incidenti • Notifiche di incidenti • Relazione ad ENISA • Ispezioni	• Certificazione di sicurezza cibernetica • Autorizza gli organismi di valutazione della conformità • Supervisione e controllo • Ispezioni • ECCG	• Membri del Consiglio di direzione ECCC • PoC nazionale – Centro di competenza nazionale • Ricerca, innovazione, sviluppo di capacità, infrastrutture e competenze di cybersicurezza • Azioni specifiche con i fondi concessi dal Centro di competenza UE

AUTORITÀ NAZIONALE DI CYBERSICUREZZA



Resilienza **Sicurezza nazionale** **Autonomia strategica**

NUCLEO PER LA CYBERSICUREZZA

ORDINARIO

PRESIEDUTO DA:
- DG o, per delega, VDG dell'ACN

COMPOSTO DA:
- Consigliere militare del Presidente del Consiglio dei ministri
- DIS, AISE, AISI
- Ministeri CIC
- Dipartimento della Protezione Civile

SE NECESSARIO, RAPPRESENTANTI DI:
- Altre amministrazioni, università, enti e istituzioni di ricerca, operatori privati.
- UCSe, per il trattamento di informazioni classificate

RISTRETTO

Rappresentanti delle sole amministrazioni e soggetti interessati, tanto in conduzione ordinaria che relativamente ai compiti di gestione delle crisi

CRISI

COMPOSIZIONE INTEGRATA CON:
- Ministero della Salute
- Dip. VV. FF., Soccorso Pubblico e Difesa Civile

SE NECESSARIO, RAPPRESENTANTI DI:
- Amministrazioni locali ed enti
- Altri soggetti pubblici o privati interessati

1. Formula proposte di iniziative in materia di cybersicurezza, anche nel quadro del contesto internazionale
2. Promuove la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica e l'elaborazione delle procedure di coordinamento interministeriale
3. Promuove e coordina lo svolgimento esercitazioni interministeriali - o la partecipazione italiana ad esercitazioni internazionali - di simulazione di eventi di natura cibernetica.
4. Valuta se le violazioni o gli incidenti assumano dimensioni, intensità o natura tali da richiedere l'assunzione di decisioni coordinate in sede interministeriale
5. Acquisisce, anche per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi
6. Riceve dal CSIRT Italia le notifiche di incidente
7. Valuta e promuove procedure di condivisione delle informazioni anche con operatori privati ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi.
8. Coordinamento della gestione delle crisi che coinvolgono aspetti di cybersicurezza

LA PRINCIPALE NORMATIVA NAZIONALE ED EUROPEA IN MATERIA

decreto legislativo n. 65/2018 - Attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. normativa NIS)

Regolamento (UE) 2019/881 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (c.d. Cybersecurity Act) e d. lgs. n. 123/2022 di adeguamento

decreto-legge n. 105/2019 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e decreti di attuazione (c.d. normativa perimetro)

Regolamento (UE) 2021/887 che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento

decreto-legge 14 giugno 2021, n. 82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale

decreto legislativo 8 novembre 2021, n. 207, di Attuazione della direttiva (UE) 2018/1972, che istituisce il Codice europeo delle comunicazioni elettroniche

decreto-legge 21 marzo 2022, n. 21, recante, tra le varie, disposizioni sulla ridefinizione dei poteri speciali in materia di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, nonché di ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica

Regolamento (UE) 2022/2554 e **Direttiva (UE) 2022/2556** relativi alla resilienza operativa digitale per il settore finanziario

Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (c.d NIS 2)

La Strategia nazionale di cybersicurezza 2022-2026

STRATEGIA NAZIONALE DI CYBERSICUREZZA

In qualità di Autorità nazionale per la cybersicurezza, l'ACN cura la predisposizione della **Strategia nazionale di cybersicurezza**, la cui adozione è attribuita, in via esclusiva, al Presidente del Consiglio dei ministri.

Il 17 maggio 2022 è stata adottata la Strategia nazionale di cybersicurezza 2022-26, i cui obiettivi strategici sono suddivisi in **82 misure** da implementare entro il 2026.

Gli obiettivi sono **raggruppati per aree tematiche** e organizzati al fine di assicurare la **concreta attuazione della strategia,** sia dal punto di vista organizzativo e di *policy* che prettamente operativo.

