PIANO DI IMPLEMENTAZIONE

STRATEGIA NAZIONALE DI CYBERSICUREZZA

2022 – 2026

Sommario

Premessa

L'efficacia di una strategia è strettamente correlata alla possibilità di misurare i risultati progressivamente raggiunti, anche al fine di poter assumere in corso d'opera gli opportuni correttivi o integrazioni, laddove necessari. Proprio per tale motivo, il legislatore ha assegnato al Presidente del Consiglio il potere di adottare, sentito il Comitato Interministeriale per la Cybersicurezza (CIC), mirate linee di indirizzo.

In quest'ottica, gli attori pubblici a cui è attribuita la messa in opera delle misure di implementazione, entro il 31 dicembre di ogni anno, comunicano gli esiti delle azioni condotte all'ACN, per riferire al CIC sullo stato di attuazione della strategia. Quest'ultimo, infatti, esercita l'alta sorveglianza sulla sua implementazione.

Il Comparto intelligence fornisce all'ACN un quadro informativo e valutativo utile a orientare il potenziamento delle misure atte a garantire la corretta implementazione del presente piano, riferendo per le misure di cui è responsabile, secondo le procedure definite dalla Legge n. 124/2007.

Un aggiornamento sui risultati conseguiti viene fornito al Parlamento e alla cittadinanza, attraverso la relazione che il Presidente del Consiglio dei Ministri è tenuto a trasmettere, entro il 30 aprile di ogni anno, sull'attività svolta dall'Agenzia nell'anno precedente in materia di cybersicurezza nazionale.

#1

Piano di implementazione delle misure

Piano di implementazione delle misure

Il presente piano di implementazione – che non incide sulle competenze attribuite dalla normativa vigente alle Amministrazioni – riporta, per ciascuno degli obiettivi della Strategia Nazionale di Cybersicurezza – protezione, risposta e sviluppo – le misure da porre in essere per il loro conseguimento, suddivise per aree tematiche, per ognuna delle quali è indicato il novero degli attori responsabili per la loro attuazione e tutti gli altri soggetti a vario titolo interessati – per la cui disamina si rimanda al paragrafo successivo sul quadro di governance nazionale – al netto di quelli che, direttamente o indirettamente, beneficiano degli effetti che ne derivano.

Le Amministrazioni indicate come attori responsabili, sono chiamate a porre in essere le attività necessarie a dare attuazione alle corrispondenti misure, utilizzando le risorse finanziarie a disposizione, a legislazione vigente comprese quelle del PNRR, occorrenti allo scopo.

PROTEZIONE	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

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

Misura #3

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

Attori responsabili
ACN

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

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, MITD

Altri soggetti interessati
MiSE,
Associazioni di categoria

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

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
MITD, MEF, ACN

Altri soggetti interessati
MPA, altre
Amministrazioni NCS

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

Misura #9

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

Attori responsabili
ACN, Min. Interno, Min. Giustizia

Misura #10

Pubblicare linee guida sulla cybersecurity per le Amministrazioni Pubbliche, con differenti gradi di cogenza (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

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
MITD, Associazioni di categoria

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

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

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
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

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

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

Misura #19

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

Attori responsabili
ACN

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

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
MITD, Operatori privati

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, MiSE, MITD, Atenei, Ricerca, Operatori privati

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

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-DIE [1], DIS

Altri soggetti interessati
AISE, AISI, MAECI, Min. Interno, Min. Difesa, ACN, AGCOM

RISPOSTA

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-NCS [2]

Altri soggetti interessati
Altre Amministrazioni NCS

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-NCS [2]

Altri soggetti interessati
MAECI, altre Amministrazioni NCS

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

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-NCS [2]

Altri soggetti interessati
Altre Amministrazioni NCS, Operatori privati

[1] Dipartimento per l'Informazione e l'Editoria

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

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-NCS *

Altri soggetti interessati
DIS, AISE, AISI,
Min. Interno, Min. Difesa

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 #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

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

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

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

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

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

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

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

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

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-NCS *

Altri soggetti interessati
ACN, MAECI, Min. Interno, Min. Giustizia, Min. Difesa, MEF

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

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

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

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
Min. Istruzione

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

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

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

SVILUPPO

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

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
MiSE, MITD, ACN

Altri soggetti interessati
Associazioni di categoria, Atenei, Ricerca

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, MITD (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

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, MITD, MEF, MiSE, Min. Difesa (ricerca militare)

Altri soggetti interessati
Regioni e Province autonome, Atenei, Ricerca, Operatori privati

Sviluppo industriale, tecnologico e della ricerca

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, MiSE, ACN

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
MiSE, MITD, MAECI, ACN

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

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, MiSE

Altri soggetti interessati
Operatori privati, Associazioni di categoria

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

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
MITD, ACN

Altri soggetti interessati
MPA, Altre Amministrazioni centrali, Regioni e Province autonome

Misura #56

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

Attori responsabili
MITD, MiSE, ACN

Altri soggetti interessati
Amministrazioni centrali, Regioni e Province autonome

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

Misura #58

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

Attori responsabili
MITD

Altri soggetti interessati
ACN

FATTORI ABILITANTI — 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

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'Agenzia per la Cybersicurezza Nazionale.

Attori responsabili
ACN

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
MITD, MEF

Altri soggetti interessati
ACN, Min. Lavoro, Regioni e Province autonome, Operatori privati

Misura #64

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

Attori responsabili
MEF, MiSE, MITD

Altri soggetti interessati
Min. Lavoro, Regioni e Province autonome

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 propiziarne l'ulteriore formazione e l'inserimento nel mondo del lavoro. Ciò, anche al fine di promuovere iniziative volte a colmare il "confidence gap" delle studentesse nei confronti di carriere in ambiti scientifici e tecnologici.

Attori responsabili
PCM, Min. Istruzione, MUR, Atenei, CINI, ACN

Altri soggetti interessati
Min. Difesa

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
MiSE, MUR, Min. Istruzione, MITD, MEF

Altri soggetti interessati
Min. Lavoro, Associazioni di categoria, Operatori privati, Atenei

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, MITD, MAECI, CINI, Min. Difesa

Altri soggetti interessati
ACN, Associazioni di categoria, Operatori privati, Atenei

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

Misura #69

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

Attori responsabili
ACN, MAECI

Altri soggetti interessati
Atenei

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
MiSE, MITD, ACN

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

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

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
Min. Istruzione, MUR, Atenei, ACN

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, Min. Istruzione, Operatori privati, Atenei

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

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, MiSE

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

Misura #77

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

Attori responsabili
MAECI, ACN, Min. Difesa

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

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

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, MITD, MiSE

Misura #81

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

Attori responsabili
ACN, MITD, MiSE

Altri soggetti interessati
MAECI, Min. Difesa (ricerca militare)

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

#2

Governance nazionale

Governance nazionale

Alla luce del Piano d'implementazione sopra delineato, appare chiaro come il successo della strategia nazionale potrà essere assicurato soltanto tramite l'azione sinergica di istituzioni, industria, accademia e società civile, il cui rispettivo contributo, attraverso il conseguimento di singole azioni nei rispettivi ambiti, è essenziale per il raggiungimento degli obiettivi generali.

Parte integrante della scelta strategica è, dunque, la creazione di un ecosistema nazionale di cybersicurezza, nel quale i diversi soggetti interessati possano operare in modo coordinato per garantire al sistema Paese di sfruttare al meglio le molteplici opportunità offerte dai processi di innovazione tecnologica, contribuendo così alla prosperità e allo sviluppo economico-sociale dell'Italia.

Questa scelta è alla base della recente riforma dell'architettura nazionale cyber – realizzata con il decreto-legge 14 giugno 2021, n. 82 – attraverso cui il legislatore ha inteso riordinare e razionalizzare le competenze nazionali in materia di sicurezza cibernetica (prima frammentate e poste in capo a una pluralità di attori istituzionali), creando un ente centrale con competenza in materia, che possa anche rappresentare il punto di raccordo tra i diversi soggetti interessati. Ciò, anche al fine di consentire l'attuazione degli obiettivi strategici all'interno di un sistema coordinato e armonizzato, nel quale l'unicità dell'indirizzo definito dal vertice politico sia garantita, in via di attuazione, tramite l'azione organizzata degli attori coinvolti.

L'evoluzione della normativa nazionale in materia di cybersicurezza

Per far fronte all'aumento dell'interconnessione e dell'interdipendenza tra i sistemi informatici e alle correlate minacce, sia l'Europa sia l'Italia si sono dotate di un apparato normativo in costante evoluzione.

In estrema sintesi, solo nell'ultimo quinquennio, l'Italia ha adottato i seguenti provvedimenti in materia di cybersicurezza:

- DPCM del 17 febbraio 2017, che ha aggiornato l'architettura nazionale di sicurezza cibernetica già delineata dal DPCM del 23 gennaio 2013;
- decreto legislativo 18 maggio 2018, n. 65 (di seguito decreto NIS), che prevede obblighi sia di notifica degli incidenti aventi un impatto rilevante sulla continuità dei servizi forniti, sia di implementazione di misure di sicurezza basate sull'analisi del rischio per gli Operatori di Servizi Essenziali e i Fornitori di Servizi Digitali;
- decreto-legge 21 settembre 2019, n. 105 (di seguito decreto Perimetro), che ha istituito il Perimetro di sicurezza nazionale cibernetica, con l'obiettivo di tutelare gli asset digitalizzati dal cui malfunzionamento, interruzioni, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, prevedendo, rispetto al decreto NIS, più stringenti criteri di notifica degli incidenti e maggiori livelli di sicurezza, estesi anche alla supply chain, nonché specifiche procedure in materia di procurement ICT ad essi destinati;
- decreto-legge 19 luglio 2020, n. 76, che ha fornito impulso alla digitalizzazione della PA, prevedendo che la stessa avvenga osservando principi di sicurezza cibernetica compresa la formazione del personale e la promozione della consapevolezza circa l'importanza della sicurezza informatica;
- decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;
- la Strategia Cloud Italia, adottata nell'ambito del Piano triennale per l'informatica nella Pubblica Amministrazione 2020-2022 e definita dal Dipartimento per la trasformazione digitale in collaborazione con l'Agenzia per la Cybersicurezza Nazionale, al fine di incentivare la diffusione di soluzioni basate sul cloud computing nel circuito delle Pubbliche Amministrazioni;
- decreto legislativo 8 novembre 2021, n. 207, di Attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche e disciplina, tra l'altro, i requisiti di cybersicurezza delle reti pubbliche di comunicazione o dei servizi di comunicazione elettronica accessibili al pubblico, l'obbligo di notifica di incidenti significativi, nonché l'adozione di misure di sicurezza, attribuendo la competenza in materia all'ACN;
- il decreto-legge 21 marzo 2022, n. 21, che ha recato, 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, ivi inclusi quelli relativi alla tecnologia cloud. In particolare, ha ridefinito gli obblighi e le procedure di notifica da parte delle imprese interessate, nonché le procedure di esercizio dei poteri speciali, di monitoraggio e sanzionatori da parte del Governo, prevedendo la partecipazione dell'Agenzia per la Cybersicurezza Nazionale, la possibilità di avvalersi anche del Centro di Valutazione e Certificazione Nazionale (CVCN) e la possibilità di condurre attività ispettive e di verifica.

In tale quadro, il **Presidente del Consiglio dei ministri,** vertice dell'architettura istituzionale e organo d'indirizzo politico-strategico in materia, esercita l'alta direzione e detiene la responsabilità generale delle politiche di cybersicurezza. Il Presidente può delegare **all'Autorità delegata per la sicurezza della Repubblica,** di cui all'articolo 3 della legge 3 agosto 2007, n. 124, le funzioni che non sono ad esso attribuite in via esclusiva.

Sempre a livello politico-strategico, primaria importanza riveste il **Comitato Interministeriale per la Cybersicurezza (CIC)**, istituito presso la Presidenza del Consiglio dei ministri, con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza. Il CIC rappresenta la sede politica nella quale esaminare e indirizzare le problematiche relative alla cybersicurezza, condividere gli obiettivi strategici e gli indirizzi, nonché monitorare l'attuazione delle politiche in materia. A tal fine, il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della difesa, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico, dal Ministro della transizione ecologica, dal Ministro dell'università e della ricerca, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale e dal Ministro delle infrastrutture e della mobilità sostenibili.

In particolare, il CIC è sentito dal Presidente del Consiglio dei ministri ai fini dell'adozione della strategia nazionale di cybersicurezza ed esercita l'alta sorveglianza sulla sua attuazione. Contribuisce, inoltre, alla realizzazione della strategia stessa proponendo al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza e promuovendo l'adozione delle iniziative necessarie a favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, alla condivisione delle informazioni e all'adozione di migliori pratiche e di misure e allo sviluppo industriale, tecnologico e scientifico in materia.

Considerato l'impatto trasversale delle politiche definite in relazione all'ambito cyber, era stata avvertita l'esigenza di una specifica autorità di raccordo con il livello politico-strategico e di coordinamento degli attori coinvolti in materia, nonché di regolamentazione, certificazione e vigilanza del settore. Ciò, in particolare, al fine di assicurare iniziative coerenti, rappresentare un chiaro e aggiornato quadro situazionale all'Autorità politica, nonché fornire un'interfaccia unica a livello nazionale, europeo e internazionale, assicurando una postura nazionale unitaria.

Pertanto, è stata istituita l'**Agenzia per la Cybersicurezza Nazionale (ACN)** che, in qualità di Autorità nazionale per la cybersicurezza deputata alla tutela della sicurezza e della resilienza nello spazio cibernetico, anche ai fini della tutela della sicurezza nazionale e della salvaguardia degli interessi nazionali, detiene un ruolo centrale nel raggiungimento dei tre macro-obiettivi individuati nella presente strategia.

Quale autorità nazionale per la cybersicurezza, l'ACN:

- assicura il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza;
- promuove, anche in un'ottica di rafforzamento della partnership pubblico-privato, la realizzazione di una

cornice di sicurezza e resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle Pubbliche Amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore.

Le funzioni attribuite all'Agenzia esprimono un approccio olistico alla gestione della cybersicurezza, nel quale acquistano rilevanza non solo gli interventi di natura prevalentemente tecnica, volti a garantire la sicurezza e la resilienza delle reti, dei sistemi informativi e dei servizi informatici, ma anche le progettualità finalizzate allo sviluppo di nuovi prodotti e tecnologie, della ricerca e della competitività industriale, nonché alla creazione di una forza lavoro nazionale di settore in grado di rispondere alle esigenze del mercato.

LE ARTICOLAZIONI DELL'ACN

Gabinetto	Mantenimento quadro normativo nazionale cyber aggiornato Tavoli cyber interministeriali (CIC, NCS, Perimetro)
Autorità e sanzioni	Adempimento disposizione decreti NIS, PSNC e Telco Sanzioni
Certificazione e vigilanza	Centro di Valutazione e Certificazione Nazionale (CVCN) Autorità nazionale di certificazione in materia di cybersicurezza Attività ispettiva e di verifica degli adempimenti di cybersicurezza
Operazioni	Computer Security Incident Response Team (CSIRT) Italia Monitoraggio, prevenzione, risposta ad attacchi cyber
Programmi industriali, tecnologici, di ricerca e formazione	Promozione programmi di ricerca Centro nazionale di coordinamento in materia di cybersicurezza (NCC) Promozione formazione in cybersicurezza
Risorse umane e strumentali	Reclutamento, formazione e sviluppo professionale del personale Gestione delle risorse strumentali
Strategie e cooperazione	Predisposizione strategia nazionale di cybersecurity Elaborazione di policy nazionali e iniziative di awareness Relazioni internazionali e cooperazione

In particolare, l'Agenzia, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni:

- opera quale ente regolatore, certificatore, nonché di vigilanza del settore della cybersicurezza, che definisce, ad esempio, i livelli minimi delle misure di sicurezza nei diversi ambiti (tra cui energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali, comunicazioni elettroniche, *cloud* nazionale, pubblica amministrazione), potendo anche effettuare ispezioni e irrogare sanzioni;
- cura e promuove la definizione ed il mantenimento di un quadro normativo aggiornato e coerente nel settore della cybersicurezza;
- contribuisce a ridurre il rischio derivante dall'approvvigionamento tecnologico, incrementando i livelli di sicurezza della *supply chain*, con particolare riguardo a soluzioni e prodotti destinati ad essere utilizzati su infrastrutture e sistemi ICT rilevanti per la sicurezza nazionale;
- sviluppa le capacità di monitoraggio, rilevamento, prevenzione, analisi e risposta agli incidenti cibernetici;
- coordina, in raccordo con il MAECI, la cooperazione internazionale nella materia della cybersicurezza;
- supporta lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche e promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza;
- svolge attività di comunicazione e di promozione della consapevolezza riguardo al tema della cybersicurezza, contribuendo così allo sviluppo di una cultura nazionale in materia;
- è designata quale Centro Nazionale di Coordinamento (NCC), ai sensi dell'articolo 6 del Regolamento (UE) 2021/887 del Parlamento e del Consiglio europeo, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

Ai fini dello svolgimento delle funzioni sopra illustrate, operano presso l'Agenzia:

- il **Computer Security Incident Response Team (CSIRT) Italia,** la cui azione è volta alla prevenzione, al monitoraggio, al rilevamento, all'analisi e alla risposta ad incidenti cibernetici;
- il **Centro di Valutazione e Certificazione Nazionale (CVCN)**, che si occuperà di verificare la sicurezza e l'assenza di vulnerabilità note in beni, sistemi e servizi ICT in uso nelle infrastrutture da cui dipendono le funzioni e i servizi essenziali del Paese;
- il **Centro Nazionale di Coordinamento** in materia di cybersicurezza nell'ambito industriale, tecnologico e della ricerca.