STRUTTURA DEL PIANO DI IMPLEMENTAZIONE

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

Altri soggetti interessati
PCM, Min. Difesa, Min. Interno, Regioni e Province autonome

Attori che hanno la **responsabilità** di condurre l'intervento

Attori che **contribuiscono** all'intervento

KPI per ogni misura da definire dagli attori responsabili

Strategia
Nazionale di Cybersicurezza

Governance nazionale

MANUALE OPERATIVO

- Si tratta della **versione operativa del Piano di implementazione** della Strategia Nazionale di Cybersicurezza 2022-2026
- Lo 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**
- L'impianto degli indicatori, unitamente ai **target** specifici definiti per ciascuno di essi, espressi in termini numerici, consentirà di calcolare, il **grado di attuazione delle misure**, attraverso **KPI** espressi in termini percentuali
- Il Manuale intende costituire un ***"living document"***, soggetto a periodici aggiornamenti e revisioni, mano a mano che le misure saranno implementate

FOCUS SULLE MISURE: POTENZIAMENTO DELLE CAPACITÀ CYBER DELLA P.A.

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
MITD, MPA

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
MITD

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
MITD, ACN

FOCUS SULLE MISURE: 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

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

FOCUS SULLE MISURE: IMPULSO ALL'INNOVAZIONE TECNOLOGICA E ALLA DIGITALIZZAZIONE

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, MITD, MiSE, MUR, Min. Difesa

Altri soggetti interessati
Atenei, Ricerca, Regioni e Province autonome

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, MITD, MEF, MiSE, MUR, Min. Difesa

Altri soggetti interessati
Operatori privati, Atenei, Ricerca

FOCUS SULLE MISURE: 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
Min. Istruzione, MUR, Atenei, ACN, Min. Difesa (alta formazione)

Altri soggetti interessati
PCM, Min. Difesa, Min. Interno, Regioni e Province autonome

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
Min. Istruzione, MUR, Atenei, ACN

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

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, Ministero dell'Istruzione, MUR

Altri soggetti interessati
Operatori privati, Regioni e Province autonome

FOCUS SULLE MISURE: 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, MITD, PCM

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

Recenti evoluzioni che rafforzano la cybersicurezza del Paese

1) NORMATIVA EUROPEA DI RECENTE ADOZIONE (27.12.2022)

NIS2

Direttiva NIS2, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione

Revisionato meccanismo di identificazione dei soggetti per mezzo di un criterio omogeneo basato sulla dimensione (cd. *Size-cap rule*). **Estesa l'applicazione della direttiva** a tutte le medie e grandi imprese che operano nei settori identificati, oltre che **alla Pubblica Amministrazione**

RECEPIMENTO

- **massimo coordinamento**
- **maggiore chiarezza agli operatori**
- **evitare eccessivo aumento degli oneri**

NOVITÀ RISPETTO ALLA DIRETTIVA NIS

Revisione del meccanismo di identificazione dei soggetti

- Criterio, salvo eccezioni, omogeneo di identificazione (cd. size cap rule)
- Superamento della dicotomia OSE/FSD
- Introduzione del concetto di soggetti essenziali e importanti

Allargamento dell'ambito di applicazione

- Aumento significativo dei settori di applicazione

Rafforzamento dei poteri di supervisione

- Indicazioni più dettagliate per la definizione delle misure di sicurezza
- Inasprimento delle sanzioni
- Maggiori funzioni allo CSIRT nazionale (e.g. Coordinated Vulnerability Disclosure)