Il disegno complessivo dell'architettura istituzionale di cybersicurezza rende imprescindibile, per il raggiungimento di elevati livelli di sicurezza nel dominio cibernetico e la protezione degli asset strategici, il concorso in stretta sinergia con altre Amministrazioni, cui la normativa vigente assegna prerogative esclusive in aderenza ai rispettivi mandati istituzionali.

Tra queste, in particolare:

- il **Comparto intelligence**, competente per la cyber-intelligence, conduce attività di ricerca e raccolta informativa finalizzata alla tutela degli interessi politici, militari, economici, scientifici e industriali dell'Italia, e provvede alla formulazione di analisi, valutazioni e previsioni sulla minaccia cibernetica, al fine di preservare la sicurezza nazionale, anche attraverso la conduzione di operazioni cyber. In particolare, secondo le modalità e le procedure stabilite dalla legge n. 124/2007, il Direttore Generale del DIS, avvalendosi degli uffici del Dipartimento, cura il coordinamento delle attività di ricerca informativa e le Agenzie, ciascuna nell'ambito delle rispettive attribuzioni, svolgono, secondo gli indirizzi definiti dalle direttive che il Presidente del Consiglio dei ministri impartisce, sentito il CISR, e le linee di coordinamento delle attività di ricerca informativa stabilite dal Direttore Generale del DIS, le attività di ricerca e di elaborazione informativa rivolte alla protezione cibernetica e alla sicurezza informatica nazionali.
- il **Ministero dell'interno**, quale autorità nazionale di pubblica sicurezza, tutela l'ordine e la sicurezza pubblica, il soccorso pubblico e la difesa civile. In particolare, il Dipartimento di pubblica sicurezza assicura le attività di prevenzione e contrasto ai crimini informatici attraverso la Polizia Postale e delle Comunicazioni, ferme restando le competenze negli ambiti definiti dal legislatore degli uffici e comandi della Polizia di Stato, dell'Arma dei carabinieri e della Guardia di finanza. Per la protezione delle infrastrutture critiche informatizzate dai reati informatici opera il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) della Polizia di Stato che svolge un costante monitoraggio della rete internet, oltre alle funzioni di punto di contatto nazionale per le emergenze in materia di criminalità informatica transnazionale.

  Nell'ambito del Dipartimento della Pubblica Sicurezza, è stata istituita – attraverso il DPR n. 231 del 19 novembre 2021, che modifica il DPCM n. 78 dell'11 giugno 2019 – e sarà prossimamente operativa la Direzione Centrale per la polizia scientifica e la sicurezza cibernetica. La Direzione diviene competente a sviluppare le attività di prevenzione e tutela informatica e cibernetica già attribuite al CNAIPIC, nonché quelle assegnate al Ministero dell'interno dal decreto Perimetro, incaricato, tra l'altro, di verificare le condizioni di sicurezza e l'assenza di vulnerabilità note per le forniture ICT da impiegare su reti, sistemi informativi e servizi informatici di propria pertinenza inclusi nel Perimetro, espletata attraverso il proprio Centro di Valutazione che opera in stretto raccordo con il CVCN.
- il **Ministero della difesa**, competente per la difesa e la sicurezza militare dello Stato.
  In particolare, il Dicastero definisce e coordina la politica militare, la *governance* e le capacità militari nell'ambiente cibernetico, nonché lo sviluppo di capacità cibernetiche e la protezione delle proprie reti e sistemi sia sul territorio nazionale sia nei teatri operativi all'estero. La Difesa, attraverso il Comando per le Operazioni in Rete (COR) e col contributo specialistico del Reparto Informazioni e Sicurezza (RIS) dello

Stato Maggiore della Difesa (SMD), è deputato alla pianificazione e conduzione di operazioni militari cibernetiche offensive e difensive nei casi previsti.

Tale Dicastero, pertanto, assicura, anche in situazioni di crisi di natura cibernetica (sia nazionale sia internazionale), tutti i servizi e le attività necessari, da un lato, a garantire la protezione, la resilienza e l'efficienza delle reti e infrastrutture militari e, dall'altro, a sviluppare le proprie peculiari capacità necessarie all'implementazione di attività di supporto, difesa, reazione e stabilizzazione.

In ambito NATO, la Difesa assicura la partecipazione dell'Italia alle attività di natura militare conseguenti all'elezione dello spazio cibernetico a dominio di operazioni. La Difesa contribuisce, altresì, nel rispetto delle competenze attribuite dalla normativa vigente ad altre Amministrazioni, ad assicurare la definizione delle policy cyber, al rafforzamento e allo sviluppo delle capacità cyber dell'Alleanza.

Analogamente al Ministero dell'interno, la Difesa verifica le condizioni di sicurezza e l'assenza di vulnerabilità note per le forniture ICT da impiegare su reti, sistemi informativi e servizi informatici di propria pertinenza inclusi nel Perimetro di sicurezza nazionale cibernetica, attraverso il proprio Centro di Valutazione che opera in stretto raccordo con il CVCN.

Parallelamente, nell'ambito del coordinamento operato dall'ACN, ciascun **Ministero e autorità con competenze e interessi trasversali in materia cyber** svolge un ruolo nel raggiungimento dei suddetti obiettivi. Tale ruolo assume rilievo sia attraverso la messa in sicurezza delle proprie reti e infrastrutture digitali, sia attraverso la partecipazione agli organismi inter-istituzionali e alle iniziative promosse dall'ACN, volte ad accrescere la cybersicurezza.

In particolare, il **Ministero degli affari esteri e della cooperazione internazionale (MAECI)** sviluppa le iniziative di cyber diplomacy, in attuazione degli indirizzi della politica estera nazionale e promuovendo la tutela dei diritti e delle libertà fondamentali nello spazio cibernetico. Inoltre, il MAECI contribuisce alla definizione della posizione italiana nei massimi consessi europei e internazionali cyber.

Il **Ministero dello sviluppo economico (MiSE)** gioca un ruolo strategico per lo sviluppo della competitività del sistema imprenditoriale, attraverso la promozione della ricerca e dell'innovazione, la diffusione delle tecnologie digitali e delle nuove tecnologie, il trasferimento tecnologico, la sostenibilità ambientale. In tale contesto, supporta l'operatività dei Digital Innovation Hub cui è affidato il compito di contribuire alla transizione digitale dell'industria, con particolare riferimento alle PMI, e della Pubblica Amministrazione attraverso l'adozione delle tecnologie digitali avanzate, intelligenza artificiale, calcolo ad alte prestazioni, sicurezza informatica.

Il trasferimento all'Agenzia delle competenze in materia di cybersecurity – in attuazione del decreto-legge n. 82/2021 – lascia comunque al Ministero un notevole patrimonio di conoscenza in materia di sicurezza informatica che sarà focalizzato essenzialmente sulle attività di formazione condotte anche grazie alla Scuola Superiore di Specializzazione in Telecomunicazioni e di Ricerca in materia di tecnologie innovative e digitali, attraverso collaborazioni con Accademia e Enti di ricerca, svolte nell'ambito della Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione.

Al MiSE sono affidate, altresì, le funzioni di Autorità di settore NIS e il compito di individuare i soggetti rientranti nel Perimetro di sicurezza nazionale cibernetica di cui al decreto-legge n. 105/2019, nell'ambito dei propri settori di competenza.

Il **Ministero dell'economia e delle finanze (MEF)** svolge per il tramite della Guardia di Finanza – in particolare il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche – attività di contrasto agli illeciti economico-finanziari perpetrati per mezzo delle tecnologie informatiche.

Banca d'Italia, in qualità di autorità di vigilanza di settore, emana regolamenti e linee guida per il rafforzamento della resilienza cyber degli operatori posti sotto la sua supervisione. Riceve, altresì, le notifiche di incidenti da parte delle banche e degli intermediari finanziari, ai sensi delle principali normative di settore.

Inoltre, Banca d'Italia presiede il CODISE, struttura di coordinamento delle crisi operative della piazza finanziaria italiana, a cui partecipano la Consob e gli operatori rilevanti di settore. In caso di incidenti cyber su larga scala, il CODISE si coordina con il CERT Finanziario Italiano (CERTFin) al fine di assicurare una costante analisi situazionale e il necessario supporto tecnico. Il CERT di Banca d'Italia si rapporta con i principali soggetti interessati nazionali (primi fra tutti, il CSIRT Italia, il CNAIPIC e il CERTFin) ed è, tra l'altro, responsabile della gestione degli incidenti cyber a danno della Banca stessa, nonché dell'organizzazione di programmi di addestramento e formazione, di iniziative di *info-sharing* e di campagne di *awareness*.

Il **Ministero dell'istruzione** e il **Ministero dell'università e della ricerca (MUR)**, promuovono – in stretta collaborazione con l'ACN, le altre Pubbliche Amministrazioni e con il settore privato – un piano strutturato di formazione e di educazione digitale che consenta di colmare la mancanza delle specifiche professionalità richieste dal mercato. In relazione, poi, alle competenze in tema di ricerca scientifica e tecnologica, il MUR assicura ogni forma di indirizzo, programmazione e coordinamento per garantire che le nuove tecnologie siano sviluppate tenendo conto degli aspetti di sicurezza cibernetica; promuove, altresì, la cooperazione scientifica in ambito nazionale, comunitario e internazionale, anche mediante specifici raccordi fra università ed enti di ricerca.

Il **Dipartimento per la Trasformazione Digitale (DTD)**, che lavora a supporto del **Ministro per l'innovazione tecnologica e la transizione digitale** e del Presidente del Consiglio dei ministri, promuove e coordina le azioni del Governo finalizzate alla definizione di una strategia unitaria in materia di trasformazione digitale della Pubblica Amministrazione e modernizzazione tecnologica del Paese, anche al fine di realizzare gli obiettivi dell'Agenda digitale italiana, svolgendo, inoltre, tutte le attività volte ad assicurare, in raccordo con le amministrazioni interessate, lo sviluppo e la diffusione delle competenze necessarie per un adeguato uso delle tecnologie digitali nei mondi della scuola, dell'università e della ricerca, della Pubblica Amministrazione centrale e locale, della giustizia, dell'impresa, del lavoro e dell'attività sociale.

L'**Agenzia per l'Italia Digitale (AgID)** promuove l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della Pubblica Amministrazione e nel rapporto tra questa, i cittadini e le imprese. In particolare, redige il Piano triennale per l'informatica nella Pubblica Amministrazione, svolge funzioni nell'ambito delle procedure in materia di acquisizione di beni e servizi ICT, rilasciando pareri tecnici sugli schemi di contratti e accordi quadro, oltre una specifica soglia, da parte delle Pubbliche Amministrazioni cen-

trali concernenti l'acquisizione di beni e servizi informativi automatizzati, e sulle procedure di gara bandite da Consip e da altri soggetti aggregatori; svolge attività di vigilanza sui servizi fiduciari, sui gestori di posta elettronica certificata, sui conservatori di documenti informatici accreditati, nonché sui soggetti pubblici e privati che partecipano al Sistema Pubblico di Identità Digitale (SPID).

Fondamentale e decisivo apporto è inoltre fornito dalle **altre Amministrazioni componenti dei diversi tavoli inter-istituzionali**, tra i quali assume particolare rilievo il **Nucleo per la Cybersicurezza (NCS).**

Come sede di coordinamento interministeriale istituita presso l'Agenzia per la Cybersicurezza Nazionale, che opera a supporto del Presidente del Consiglio dei ministri per gli aspetti relativi alla prevenzione e alla preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento, l'NCS può facilitare, in particolare, il raggiungimento dell'obiettivo n. 2. L'NCS garantisce, infatti, l'allineamento tra l'ACN, il Consigliere militare del Presidente del Consiglio dei ministri, il Comparto intelligence, il Ministero degli affari esteri e della cooperazione internazionale, il Ministero dell'interno, il Ministero della giustizia, il Ministero della difesa, il Ministero dell'economia e delle finanze, il Ministero dello sviluppo economico, il Ministero della transizione ecologica, il Ministero delle infrastrutture e della mobilità sostenibili, il Ministero dell'università e della ricerca, il Dipartimento per la trasformazione digitale. Al contempo, il Nucleo, cui spetta il compito di formulare proposte di iniziativa in materia di cybersicurezza, è anche una piattaforma nella quale discutere le diverse iniziative promosse dalle Amministrazioni con riflessi sulle politiche di cybersicurezza e può, pertanto, rappresentare la sede principale attraverso cui assicurare lo sviluppo coordinato di iniziative concernenti anche gli obiettivi n. 1 e 3. In tale contesto, possono essere chiamati a partecipare i soggetti interessati anche privati.

Sempre nell'ambito del coordinamento inter-istituzionale, oltre all'NCS, ulteriori sedi per il raggiungimento degli obiettivi, in particolare dell'obiettivo n. 1 (protezione degli asset strategici), sono rappresentate dal Tavolo interministeriale per l'attuazione del Perimetro di sicurezza nazionale cibernetica, nonché, una volta istituito, dal Comitato tecnico di raccordo di cui al decreto NIS.

Sul versante privato, gli **operatori economici**, l'**accademia** e la **ricerca** e, non ultima, la **società civile**, rappresentano elementi imprescindibili per la resilienza del istema-Paese e costituiscono, pertanto, parte essenziale dell'ecosistema nazionale di cybersicurezza. In tal senso, anche attraverso il fondamentale stimolo e contributo offerto dall'Agenzia per la Cybersicurezza Nazionale e sulla base delle funzioni ad essa attribuite per legge, andrà ricercata e sostenuta una costante collaborazione, da incrementare tramite specifiche intese e convenzioni, fra le amministrazioni pubbliche sopra elencate, le università, gli enti di ricerca e gli operatori privati (anche attraverso le associazioni di categoria). Ciò al fine di garantire una proficua interazione tanto con i soggetti che gestiscono asset ICT strategici, quanto con l'intero tessuto produttivo nazionale, incluse le PMI e le startup.

Frutto di un'efficiente collaborazione pubblico-privata è, ad esempio, il Framework Nazionale per la Cybersecurity e la *Data Protection*, realizzato dal CIS-Sapienza e dal Consorzio Interuniversitario Nazionale per l'Informatica (CINI). Il framework fornisce una metodologia applicabile, a livello trasversale e indipendentemente dalla dimensione, da organizzazioni pubbliche e private, per supportare l'avvio di iniziative orientate alla

cybersecurity e alla protezione dei propri asset, così da ridurre le vulnerabilità e i rischi a cui tali organizzazioni sono esposte. Il documento viene periodicamente aggiornato e integrato, al fine di assicurare piena aderenza alle più recenti normative di settore, dal Regolamento Generale sulla Protezione dei Dati (GDPR), al Cybersecurity Act e alle misure in materia di sicurezza della supply chain.

Ulteriori iniziative volte ad accrescere la partnership pubblico-privata e con il mondo dell'accademia e della ricerca sono quelle avviate in materia di promozione e rafforzamento della consapevolezza circa l'importanza della sicurezza informatica. Tra queste, si annoverano le conferenze e gli eventi organizzati su scala nazionale quali ITASEC, nonché quelle finalizzate alla creazione di una solida forza lavoro nazionale di giovani talenti altamente specializzati nel settore della sicurezza cibernetica, come CyberChallenge.it, programma di formazione avviato dal CINI e che proseguirà beneficiando anche della collaborazione dell'ACN.