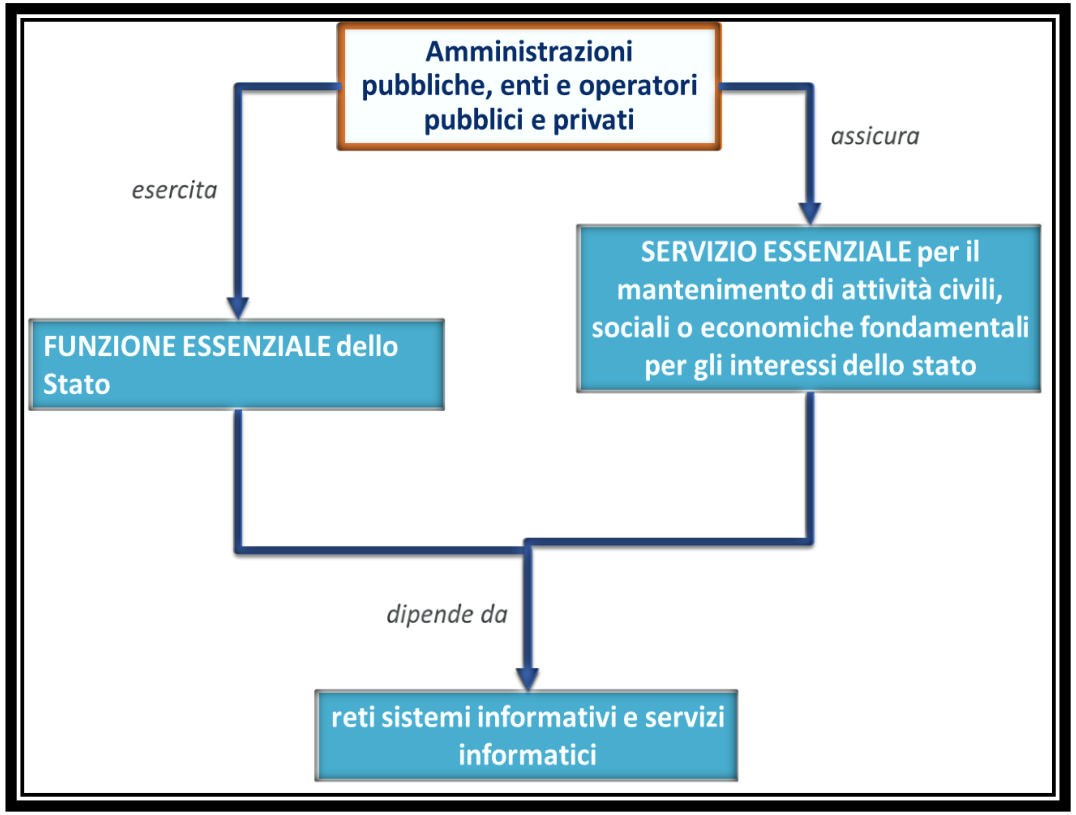
Gestione delle crisi cyber

- Previsione di un quadro nazionale in materia
- Istituzionalizzazione del Cyber Crises Liaison Organisation Network (CyCLONe)

2) IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

«*Al fine di assicurare un* ***livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici*** *delle* ***amministrazioni pubbliche, degli enti e degli operatori pubblici e privati*** *aventi una sede nel territorio nazionale,* ***da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale*** *per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e* ***dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale,*** *è istituito il perimetro di sicurezza nazionale cibernetica*»

Decreto-legge n. 105/2019, art. 1, comma 1



IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

A CHI SI APPLICA →

Amministrazioni pubbliche, enti e operatori pubblici e privati aventi sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o l'erogazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche.

A COSA SI APPLICA →

ASSET ICT: reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.

CHE COSA COMPORTA →

- Misure di sicurezza
- Notifica incidenti
- Screening tecnologico su determinate categorie di *procurement* destinate agli asset ICT Perimetro (CVCN)
- Ispezioni, verifiche e sanzioni

IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA. I SETTORI.

Settori	Amministrazione competente
Governativo	Amministrazioni CIC
Interno	Ministero dell'interno
Difesa	Ministero della difesa
Spazio e aerospazio	PCM – UCM
Energia	Ministero dell'ambiente e della sicurezza energetica
Telecomunicazioni	Ministero delle imprese e del Made in Italy
Economia e finanze	Ministero dell'economia e delle finanze
Trasporti	Ministero delle infrastrutture e dei trasporti
Servizi digitali	Ministero delle imprese e del Made in Italy PCM – DTD
Tecnologiche critiche	PCM – DTD Ministero delle imprese e del Made in Italy Ministero dell'università e della ricerca
Enti previdenziali e lavoro	Ministero del lavoro e delle politiche sociali

IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA. FUNZIONE E SERVIZIO ESSENZIALE.