Dal punto di vista dello sviluppo della ricerca nel campo della cybersecurity, rilevano, inoltre, gli otto centri di competenza istituiti dal MiSE – in cui la partnership pubblico-privata è orientata a realizzare attività di addestramento e supporto nella realizzazione di progetti innovativi nel settore Impresa 4.0 – i Digital Innovation Hub (DIH) e i dodici Cluster tecnologici istituiti dal MUR.

Simili iniziative di cooperazione continueranno ad essere sviluppate sinergicamente dai soggetti interessati, nell'ambito del coordinamento operato dall'ACN e nel rispetto degli indirizzi del Presidente del Consiglio dei ministri, dell'Autorità delegata e del CIC, con il fine di contribuire al continuo innalzamento dei livelli di cybersicurezza del Paese.

#3

Glossario

Glossario

A

Amministrazioni CISR

Amministrazioni che compongono il Comitato Interministeriale per la Sicurezza della Repubblica, ovvero Ministeri degli affari esteri e della cooperazione internazionale, dell'interno, della giustizia, della difesa, dell'economia e delle finanze e dello sviluppo economico, nonché della transizione ecologica. Il CISR è altresì composto dal Presidente del Consiglio dei ministri, che lo presiede, e dall'Autorità delegata laddove nominata. Al Direttore Generale del DIS sono assegnate le funzioni di segretario del Comitato.

Amministrazioni NCS

Amministrazioni che compongono il Nucleo per la cybersicurezza, ovvero Consigliere militare del Presidente del Consiglio dei ministri, Dipartimento delle informazioni per la sicurezza (DIS), Agenzia informazioni e sicurezza esterna (AISE), Agenzia informazioni e sicurezza interna (AISI), Ministeri degli affari esteri e della cooperazione internazionale, dell'interno, della giustizia, della difesa, dell'economia e delle finanze, dello sviluppo economico, della transizione ecologica, dell'università e della ricerca, dell'innovazione tecnologica e la transizione digitale, delle infrastrutture e della mobilità sostenibili, nonché Dipartimento della protezione civile.

Autorità nazionale competente NIS

Autorità incaricata di attuare il decreto NIS, vigilando sulla sua applicazione ed esercitando le relative potestà ispettive e sanzionatorie. A seguito delle modifiche introdotte al decreto NIS dal D.L. 82/2021 (art. 15, co. 1, lett. g), l'ACN è designata quale Autorità nazionale competente NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III del decreto NIS.

Autorità settoriali NIS

A seguito delle modifiche introdotte al decreto NIS dal D.L. 82/2021 (art. 15, co. 1, lett. g), sono autorità settoriali NIS:

- il Ministero dello sviluppo economico, per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali;
- il Ministero delle infrastrutture e della mobilità sostenibili, per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada;
- il Ministero dell'economia e delle finanze, per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob, secondo modalità di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze;
- il Ministero della salute, per l'attività di assistenza sanitaria, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso, e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati dalle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza;
- il Ministero della transizione ecologica per il settore energia, sottosettori energia elettrica, gas e petrolio;
- il Ministero della transizione ecologica e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

B

Blockchain

Struttura di dati sotto forma di registro distribuito, composto da blocchi in cui sono inserite, in ordine cronologico e in modo immutabile e irreversibile, le informazioni necessarie al funzionamento di un determinato sistema. In quanto distribuito, il registro è costituito da più copie, ognuna gestita da un diverso soggetto. Dal momento che è necessario garantirne la coerenza, le copie sono aggiornate in maniera indipendente, ma dovranno contenere le stesse informazioni nello stesso ordine. La tecnologia blockchain è impiegata per lo sviluppo delle più disparate applicazioni, quali, ad esempio, le criptovalute.

Border Gateway Protocol (BGP)

Standard di rete che stabilisce i percorsi logici di connessione tra i sistemi autonomi (quali gruppi di dispositivi di rete e reti sotto il controllo di una specifica autorità), attraverso i quali passano i dati.

C

Centri di competenza ad alta specializzazione

Partenariati pubblico-privati il cui compito è quello di svolgere attività di orientamento e formazione alle imprese su tematiche Industria 4.0 nonché di supporto nell'attuazione di progetti di innovazione, ricerca industriale e sviluppo sperimentale finalizzati alla realizzazione, da parte delle imprese fruitrici, in particolare delle PMI, di nuovi prodotti, processi o servizi (o al loro miglioramento) tramite tecnologie avanzate in ambito Industria 4.0.

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

Istituito dal Regolamento (UE) 887/2021, l'ECCC ha l'obiettivo generale di promuovere la ricerca e l'innovazione nel settore della cybersicurezza al fine di potenziare l'autonomia strategica dell'Unione, sostenerne le capacità e le competenze tecnologiche e aumentare la competitività dell'industria europea in tale settore. Ciò, rafforzando le competenze, le capacità e le infrastrutture di cybersicurezza degli Stati membri, attuando specifiche azioni e promuovendo la resilienza e l'adozione di migliori pratiche in materia.

Per assolvere tale missione, l'ECCC è responsabile dell'attuazione delle azioni individuate nelle parti relative alla cybersicurezza dei programmi di finanziamento "Digital Europe Programme" e "Horizon Europe Programme".

Centro Nazionale di Coordinamento (NCC)

Previsto dall'articolo 6 del Regolamento (UE) 887/2021, tra le altre cose: funge da punto di contatto a livello nazionale nei confronti dell'ECCC per assisterlo nel conseguimento dei suoi obiettivi; attua azioni specifiche finanziate dall'ECCC, anche fornendo sostegno finanziario a terzi e creando sinergie con attività pertinenti a livello nazionale; incoraggia la partecipazione della società civile, dell'industria, della comunità accademica e della ricerca, nonché di altri portatori di interessi a livello nazionale ai progetti transfrontalieri e alle azioni finanziate dai pertinenti programmi dell'Unione.

Centro di Valutazione e Certificazione Nazionale (CVCN)

Inizialmente istituito presso il Ministero dello sviluppo economico, a seguito delle modifiche introdotte dal D.L. 82/2021 (art. 7, co. 4), il CVCN è trasferito presso l'ACN. Il CVCN ha il compito di: verificare – avvalendosi anche di laboratori accreditati – le condizioni di sicurezza e di assenza di vulnerabilità note di forniture ICT, appartenenti a determinate categorie, da impiegare sui beni ICT inclusi nel Perimetro; elaborare e adottare schemi di certificazione cibernetica – tenendo conto degli standard definiti a livello internazionale e dell'Unione europea – qualora, per ragioni di sicurezza nazionale, quelli esistenti non siano ritenuti adeguati alle esigenze di tutela del Perimetro.

Centri di Valutazione (CV)

Centri di valutazione del Ministero dell'interno e del Ministero della difesa, accreditati dal CVCN ai sensi del decreto Perimetro.

CERT (Computer Emergency Response Team)

Struttura con compiti di prevenzione e di coordinamento della risposta ad eventi cibernetici. Diversi CERT svolgono anche funzioni di formazione ed informazione nei confronti degli utenti.

Cloud Computing

Paradigma di utilizzo e gestione di risorse computazionali e di servizi informatici erogati su richiesta. I servizi Cloud si differenziano, sulla base del modello di risorse computazionali offerte, in tre modelli di servizio:

1. servizi sistemistici infrastrutturali, c.d. Infrastructure-as-a-Service (IaaS);
2. servizi di piattaforme computazionali, c.d. Platform-as-a-Service (PaaS), per l'erogazione di ambienti pre-configurati e amministrati per lo sviluppo di specifiche applicazioni;
3. servizi applicativi, c.d. Software-as-a-Service (SaaS), per l'erogazione di un'applicazione agli utenti finali.

I servizi sono erogati da fornitori di servizi Cloud (Cloud Service Provider-CSP) e il relativo modello di distribuzione può essere organizzato in modalità: Cloud pubblico, Cloud privato, Cloud ibrido e Multi-Cloud.

Cluster tecnologici

Reti di soggetti pubblici e privati che operano quali catalizzatori di risorse per coordinare il mondo della ricerca e delle imprese in settori quali la ricerca industriale, la formazione e il trasferimento tecnologico.

Comitato Interministeriale per la Cybersicurezza (CIC)

Comitato istituito presso la Presidenza del Consiglio dei Ministri con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza. Il CIC, tra i suoi compiti, esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza e promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza. È presieduto dal Presidente del Consiglio dei Ministri ed è composto dall'Autorità delegata, ove istituita, e dai Ministri degli affari esteri e della cooperazione internazionale, dell'interno, della giustizia, della difesa, dell'economia e delle finanze, dello sviluppo economico, della transizione ecologica, dell'università e della ricerca, per l'innovazione tecnologica e la transizione digitale e delle infrastrutture e della mobilità sostenibili. Le funzioni di segretario sono svolte dal Direttore generale dell'ACN.

Comitato Interministeriale per la Sicurezza della Repubblica (CISR)

Organo collegiale del Sistema di informazioni per la sicurezza della Repubblica con funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza. È l'organismo al quale, tra l'altro, compete definire, su base annuale, gli obiettivi informativi su cui concentrare l'attività di informazione per la sicurezza e deliberare sulla ripartizione delle risorse finanziarie tra il Dipartimento delle informazioni per la sicurezza e i servizi di informazione, nonché sui relativi bilanci. È presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, e dai Ministri degli affari esteri, dell'interno, della giustizia, della difesa, dell'economia e finanze, dello sviluppo economico e della transizione ecologica. Le funzioni di segretario sono svolte dal Direttore generale del DIS.

Comitato tecnico di raccordo NIS

Organo collegiale, previsto dal decreto NIS ed istituito presso l'ACN, finalizzato ad assicurare la collaborazione delle Autorità di settore con l'Autorità competente NIS, per l'adempimento degli obblighi attribuiti dal decreto NIS. Il Comitato è presieduto dall'ACN, quale autorità competente NIS, ed è composto dai rappresentanti delle Amministrazioni statali individuate quali autorità di settore e da rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati dalle Regioni e Province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano.

Confidence Building Measures (CBMs)

Misure definite in ambito OSCE e volte a ridurre i rischi connessi alla possibile emersione di tensioni politico-militari derivanti da attacchi cibernetici e a rafforzare la cooperazione tra gli Stati partecipanti.

Consorzio Interuniversitario Nazionale per l'Informatica (CINI)

Il Consorzio è costituito da 49 Università pubbliche e da più di 1.300 docenti. Promuove e coordina attività scientifiche, di ricerca e di trasferimento, sia di base sia applicative, nel campo dell'informatica, di concerto con le comunità scientifiche nazionali di riferimento.

Controlli essenziali di cybersecurity

Elenco di 15 controlli che rappresentano le pratiche imprescindibili di sicurezza informatica implementabili, in modo facile ed economico, da medie, piccole o micro imprese, per ridurre il numero di vulnerabilità presenti nei loro sistemi e aumentare la consapevolezza del personale interno. I controlli, derivati dal Framework Nazionale per la Cybersecurity, sono stati pubblicati dal Centro di Ricerca di Cyber Intelligence and Information Security (CIS) dell'Università La Sapienza e dal Laboratorio Nazionale di Cybersecurity del Consorzio Interuniversitario Nazionale per l'Informatica (CINI).

Coordinated vulnerability disclosure

Processo strutturato da uno Stato, attraverso il quale le vulnerabilità informatiche non note, rilevate da ricercatori/ethical hacker, sono segnalate alle organizzazioni in modo tale da consentire a queste ultime di diagnosticarle ed eliminarle. La divulgazione coordinata delle vulnerabilità comprende anche il coordinamento tra il soggetto segnalante e l'organizzazione, relativamente ai tempi per la risoluzione e la pubblicazione delle vulnerabilità.

Cryptojacking

Trattasi del mining malevolo di criptovalute, consistente nell'utilizzo, non autorizzato, di un dispositivo di un soggetto terzo per finalità di mining di valute digitali.

CSIRT (Computer Security Incident Response Team)

Unità organizzativa deputata a coordinare la risposta a incidenti informatici, a mitigarne gli effetti e a prevenire il verificarsi di ulteriori eventi.

CSIRT Italia

Inizialmente istituito presso il DIS, a seguito delle modifiche introdotte dal D.L. 82/2021 (art. 7, co. 3) lo CSIRT è stato trasferito presso l'ACN assumendo la denominazione di "CSIRT Italia". Ha il compito di: monitorare gli incidenti a livello nazionale; emettere preallarmi, allerte, annunci e divulgare informazioni alle parti interessate in merito a rischi e incidenti; intervenire in caso di incidente; effettuare l'analisi dinamica dei rischi e degli incidenti; effettuare la sensibilizzazione situazionale; partecipare alla rete europea degli CSIRT. A tal fine, lo CSIRT stabilisce relazioni di cooperazione con il settore privato e promuove l'adozione e l'uso di prassi comuni o standardizzate nei settori delle procedure di trattamento degli incidenti e dei rischi e sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

CSIRT Network

Rete degli CSIRT degli Stati membri dell'UE a cui partecipa anche il CERT-UE. La Commissione Europea partecipa alla rete in qualità di osservatore ed ENISA funge da segretariato della rete, con il compito di sostenere attivamente la cooperazione tra CSIRT e, su richiesta, fornire supporto attivo per il coordinamento degli incidenti. La rete CSIRT fornisce un forum in cui i membri possono cooperare e scambiare informazioni. L'Italia è rappresentata dal CSIRT Italia dell'ACN.

Cyber hygiene

Insieme di principi e regole per gli utenti di sistemi informatici, volte a minimizzare i rischi cyber derivanti dal loro utilizzo e che espongono ad attacchi cyber.

Cybersecurity Act

Regolamento (UE) 2019/881, con cui è stato reso permanente il mandato di ENISA, potenziandone i compiti, ed è stato istituito un quadro europeo di certificazione di cybersecurity per prodotti, processi e servizi ICT secondo un approccio comune e armonizzato a livello UE. Ciò al fine di verificare la conformità delle soluzioni ICT in base a specifici requisiti di sicurezza volti a proteggere, per tutto il loro ciclo di vita, la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, delle funzioni e dei servizi da queste offerte o accessibili. Requisiti, questi, che saranno definiti in appositi schemi di certificazione. L'Autorità nazionale di certificazione nell'ambito dei processi di certificazione europea definiti dal Cybersecurity Act è l'Agenzia per la Cybersicurezza Nazionale.

CyberShield

Progetto previsto dalla "EU Cybersecurity Strategy for the Digital Decade" del 16 dicembre 2020, con cui si propone di creare una rete di SOC europei in grado di condividere e correlare in modo più efficiente gli eventi rilevati e di creare analisi di alta qualità sulle minacce, anche impiegando l'intelligenza artificiale e tecniche di machine learning. Lo "EU CyberShield" si completa, poi, con il ruolo degli ISAC e degli CSIRT, così da consentire la segnalazione tempestiva di eventuali incidenti di cybersicurezza alle autorità e a tutti i portatori di interessi coinvolti, in modo tale da ottenere una maggiore consapevolezza situazionale.

CyCLONe

Cyber Crisis Liaison Organisation Network, rete prevista dalla Raccomandazione della Commissione europea 2017/1584 (cd. Blueprint) e volta a garantire la preparazione, la conoscenza situazionale dell'Unione, nonché il raccordo nella gestione delle crisi ed il supporto al decisore politico sia nazionale che europeo. La rete si incardina nel framework delineato dal Blueprint per una risposta coordinata agli incidenti e alle crisi su larga scala organizzando la cooperazione transfrontaliera su tre piani: politico, rappresentato dai dispositivi integrati per la risposta politica alle crisi (IPCR) del Consiglio UE; operativo, da CyCLONe; e tecnico, dalla rete degli CSIRT. In questo contesto, CyCLONe rappresenta l'infrastruttura transfrontaliera utile ad un efficace coordinamento tra il Presidente del NCS e i suoi omologhi negli altri Stati membri. L'Italia è rappresentata dall'ACN.

D

Deepfake

Foto, video e audio creati grazie a software di intelligenza artificiale che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e ad imitare fedelmente una determinata voce.

Digital Innovation Hub (DIH)

Reti di collegamento con il mondo industriale a livello regionale, per facilitare il processo di trasformazione digitale e l'accesso delle imprese al mercato europeo.

E

Edge computing

Forma di elaborazione eseguita in sede o in prossimità di una particolare origine dati, riducendo al minimo la necessità di elaborare i dati in un data center centralizzato.