FUNZIONE ESSENZIALE DELLO STATO	SERVIZIO ESSENZIALE
un soggetto esercita una funzione essenziale dello Stato, di seguito funzione essenziale, laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti.	*un soggetto, pubblico o privato, presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, di seguito servizio essenziale, laddove ponga in essere: attività strumentali all'esercizio di funzioni essenziali dello Stato; attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.*

Art. 2 del DPCM n. 131/2020

IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA. INDIVIDUAZIONE SOGGETTI E BENI ICT

PROCEDIMENTO: Amministrazioni PSNC identificano soggetti individuabili → Tavolo Perimetro → Proposta CIC → Atto amministrativo del Presidente del Consiglio dei ministri con elenco soggetti PSNC

ACN comunica al soggetto l'inserimento nel PSNC per specifici funzioni o servizi essenziali

Entro 6 mesi, **il soggetto perimetro:**

- Svolge analisi del rischio/impatto per ogni funzione/servizio essenziale
- Individua i beni ICT necessari a svolgere la funzione/servizio, valutando l'impatto di un incidente sul bene ICT ai fini dello svolgimento della funzione/servizio e le dipendenze con altre reti, sistemi informativi, servizi informatici
- Predispone l'elenco dei beni ICT da inserire nel perimetro, descrivendone la relativa componentistica e architettura
- Comunica l'elenco all'ACN

Bene ICT

- per **bene ICT** si intende un insieme di reti, sistemi informativi e servizi informatici, o parti di essi, di qualunque natura, considerato unitariamente ai fini dello svolgimento di funzioni essenziali dello Stato o per l'erogazione di servizi essenziali.

Gradualità nell'individuazione beni ICT

- in fase di **prima applicazione** sono individuati i beni ICT che, in caso di incidente, causerebbero l'**interruzione totale** dello svolgimento della funzione essenziale o del servizio essenziale o una **compromissione** degli stessi con **effetti irreversibili** sotto il profilo dell'integrità o della riservatezza dei dati e delle informazioni.

IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

A CHI SI APPLICA → Amministrazioni pubbliche, enti e operatori pubblici e privati aventi sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o l'erogazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche.

A COSA SI APPLICA → **ASSET ICT**: reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.

CHE COSA COMPORTA →

- Misure di sicurezza
- Notifica incidenti
- Screening tecnologico su determinate categorie di *procurement* destinate agli asset ICT Perimetro (CVCN)
- Ispezioni, verifiche e sanzioni

LA NOTIFICA DI INCIDENTI CON IMPATTO SU BENI ICT INSERITI NEL PSNC

TERMINE

- **Entro 1 ora**, nei casi più gravi di incidente
- **Entro 6 ore**, nei casi meno gravi di incidente

DECORRENZA

Dal momento in cui i Soggetti perimetro **ne vengono a conoscenza**

MODALITÀ

Portale CSIRT Italia

EVOLUZIONE NORMATIVA

ART. 37-QUATER, CO. 1, DL 115/2022 (DL AIUTI BIS)

INSERISCE

ART. 1, CO. 3-BIS, DL 105/2019

Obbligatorietà di notifica *anche* degli incidenti che impattano su reti, sistemi informativi e servizi informatici diversi dai beni ICT conferiti al Perimetro*.

DÀ ATTUAZIONE

DETERMINA DG ACN DEL 03.01.2023

Tassonomia degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici diversi dai beni ICT conferiti al Perimetro.