ENISA (Agenzia europea per la cybersecurity)

Istituita dal Regolamento (UE) 2004/460 al fine di contribuire a sviluppare le capacità e la preparazione cibernetica dell'Unione, promuovendo lo scambio di buone pratiche tra gli Stati membri e la cooperazione operativa tra questi e le istituzioni europee, e fungendo da punto di riferimento per iniziative dell'Unione su questioni di sicurezza cibernetica. Il suo mandato è stato reso permanente ed i suoi compiti sono stati confermati e ampliati, da ultimo, con il Regolamento (UE) 2019/881 (Cybersecurity Act).

F

Fake news

Contenuto informativo falso o distorto, artatamente costruito, il cui deliberato utilizzo è volto ad ottenere un vantaggio politico o finanziario illecito.

Fornitori di Servizi Digitali (FSD)

Persone giuridiche che forniscono un servizio di e-commerce, motore di ricerca online e cloud computing, ai sensi del decreto NIS.

Framework Nazionale per la Cybersecurity e la Data Protection

Strumento operativo per l'organizzazione dei processi e delle strategie volte alla protezione dei dati personali e alla sicurezza cyber delle organizzazioni pubbliche e private, pubblicato dal CIS Sapienza e dal Laboratorio Nazionale di Cybersecurity del CINI.

H

High Performance Computing (HPC)

Sistemi di elaborazione di grande potenza costituiti dalla combinazione di un elevato di numero di nodi di elaborazione.

Hyper SOC

Sistema centralizzato da istituire presso l'ACN per la raccolta, correlazione e analisi di eventi di interesse provenienti dalla constituency di interesse.

I

Impresa 4.0 (Piano nazionale Impresa 4.0)

Il Piano nazionale Impresa 4.0, sviluppato dal MiSE, individua una serie di misure per favorire gli investimenti per l'innovazione e la competitività e per rispondere alle esigenze emergenti dettate dalla globalizzazione e dai cambiamenti tecnologici. Il Piano coinvolge tutti gli aspetti del ciclo di vita delle imprese, offrendo un supporto negli investimenti, nella digitalizzazione dei processi produttivi, nella valorizzazione della produttività dei lavoratori, nella formazione di competenze adeguate e nello sviluppo di nuovi prodotti e processi.

Incidente

Ogni evento con un effetto pregiudizievole per la sicurezza della rete, dei sistemi informativi o dei servizi informatici.

Information Sharing and Analysis Center (ISAC)

Organizzazioni che forniscono una risorsa centrale per la raccolta di informazioni sulle minacce informatiche e consentono la condivisione bidirezionale di informazioni tra il settore privato e quello pubblico su incidenti e minacce, nonché esperienze, conoscenze e analisi.

Intelligenza Artificiale (IA)

Disciplina che si occupa dello studio di funzioni tipiche dell'intelligenza umana e della loro possibile replicazione mediante metodi e strumenti informatici.

Internet Exchange Point (IXP)

Infrastruttura di rete che consente l'interconnessione tra più di due sistemi autonomi indipendenti, principalmente allo scopo di facilitare lo scambio di traffico Internet.

Internet-of-Things (IoT)

Neologismo riferito all'interconnessione di oggetti e dispositivi in grado di trasmettere e ricevere dati su una rete, offrendo un nuovo livello di interazione e di controllo a distanza dei dispositivi. I campi di impiego sono molteplici: dalle applicazioni industriali (processi produttivi), alla logistica e all'infomobilità, dall'efficienza energetica all'assistenza remota, dalla tutela ambientale alla domotica.

Internet Service Provider (ISP)

Soggetto che esercita un'attività imprenditoriale consistente nell'offrire agli utenti la fornitura di servizi inerenti a Internet, quali connettività e posta elettronica.

L

Log

Un log è il risultato di una registrazione sequenziale e cronologica delle operazioni effettuate da un sistema informatico, sia esso un server, un client, un'applicazione o un programma.

M

Machine learning

Il machine learning è una sottocategoria dell'intelligenza artificiale, che automatizza in modo efficiente il processo di costruzione di modelli analitici e consente alle macchine di adattarsi a nuovi scenari in modo autonomo.

Multi-Factor Authentication (MFA)

L'autenticazione a più fattori è quella tecnologia che permette di riconoscere, attraverso più di due metodi di autenticazione, la persona che effettua l'accesso ad un sistema o ad un'applicazione.

O

Operatore di Servizi Essenziali (OSE)

Ai sensi del decreto NIS, gli OSE sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali.

P

Perimetro di sicurezza nazionale cibernetica

Il Perimetro di sicurezza nazionale cibernetica è volto a tutelare la sicurezza nazionale, mirando a un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici da cui dipende l'esercizio di una funzione essenziale o l'erogazione di un servizio essenziale dello Stato ("beni ICT"). Si applica, pertanto, ai beni ICT che i soggetti inclusi nel Perimetro hanno individuato come necessari allo svolgimento di tali funzioni o servizi essenziali e che, in caso di incidente, causerebbero l'interruzione totale o una compromissione degli stessi con effetti irreversibili sotto il profilo dell'integrità o della riservatezza dei dati e delle informazioni.

I soggetti inclusi nel Perimetro sono Amministrazioni pubbliche, enti o operatori pubblici o privati, con sede nel territorio nazionale, che esercitano funzioni essenziali dello Stato o prestano servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, in modalità dipendenti dall'utilizzo di reti, sistemi informativi e servizi informatici.

Piano Nazionale di Ripresa e Resilienza (PNRR)

Piano dell'Italia nell'ambito del programma europeo Next Generation EU, sviluppato a seguito della recessione economica causata dalla pandemia da COVID-19, al fine di prevedere investimenti e riforme per accelerare la transizione ecologica e digitale, migliorare la formazione delle lavoratrici e dei lavoratori, e conseguire una maggiore equità di genere, territoriale e generazionale.

Polo Strategico Nazionale (PSN)

In accordo a quanto definito nella Strategia Cloud Italia, il Polo Strategico Nazionale (PSN) sarà un'infrastruttura, distribuita sul territorio nazionale, gestita da un operatore economico selezionato attraverso un partenariato pubblico-privato e orientata al Cloud, con adeguati livelli di continuità operativa e tolleranza ai guasti.

Obiettivo del PSN è quello di ospitare i dati ed i servizi critici e strategici delle Amministrazioni centrali, delle Aziende Sanitarie Locali (ASL) e delle principali Amministrazioni locali.

Punto di contatto unico NIS (PoC)

A seguito delle modifiche introdotte al decreto NIS dal D.L. 82/2021 (art. 15, co. 1, lett. g), l'ACN è designata quale punto di contatto unico NIS. Il PoC svolge una funzione di collegamento per garantire la cooperazione transfrontaliera dell'Autorità nazionale competente NIS con le autorità competenti degli altri Stati membri, nonché con il Gruppo di Cooperazione NIS – istituito presso la Commissione UE – e lo CSIRT Network.

Q

Quantum computing

Modalità di calcolo, implementata da computer basati sulla meccanica quantistica, in grado di processare, nello stesso momento, attraverso il calcolo parallelo, più soluzioni ad un singolo problema.

S

Security Operation Centre (SOC)

Il SOC è il centro dal quale sono forniti i principali servizi finalizzati alla gestione operativa dei rischi cyber dei sistemi informativi di un'organizzazione. Tipicamente, oltre alle funzioni di monitoraggio e gestione delle componenti di sicurezza, il SOC svolge prime funzioni di valutazione e gestione di eventi di interesse.

Sistema Pubblico di Identità Digitale (SPID)

Il Sistema Pubblico di Identità Digitale è la chiave di accesso ai servizi digitali delle Amministrazioni locali e centrali. Un'unica credenziale (username e password) che rappresenta l'identità digitale e personale di ogni cittadino, con cui è riconosciuto dalla Pubblica Amministrazione per utilizzare in maniera personalizzata e sicura i servizi digitali.

SPID consente anche l'accesso ai servizi pubblici degli Stati membri dell'Unione europea e di imprese o commercianti che l'hanno scelto come strumento di identificazione.

Anche il settore privato può trarre vantaggi dall'identità digitale, migliorando l'esperienza utente e la gestione dei dati personali dei propri clienti.

T

Tavolo interministeriale Perimetro

Istituito con DPCM 30 luglio 2020, n. 131, attuativo del decreto Perimetro. Con il D.L. 82/2021 è stata prevista la sua costituzione presso l'Agenzia per la Cybersicurezza Nazionale. È presieduto dal Direttore Generale dell'ACN ed è composto da due rappresentanti di ciascuna amministrazione CIC, da un rappresentante di AISE e AISI, nonché da due rappresentanti degli altri Ministeri di volta in volta interessati, che sono chiamati a partecipare alle riunioni, anche su loro richiesta, in relazione agli argomenti da trattare. Nello specifico, il CIC si avvale del Tavolo per l'esercizio delle funzioni istruttorie relative all'elencazione dei soggetti inclusi nel Perimetro e ai fini del supporto per ogni altra attività attribuita dal decreto Perimetro allo stesso tavolo interministeriale.