RAZIONALE

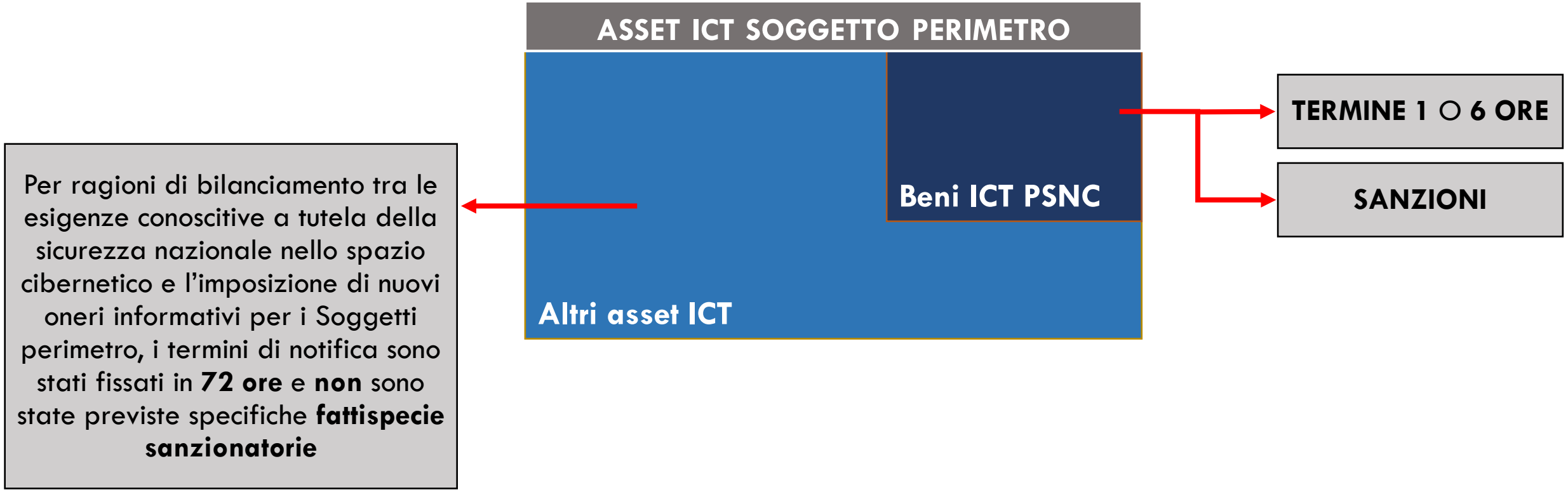
→ miglioramento capacità di prevenzione degli incidenti

→ valutare in anticipo eventuali attacchi sistemici e possibili spillover su asset conferiti al Perimetro dal soggetto.

** eccezione Ministero della Difesa*

NOTIFICA DI INCIDENTI SU RETI, SISTEMI INFORMATIVI E SERVIZI INFORMATICI NO PSNC

(ART. 1, co. 3-BIS, DL PERIMETRO)



DETERMINA DIRETTORE GENERALE ACN 3 GENNAIO 2023

TASSONOMIA INCIDENTI AVENTI IMPATTO SU RETI, SISTEMI INFORMATIVI E SERVIZI INFORMATICI NO PSNC

NOTIFICA

- **Obbligatoria, entro 72 ore:** All. A, Sezione 1 (accesso iniziale, esecuzione, installazione, movimenti laterali, azioni sugli obiettivi)
- **Volontarie:** All. A, Sezione 2 (ricognizione riferita ad attività di *spearphishing)*

DECORRENZA

Dal momento in cui i Soggetti PSNC **ne vengono a conoscenza**

MODALITÀ

Portale CSIRT Italia

IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA. NORMATIVA

Decreto legge n. 105/2019 → 5 provvedimenti attuativi

1. **DPCM n. 131/2020** che definisce i settori ai quali si applica la normativa perimetro, le nozioni di funzione e servizio essenziale, i criteri per l'individuazione dei soggetti perimetro e il procedimento per l'individuazione e la comunicazione dei beni ICT inclusi nello stesso

2. **DPCM n. 81/2021** che definisce le misure volte a garantire la sicurezza dei beni ICT inclusi nel perimetro e le modalità di notifica degli incidenti

3. **DPR n. 54/2021** relativo all'esecuzione di attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel d.l. 105/2019 e decreti attuativi; ispezioni e modalità di scrutinio tecnologico da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e dei Centri di Valutazione (CV) del Ministero dell'Interno e del Ministero della Difesa; criteri di natura tecnica per l'individuazione delle categorie di beni, sistemi e servizi ICT a cui si applica la procedura di valutazione

4. **DPCM 15 giugno 2021** che individua le categorie di prodotti ICT sottoposti alle valutazioni del CVCN e dei CV in fase di procurement da parte dei soggetti perimetro

5. **DPCM n. 92/2022** riguardante le modalità di accreditamento dei CV e dei Laboratori Accreditati di Prova (LAP), nonché relativo al coordinamento tra CVCN, CV e LAP

Agenzia per la Cybersicurezza Nazionale

GRAZIE!

https://www.acn.gov.it
info@acn.gov.it