Il Tavolo si riunisce periodicamente ed almeno una volta ogni 6 mesi. Può essere convocato d'iniziativa del presidente o su richiesta di almeno un componente designato, in relazione alla trattazione di specifici argomenti. Possono essere chiamati a partecipare alle riunioni rappresentanti di altre Pubbliche Amministrazioni, nonché di enti e operatori pubblici e privati.

Acronimi

Elenco degli acronimi

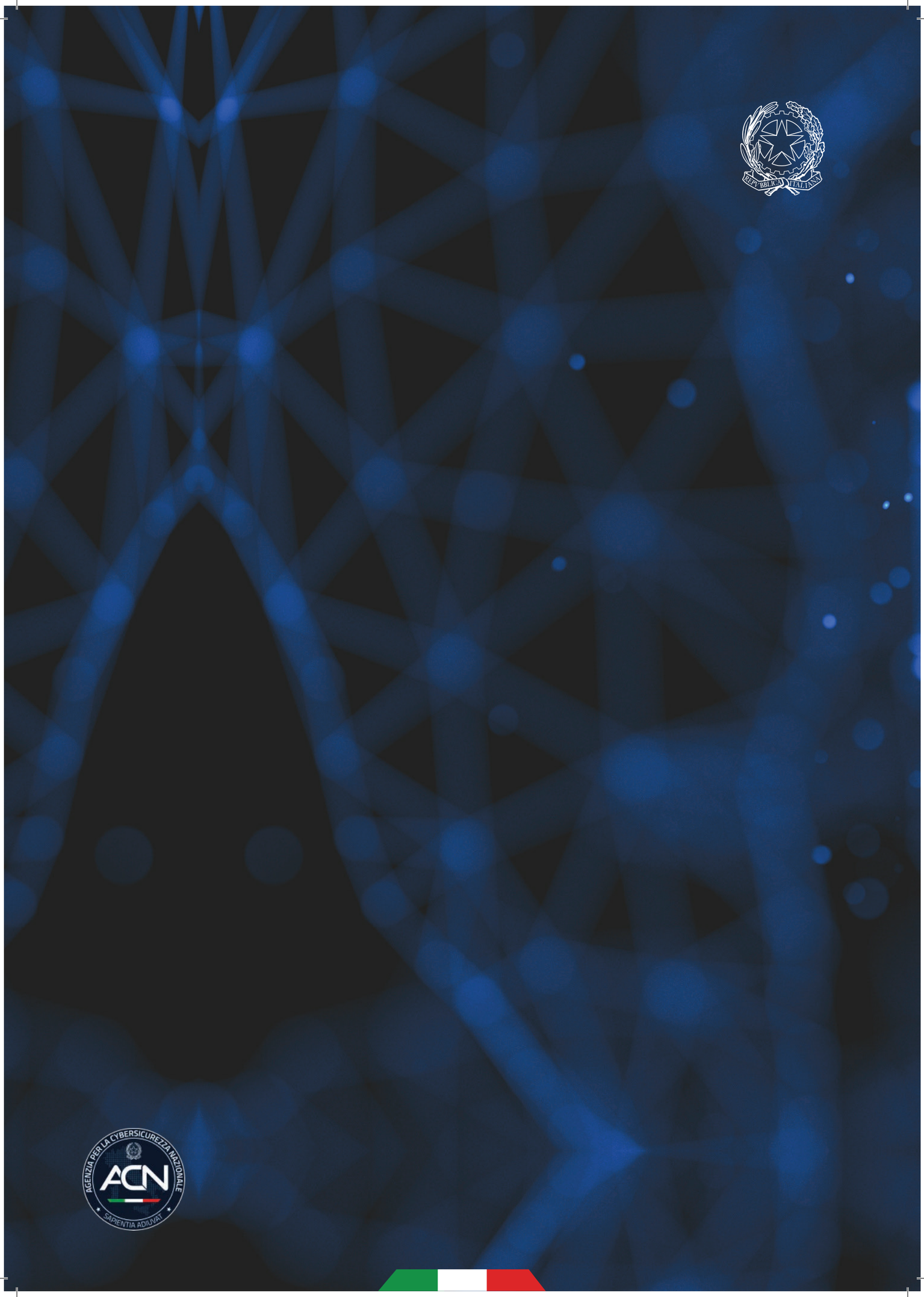
ACN	Agenzia per la Cybersicurezza Nazionale
AGCOM	Autorità per le garanzie nelle comunicazioni
AgID	Agenzia per l'Italia Digitale
AISE	Agenzia Informazioni e Sicurezza Esterna
AISI	Agenzia Informazioni e Sicurezza Interna
BGP	Border Gateway Protocol
CBM	Confidence Building Measure
CERT	Computer Emergency Response Team
CERTFin	CERT Finanziario Italiano
CIC	Comitato Interministeriale per la Cybersicurezza
CINI	Consorzio Interuniversitario Nazionale per l'Informatica
CIS Sapienza	Centro di Ricerca di Cyber Intelligence and Information Security
CISR	Comitato Interministeriale per la Sicurezza della Repubblica
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche della Polizia di Stato
CNR	Consiglio Nazionale delle Ricerche
CONSIP	Concessionaria Servizi Informativi Pubblici
COR	Comando per le Operazioni in Rete
CSIRT	Computer Security Incident Response Team
CSP	Cloud Service Provider
CVCN	Centro di Valutazione e di Certificazione Nazionale
CV	Centro di Valutazione
CyCLONe	Cyber Crisis Liaison Organisation Network
DIE	Dipartimento per l'Informazione e l'Editoria

DIH	Digital Innovation Hub
DIS	Dipartimento delle Informazioni per la Sicurezza
DL	Decreto-Legge
DNS	Domain Name System
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
DTD	Dipartimento per la Trasformazione Digitale
ECCC	Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca (European Cybersecurity Competence Centre)
ENISA	Agenzia dell'Unione Europea per la Cybersicurezza
FSD	Fornitori di Servizi Digitali
G7	Gruppo dei Sette
GDPR	Regolamento Generale sulla Protezione dei Dati (General Data Protection Regulation)
HPC	High Performance Computing
IA	Intelligenza Artificiale
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technologies
IoT	Internet of Things
IPCR	Integrated Political Crisis Response
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
ISTAT	Istituto Nazionale di Statistica
ITASEC	Italian Conference on Cybersecurity
ITS	Istituti Tecnici Superiori
IXP	Internet Exchange Point
KPI	Key Performance Indicator

MAECI	Ministero degli Affari Esteri e della Cooperazione Internazionale
MEF	Ministero dell'Economia e delle Finanze
MiSE	Ministero dello Sviluppo Economico
MITD	Ministro per l'Innovazione tecnologica e la Transizione Digitale
MFA	Multi-Factor Authentication
MPA	Ministro per la Pubblica Amministrazione
MUR	Ministero dell'Università e della Ricerca
NATO	North Atlantic Treaty Organization
NCC	Centro Nazionale di Coordinamento (National Coordination Centre)
NCS	Nucleo per la Cybersicurezza
NIS	Network and Information Security
OSCE	Organizzazione per la Sicurezza e la Cooperazione in Europa
OSE	Operatori di Servizi Essenziali
PA	Pubblica Amministrazione
PaaS	Platform-as-a-Service
PCM	Presidenza del Consiglio dei Ministri
PMI	Piccole e Medie Imprese
PNRR	Piano Nazionale di Ripresa e Resilienza
PoC NIS	Punto di contatto unico NIS
PSIRT	Product Security Incident Response Team
PSN	Polo Strategico Nazionale
PSNC	Perimetro di sicurezza nazionale cibernetica
RIS	Reparto Informazioni e Sicurezza
SaaS	Software-as-a-Service
SMD	Stato Maggiore della Difesa

SOC	Security Operation Center
SPID	Sistema Pubblico di Identità Digitale
TLD	Top Level Domain
UCSe	Ufficio Centrale per la Segretezza
UE	Unione Europea

Strategia
Nazionale di Cybersicurezza


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADJUVAT