ATTI PARLAMENTARI

XIX LEGISLATURA

CAMERA DEI DEPUTATI

Doc. CCXVIII
n. 3

R E L A Z I O N E

SULL'ATTIVITÀ SVOLTA DALL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE

(Anno 2023)

(Articolo 14, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni, dalla legge 4 agosto 2021, n. 109)

Presentata dal Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri

(MANTOVANO)

Trasmessa alla Presidenza il 23 aprile 2024

PAGINA BIANCA

RELAZIONE ANNUALE AL PARLAMENTO 2023

SOMMARIO

PREFAZIONE

Come per larga parte delle Nazioni Occidentali, per l'Italia il 2023 è stato un anno di pesanti e diversificate aggressioni alla sicurezza cyber, che spesso hanno proceduto in parallelo ai conflitti in corso in Ucraina e in Medio Oriente.

Lo spostamento delle nostre vite nel cyberspazio, soprattutto dopo il massiccio ricorso allo spazio virtuale durante la pandemia, ha accresciuto la pericolosità degli attori ostili, e in più occasioni ha messo a rischio la possibilità per i cittadini di fruire di servizi essenziali, in primis quelli sanitari.

In un simile scenario, porre in sicurezza gli interessi nazionali nel campo cyber richiede capacità tecniche e strategiche elevate, che fronteggino l'uso sempre più devastante della tecnologia da parte sia di entità statali o parastatali che hanno interessi contrapposti ai nostri, sia di bande criminali o di singoli hacker.

Tutto questo rende indispensabile uno sforzo condiviso, che faccia convergere le migliori competenze e risorse della Nazione, e assicuri la preparazione più adeguata alle minacce informatiche di oggi e di domani. Va rafforzata e affinata la capacità di reagire in caso di attacco; al tempo stesso, lavoriamo per far crescere il livello di resilienza della comunità nel suo complesso.

Lo sforzo dell'Italia si inserisce poi in un quadro di collaborazione europea e internazionale, nella convinzione che la dimensione digitale, trasversale rispetto a ogni segmento della vita istituzionale e sociale, richieda oggi un impegno deciso. La cybersicurezza rappresenta peraltro tema qualificante della Presidenza italiana del G7 per il 2024, insieme a quello dell'Intelligenza Artificiale.

L'impegno del Governo si è declinato anche sul piano normativo: il Consiglio dei ministri ha varato un disegno di legge, oggi all'esame del Parlamento, che aggiorna il quadro giuridico nazionale della cybersicurezza.

In tal senso, è importante il contributo dell'Agenzia per la cybersicurezza nazionale, la cui relazione annuale illustra, nei termini che seguono, le sfide in atto, le azioni per affrontarle e quanto va fatto in più e di più.

Alfredo Mantovano

INTRODUZIONE

In un contesto in cui le minacce informatiche sono in costante aumento e interessano sempre più da vicino le vite di numerosi cittadini, nonché le funzioni essenziali dello Stato, la cybersicurezza diventa cruciale per garantire l'interesse del Paese.

La pervasività crescente delle tecnologie digitali che, a ritmi sempre più sostenuti, stanno rivoluzionando il nostro modo di amministrare, di fare impresa, di vivere la quotidianità e di esercitare i diritti fondamentali, richiede un impegno deciso a sostegno della sicurezza cibernetica. Non si può restare indietro in un panorama tecnologico in costante evoluzione, dove l'avvento di tecnologie dirompenti, come l'intelligenza artificiale e il calcolo quantistico, si accompagna alla transizione di una considerevole mole di dati, anche sensibili, su infrastrutture cloud.

È per questo che l'Agenzia per la cybersicurezza nazionale è in prima linea per accompagnare il Paese in uno sforzo multidimensionale volto ad assicurare una maggiore sicurezza e resilienza cibernetica. La presente relazione illustra le modalità con cui è stata portata avanti questa missione.

Proteggere infrastrutture e sistemi informatici richiede il costante monitoraggio delle attività malevole, l'intervento in caso di incidente e la condivisione informativa in merito ad attacchi e vulnerabilità.

Ciò consente, da un lato, di prevenire l'insorgere di minacce cyber che possano generare danni significativi e, dall'altro, di essere meglio preparati per farvi fronte.

Altrettanto indispensabile, a tale riguardo, è l'utilizzo di reti e sistemi sicuri, specialmente se sono funzionali all'operatività delle infrastrutture cruciali per la tenuta del Sistema Paese.

L'Agenzia sta contribuendo a gestire la minaccia cyber a tutela degli interessi nazionali nello spazio cibernetico, mettendo in atto un coordinamento istituzionale capace di anticipare e rispondere a minacce sistemiche. Sta inoltre coltivando ogni possibile sinergia con gli operatori privati, con le amministrazioni pubbliche e con il mondo dell'università, della ricerca e dell'innovazione, così da promuovere, a tutti i livelli, un innalzamento della postura di cybersicurezza che contribuisca a ridurre le vulnerabilità e prevenire eventuali rischi.

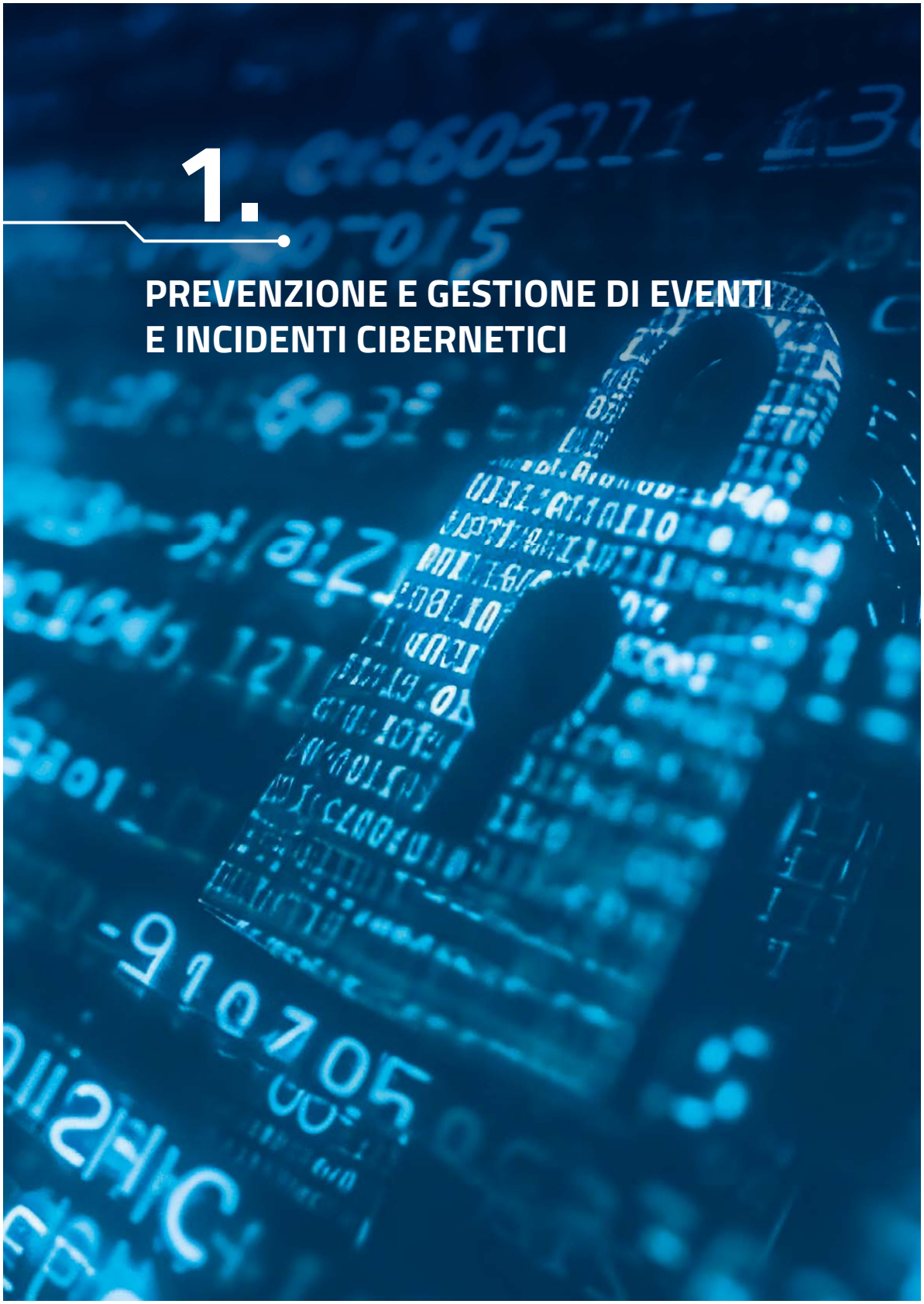
Lo sviluppo di un ecosistema della cybersicurezza all'avanguardia può basarsi, infatti, solamente su un costante scambio con tutti questi attori, che favorisca l'emergere di soluzioni tecnologiche innovative, a sostegno dell'autonomia tecnologica nazionale ed europea.

Particolare attenzione va poi dedicata alla formazione, non solo per incoraggiare la crescita di lavoratori qualificati, ma anche per allargare la conoscenza dalla scuola primaria fino ai percorsi professionalizzanti per chi è già impiegato. Oltre agli specialisti, è però indispensabile approfondire la consapevolezza cyber di base di tutti i cittadini, così da garantire la pervasività della resilienza attraverso una maggiore attenzione al tema e pratiche di igiene digitale più diffuse.

Grazie a una visione di lungo periodo e al sostegno del Governo, l'ACN sta dando il proprio contributo, in collaborazione con gli altri attori interessati, per raggiungere gli obiettivi specificati dalla Strategia nazionale di cybersicurezza.

Lungo queste direttrici si è articolata, nel corso del 2023, l'attività dell'Agenzia per la cybersicurezza nazionale, che sta avanzando nel suo percorso verso la piena operatività, dotandosi di competenze, strumenti e procedure per assolvere al meglio alle sue funzioni istituzionali.

Bruno Frattasi



1. PREVENZIONE E GESTIONE DI EVENTI E INCIDENTI CIBERNETICI

Nel corso del 2023, in un contesto caratterizzato dal considerevole incremento della minaccia *cyber*, l'Agenzia per la cybersicurezza nazionale (ACN) ha rafforzato il proprio impegno per garantire la diffusione di informazioni sui rischi *cyber* oltre che per fornire assistenza alle vittime. Attraverso la sua articolazione tecnico-operativa, il CSIRT Italia, l'Agenzia ha potuto monitorare l'evoluzione della minaccia, caratterizzata sempre più da eventi di tipo *ransomware* e DDoS – ma anche diffusione di *malware* via e-mail e *phishing* – e indirizzata a diverse realtà pubbliche oltre che ad aziende attive nei settori più disparati (primi fra tutti telecomunicazioni, trasporti e servizi finanziari).

Grazie anche a un'opera di rilevamento, analisi e allertamento su possibili attacchi e vulnerabilità, è stata portata avanti una costante e puntuale attività di prevenzione, non disgiunta dal supporto in caso di incidenti; in questi ultimi casi, i tecnici dell'Agenzia intervengono, sia da remoto che *in loco*, per aiutare i soggetti colpiti nella gestione degli incidenti.

In tale contesto, le periodiche riunioni del Nucleo per la cybersicurezza hanno consentito all'Agenzia di assicurare la condivisione informativa in merito allo stato della minaccia *cyber*, nonché il coordinamento interistituzionale a livello tecnico-operativo tra le varie amministrazioni coinvolte. A livello europeo, l'ACN ha contribuito al consolidamento dei meccanismi europei per la prevenzione e preparazione alle crisi cibernetiche, attraverso la partecipazione alla rete CyCLONe e alle numerose esercitazioni.

1.1 I NUMERI DEL CSIRT ITALIA

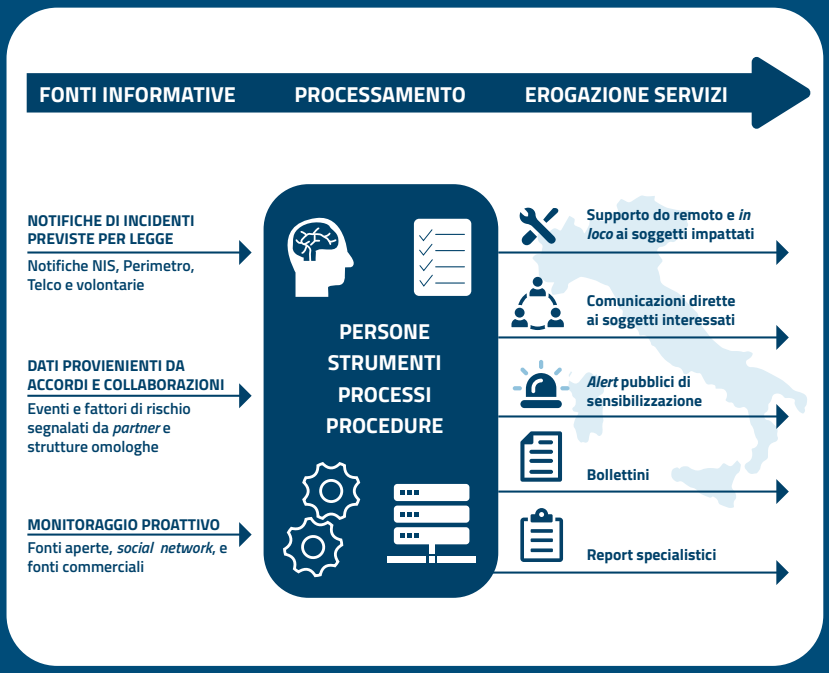
Le attività operative dell'Agenzia, sia nella fase preventiva di monitoraggio, analisi delle minacce e allertamento dei soggetti esposti ai rischi, sia nella fase reattiva di risposta agli incidenti, hanno subito nel 2023 un notevole incremento in termini numerici rispetto all'anno precedente, indice di un generale aumento delle attività *cyber*, rilevato anche a livello europeo e globale.

METODOLOGIA

Il *Computer Security Incident Response Team* (CSIRT) nazionale, CSIRT Italia, in quanto *hub* nazionale, riceve le notifiche obbligatorie e volontarie di incidenti cibernetici previste dalla normativa di riferimento (D.L. n. 105/2019 e relativi provvedimenti attuativi in materia di Perimetro di sicurezza nazionale cibernetica, D.Lgs. n. 65/2018, di attuazione della Direttiva NIS e Decreto del Ministro dello sviluppo economico del 12 dicembre 2018, c.d. Decreto Telco). Il CSIRT Italia, accreditato alle reti internazionali FIRST e *Trusted Introducer*, esamina e raffronta, inoltre, informazioni provenienti da fonti aperte, chiuse e commerciali, nonché da altre strutture omologhe nazionali e internazionali.

Tutte le informazioni raccolte dal CSIRT Italia vengono studiate e valorizzate dagli operatori i quali, nella cosiddetta fase di *triage,* le analizzano e classificano come eventi *cyber,* eseguendo, quindi, diverse attività a seconda del soggetto impattato e del tipo di evento. In particolare, il CSIRT Italia:

- approfondisce le informazioni a disposizione, analizzando i contenuti anche dal punto vista strettamente tecnico, ad esempio studiando i *malware*, valutando il rischio d'impatto sistemico di vulnerabilità e incidenti;
- se necessario, invia richieste di informazioni ai soggetti;
- fornisce supporto da remoto o *in loco* ai soggetti impattati;
- invia comunicazioni ai soggetti impattati, nonché a tutti i soggetti potenzialmente impattati da eventi *cyber* o da altri fattori di rischio individuati dalle attività di monitoraggio;
- pubblica *alert* o bollettini sul sito web www.csirt.gov.it e sui propri canali *social.*



DEFINIZIONI

- ***Asset* a rischio:** sistemi o servizi esposti su Internet da soggetti italiani, rilevati dalle attività di monitoraggio proattivo e per i quali vengono inviate specifiche comunicazioni.
- ***Case*:** un avvenimento d'interesse per il CSIRT Italia, opportunamente approfondito al fine di identificare il possibile impatto e valutare la necessità di azioni di resilienza. I *case* possono diventare eventi *cyber*.
- **Comunicazione inviata:** *alert*, anche massivi, inviati a Pubbliche Amministrazioni e soggetti privati potenzialmente interessati da eventi *cyber*.
- **Comunicazione ricevuta:** e-mail ricevute dal CSIRT Italia relative a informazioni contenenti profili di natura *cyber* anche generiche, sottoposte a valutazione preliminare (*triage*) per determinare l'apertura o meno di un *case*.
- ***Constituency*:** insieme dei soggetti nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli incidenti di sicurezza informatica.
- **Evento *cyber*:** *case* con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, il CSIRT Italia dirama *alert* e/o supporta, eventualmente anche *in loco*, i soggetti colpiti.
- **Incidente:** un evento *cyber* con impatto su confidenzialità, integrità o disponibilità delle informazioni confermato dalla vittima.
- **Portale di *collaboration*:** portale riservato ai membri della *constituency* del CSIRT Italia; costituisce lo strumento privilegiato per favorire lo scambio di informazioni tecniche specifiche con i soggetti accreditati.
- **Portale pubblico:** sito web del CSIRT Italia accessibile all'intera comunità.
- **Richiesta di informazioni:** richiesta effettuata dal CSIRT Italia al soggetto potenzialmente impattato da un evento *cyber* per acquisire ulteriori elementi, ad esempio la conferma di una possibile compromissione (e la conseguente classificazione dell'evento *cyber* quale incidente).
- **Segnalazione:** comunicazione prevista per legge per i soggetti appartenenti al Perimetro di sicurezza nazionale cibernetica (PSNC), per gli operatori di servizi essenziali e fornitori di servizi digitali (Direttiva NIS), e per gli operatori del settore comunicazione (Decreto Telco). Le segnalazioni vengono trattate direttamente come eventi *cyber*.
- ***Triage*:** fase in cui gli operatori analizzano le segnalazioni, le comunicazioni ricevute e ogni possibile evento *cyber* di cui il CSIRT Italia venga a conoscenza, anche a seguito di attività di monitoraggio proattivo, al fine di identificare i potenziali impatti e classificare quindi l'informazione come evento *cyber*, proseguendo o meno con le ulteriori fasi di trattazione.

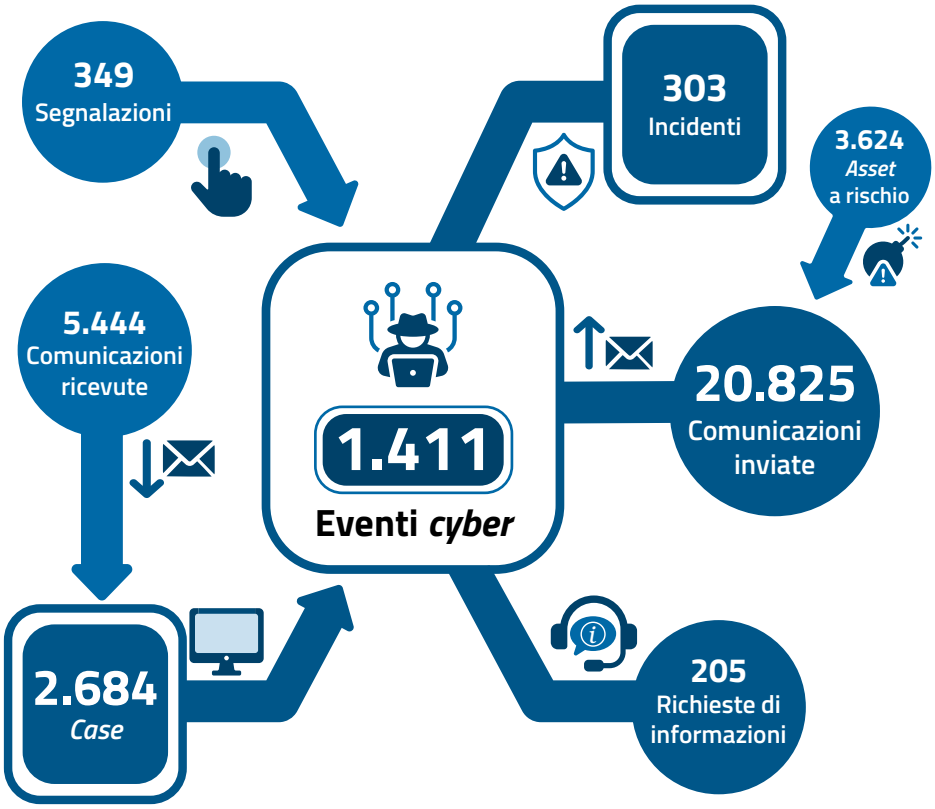


Figura 1 – Riepilogo dello stato della minaccia *cyber* in Italia

Nel box che segue sono riassunti i numeri delle principali attività svolte dal CSIRT Italia nel 2023 e si confrontano alcuni dei numeri relativi alle funzioni di gestione eventi, allertamento e monitoraggio con quelli del 2022.

Dai dati emerge chiaramente un sensibile aumento delle segnalazioni indirizzate all'Agenzia; si nota, inoltre, che a fronte di un numero di comunicazioni ricevute sostanzialmente allineato a quello del 2022, sono aumentati di circa il 30% il numero di eventi *cyber* e più

ATTIVITÀ E NUMERI DEL CSIRT ITALIA 2023

Gestione eventi

- **1.411 eventi** *cyber* gestiti
- **3.302 soggetti *target***
- **303 incidenti con impatto confermato**
- **13 interventi *in loco*** a supporto della vittima
- **31 interventi da remoto**

Allertamento

- **20.825 comunicazioni** inviate ai soggetti
- **447 *alert* e bollettini** pubblicati sul **portale pubblico**
- **72** pubblicati sul **portale di *collaboration***
- **468 stime di impatto di nuove vulnerabilità**
- **180.000+ indicatori di compromissione** condivisi

Monitoraggio sistemi italiani

- **3.624 dispositivi e servizi** a rischio segnalati ai soggetti
- **584 tentativi di *phishing* segnalati** alle vittime

Monitoraggio attori *cyber*

- **56 attori *ransomware*** monitorati
- **265 hacktivisti** monitorati

Analisi minacce

- **15** campagne **APT**
- **100 *malware*** analizzati
- **55 report specialistici**

Documenti di analisi dati

- **6 *Operational Summary*** sullo stato della minaccia in Italia
- **472 bollettini di approfondimento** su mitigazione minacce specifiche

		2022	2023	variazione percentuale
Gestione eventi	Segnalazioni	81	349	+330,9%
	Comunicazioni ricevute	5.974	5.444	-8,9%
	Case	2.643	2.684	+1,6%
	Eventi *cyber*	1.094	1.411	+29,0%
	Incidenti	126	303	+140,5%
	Interventi *in loco*	10	13	+30,0%
	Soggetti *target*	1.150	3.302	+187,1%
Allertamento	*Alert* e bollettini portale pubblico	410	447	+9,0%
	Alert e bollettini portale di *collaboration*	38	72	+89,5%
	Richieste di informazioni	185	205	+10,8%
Monitoraggio	*Asset* a rischio	764	3.624	+374,3%

che raddoppiati gli incidenti. Nel 2023 sono stati 3.302 i soggetti italiani *target* di eventi *cyber* individuati dal CSIRT Italia, a fronte dei 1.150 del 2022. L'aumento del numero di *asset* a rischio è da ascrivere all'incremento delle capacità di monitoraggio dell'ACN, che permettono ora di individuare, oltre agli *asset* potenzialmente compromessi, anche quelli potenzialmente vulnerabili.

A tutto ciò si accompagnano le attività di allertamento svolte dall'Agenzia effettuate per segnalare eventuali compromissioni o fattori di rischio ai soggetti monitorati. Ciò sia tramite il portale pubblico, sia attraverso il portale di *collaboration* ad accesso riservato, dove, in particolare, gli *alert* e i bollettini sono quasi raddoppiati.

1.2 ANALISI DEGLI EVENTI

Nel corso del 2023 il CSIRT Italia ha trattato 1.411 eventi *cyber,* per una media di circa 117 al mese, con un picco di 169 a ottobre. Di questi, 303 sono stati classificati come incidenti, per una media di circa 25 al mese (Figura 2).

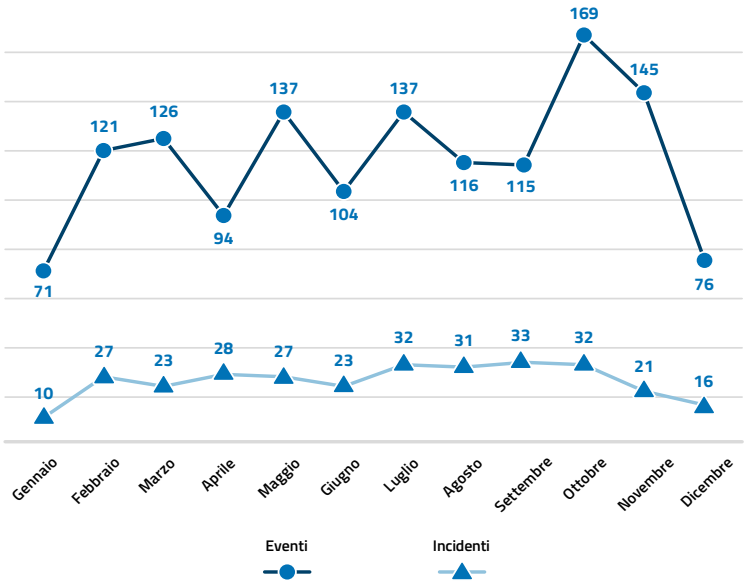


Figura 2 – Distribuzione temporale degli eventi e incidenti con impatto sul territorio nazionale nel 2023

Dall'analisi e successiva classificazione dei 1.411 eventi *cyber* è stato possibile individuare le tipologie riportate in Figura 3. Per una corretta lettura del dato, si noti che ognuno

di tali eventi può essere stato associato a una o più tipologie: ad esempio, un evento di *phishing* spesso è finalizzato anche alla diffusione di un *malware*, che può essere a sua volta un evento di tipo *ransomware*.

Phishing

Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (user ID, password, numeri di carte di credito, PIN) con l'invio di false e-mail generiche a un gran numero di indirizzi. Le e-mail sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. L'attaccante utilizza i dati carpiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Malware

Programma inserito in un sistema informatico, generalmente in modo abusivo e occulto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

Ransomware

In questo tipo di minaccia l'attaccante, di regola, si introduce nei sistemi di un privato o di un'organizzazione per cifrarne i dati, al fine di ottenere il pagamento di un riscatto per rendere nuovamente disponibili i dati al legittimo proprietario e/o non diffonderli pubblicamente.

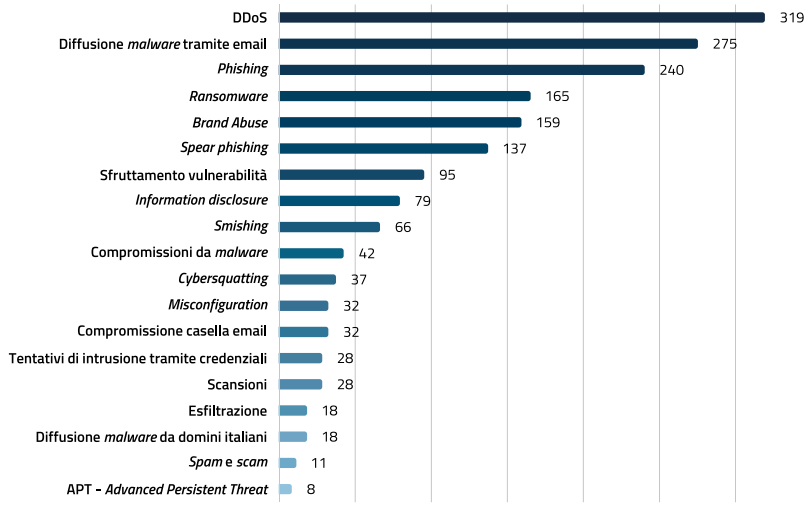


Figura 3 – Tipologia di eventi *cyber* trattati nel 2023

Per quanto riguarda i settori di attività dei soggetti *target*[1], prevalgono le telecomunicazioni e la Pubblica Amministrazione (PA), sia a livello locale che centrale (Figura 4). Anche in questo caso, per interpretare correttamente il dato, è importante sottolineare che ciascun evento può essere associato a uno o più settori di attività.

[1] Non sono stati considerati gli eventi rilevati a seguito di monitoraggio proattivo, per non creare sbilanciamenti verso quei settori più interessati da tale attività.

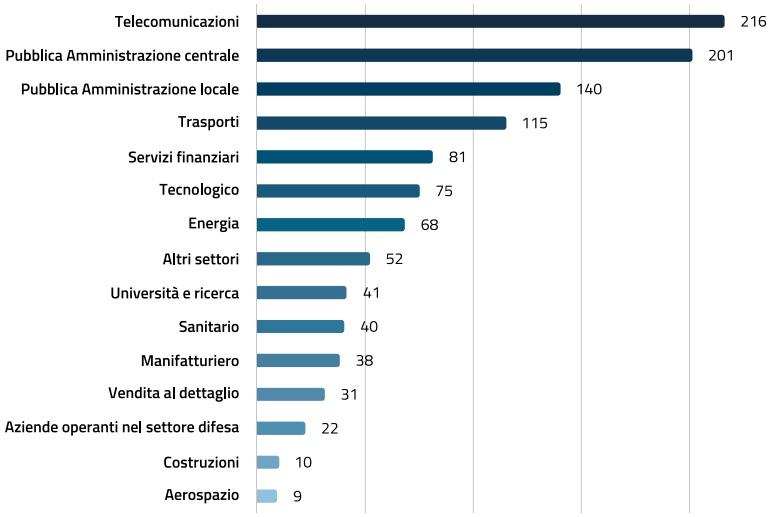


Figura 4 – Eventi *cyber* trattati nel 2023 per settore *target*

In Figura 5 si riporta, invece, la distribuzione dal punto di vista geografico dei soggetti impattati dagli eventi cibernetici.

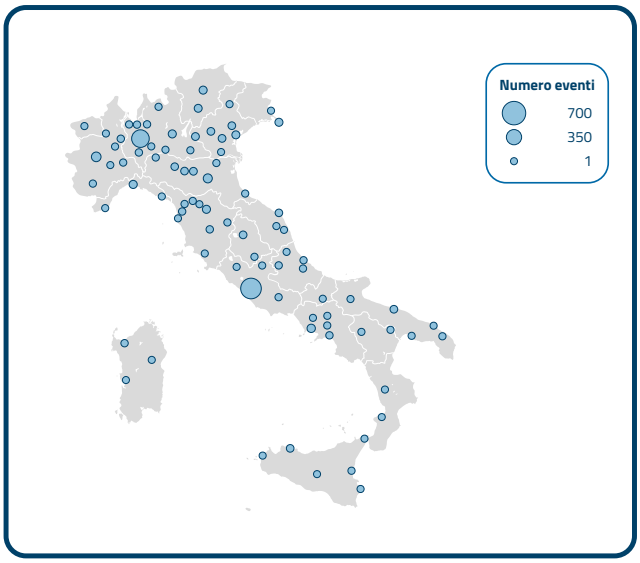


Figura 5 – Distribuzione geografica dei soggetti impattati dagli eventi *cyber* trattati nel 2023

1.2.1 FOCUS SULLE ATTIVITÀ CONNESSE AI CONFLITTI IN CORSO. IL *CYBER* ATTIVISMO

L'acutizzarsi delle tensioni geopolitiche, relative sia al perdurare della guerra tra Russia e Ucraina sia al mutamento degli equilibri in Medio Oriente a seguito degli attentati di Hamas ai danni di Israele, hanno visto l'ascesa di un fenomeno *cyber* prima di allora estremamente poco significativo: il *cyber* attivismo. Con tale denominazione si fa riferimento a gruppi che hanno lo scopo di sostenere la causa di una delle parti in conflitto attraverso azioni *cyber* malevole con impatti chiaramente visibili, rivendicati successivamente dal gruppo stesso. Si tratta principalmente di eventi di tipo DDoS a danno di siti web di Pubbliche Amministrazioni e imprese e, in numero esiguo (24 eventi), di tipo *defacement*, ossia intrusioni informatiche che consistono nel modificare pagine di siti web (in genere obsoleti e poco protetti), sostituendole con un messaggio di rivendicazione, di apologia e simili. Proprio a causa del *cyber* attivismo legato ai conflitti in corso, si è avuto un significativo aumento degli eventi DDoS. Infatti, nel 2023 sono stati rilevati 319 eventi DDoS, con un incremento rispetto al 2022 del 625% (Figura 6).

DDoS

Gli eventi DDoS (Distributed Denial of Service) mirano a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria. L'effetto più immediato di tale tipologia di attacco è l'indisponibilità del sito o del servizio colpito.

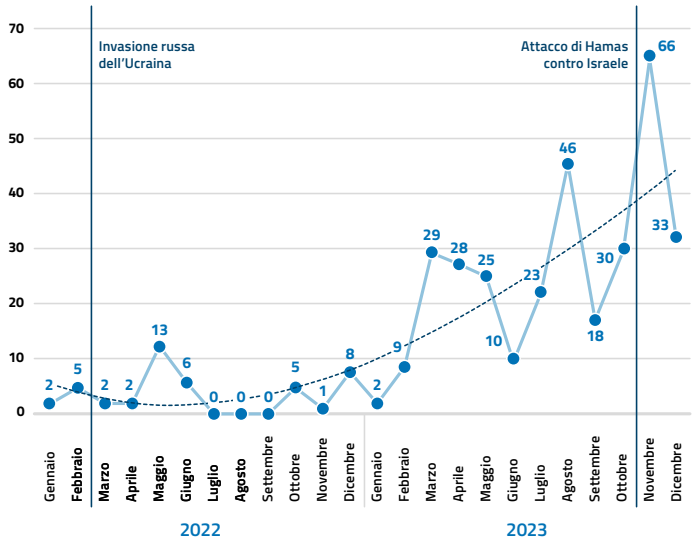


Figura 6 – Numero di eventi di tipo DDoS gestiti dall'Agenzia nel 2022 e 2023

La maggior parte degli eventi (248) è stata rivendicata da collettivi filorussi, mentre un gruppo filopalestinese ha condotto una singola campagna con 15 attacchi DDoS. I restanti eventi DDoS, non essendo stati rivendicati, non possono essere associati a specifiche compagini o ricondotti ai conflitti in atto.

Il CSIRT Italia ha effettuato campagne di allertamento per i soggetti obiettivo dei DDoS, indicando loro contromisure di mitigazione specifiche per gli attacchi in corso, oltre a pubblicare sul portale pubblico bollettini dedicati. Ha inoltre proseguito le attività di sensibilizzazione, avviate nel 2022, al fine di elevare il livello di allerta degli operatori pubblici e privati su potenziali effetti di *spillover* di incidenti, ovvero infezioni di soggetti operanti sui territori coinvolti nei conflitti e con i quali aziende italiane condividono reti e sistemi.

Per quanto riguarda i soggetti interessati da DDoS nel 2023, questi sono stati principalmente Pubbliche Amministrazioni centrali e aziende del settore dei trasporti e dei servizi finanziari (Figura 7). Leggendo il dato complessivo emerge, tuttavia, come il DDoS si sia concentrato in prevalenza su soggetti privati (Figura 8).

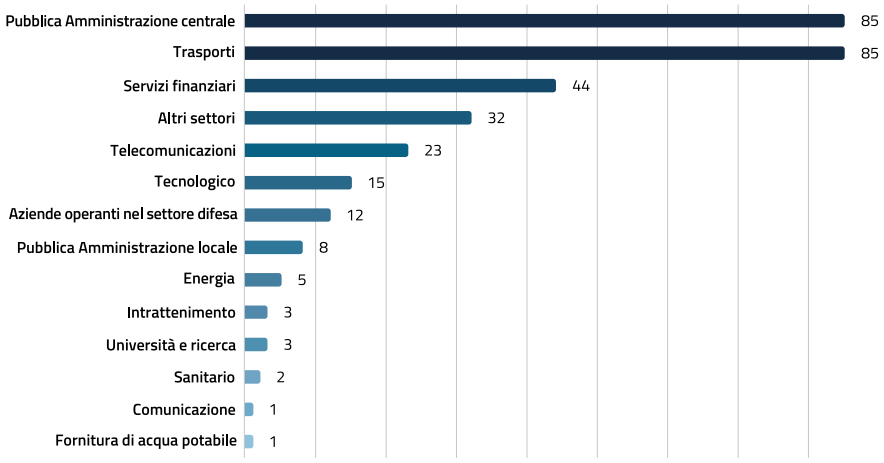


Figura 7 – Numero di eventi DDoS per settore di attività economica del soggetto interessato

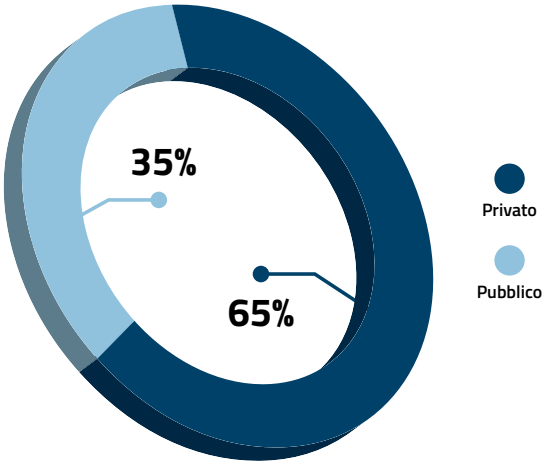


Figura 8 – Eventi DDoS per tipologia di soggetto interessato

Dal monitoraggio delle piattaforme utilizzate dagli attaccanti per le rivendicazioni degli eventi DDoS, è stato rilevato, inoltre, che l'Italia è il sesto Paese al mondo più interessato da questi eventi e il terzo tra i Paesi UE (Figura 9).

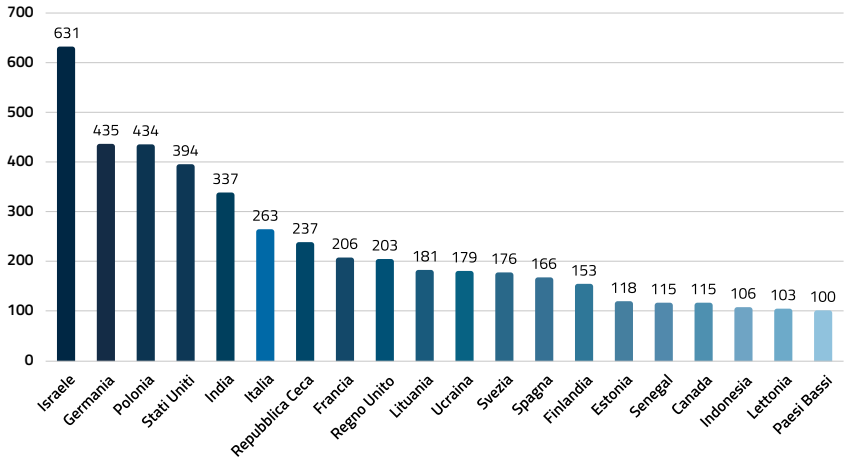


Figura 9 – Numero di rivendicazioni di DDoS per Paese

1.2.2 EVENTI *RANSOMWARE*

Anche nel 2023, il *ransomware* si è confermato quale minaccia maggiormente significativa, soprattutto alla luce dell'impatto che ha avuto a livello nazionale. L'Agenzia ha osservato 165 eventi diretti verso operatori privati e PA, con un incremento percentuale del 27% rispetto al 2022. La distribuzione temporale dei *ransomware* seguiti dal CSIRT Italia è mostrata in Figura 10.

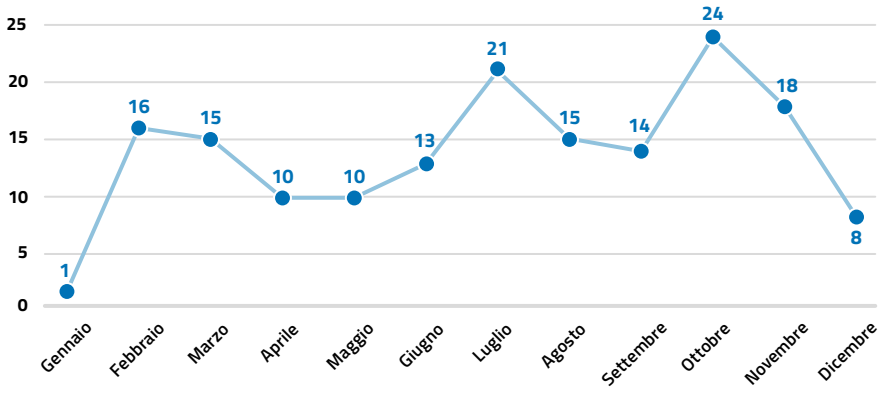


Figura 10 – Numero di eventi di tipo r*ansomware* seguiti dall'Agenzia nel 2023

È da ritenere, tuttavia, che il dato rappresenti solo una parte del numero complessivo di attacchi *ransomware* effettivamente avvenuti, tenuto conto che le vittime, spesso sprovviste di *know-how* e strutture interne dedicate – in particolare le piccole e medie imprese (PMI) – talvolta non segnalano l'evento; ciò di fatto impedisce non solo che esso venga pubblicamente conosciuto, ma anche che vi sia posta la dovuta attenzione da parte delle istituzioni preposte a monitorare e contrastare il fenomeno.

Anche nel caso dei *ransomware*, nella grande maggioranza dei casi (84%) le vittime appartengono al settore privato. Per quanto attiene alla dimensione aziendale dei soggetti privati colpiti, circa il 23% degli eventi *ransomware* ha interessato grandi imprese, mentre in oltre il 75% dei casi sono state coinvolte piccole (46,3%) e medie imprese (30,6%) (Figura 11).

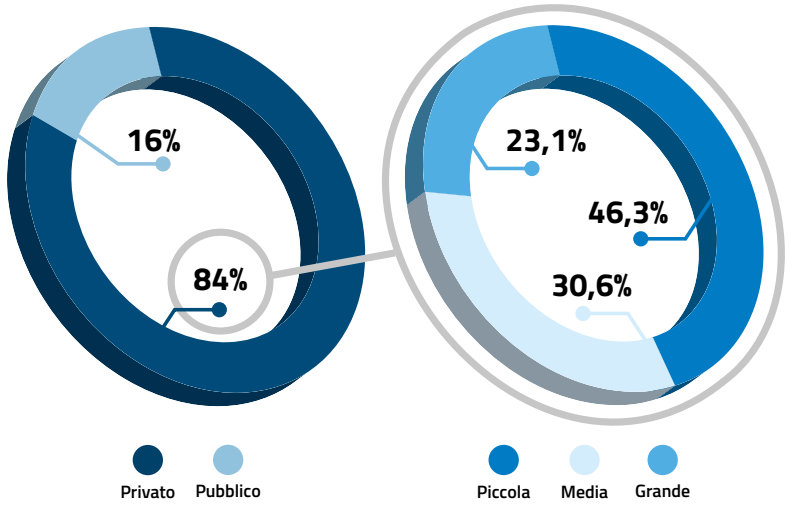


Figura 11 – Eventi *ransomware* per tipologia di vittima e dimensione aziendale

Classificando, ove possibile, le vittime in base ai settori di attività economica, emerge come quello manifatturiero sia stato il più colpito, in continuità con il 2022, seguito, quest'anno, dalla vendita al dettaglio e dai settori sanitario e tecnologico (Figura 12).

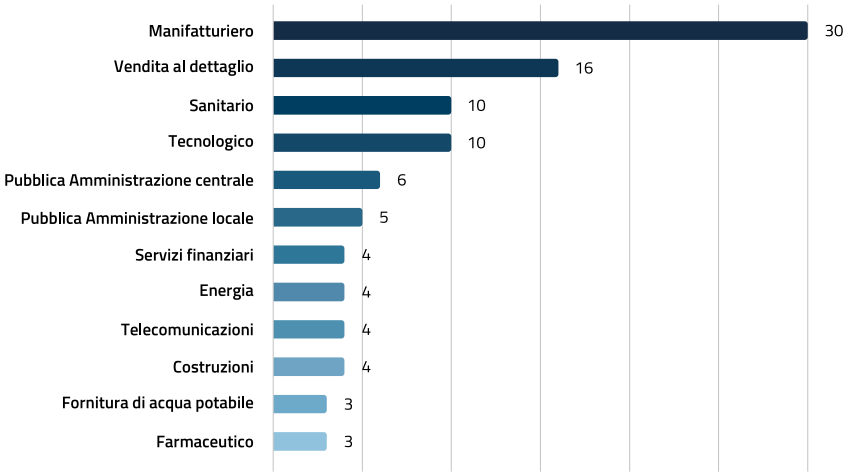


Figura 12 – Numero di eventi *ransomware* per settore di attività economica della vittima

Da un punto di vista geografico, le zone più interessate dal fenomeno corrispondono alle aree metropolitane di Roma e Milano e ai distretti industriali del Nord-Ovest e Nord-Est (Figura 13). Ciò è presumibilmente determinato dalla maggiore presenza, in tali zone, di imprese operanti nel settore manifatturiero.

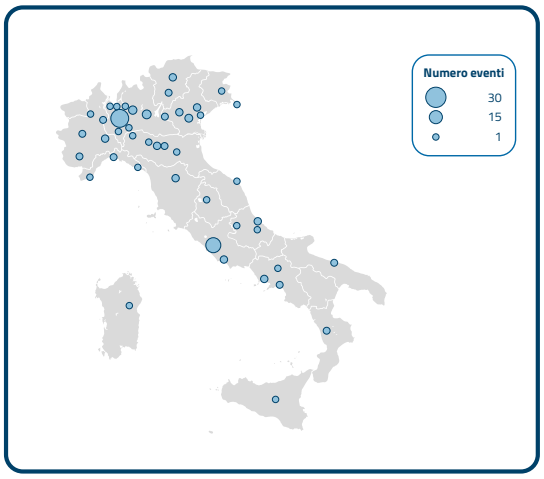


Figura 13 – Distribuzione geografica delle vittime di eventi *ransomware*

Con riferimento ai *threat actor*, nel 2023 gli attacchi sono stati principalmente condotti da 20 diversi gruppi, tra i quali i più attivi sono risultati LockBit 3.0, LockBit (come già rilevato nel 2022) e NoEscape (Figura 14).

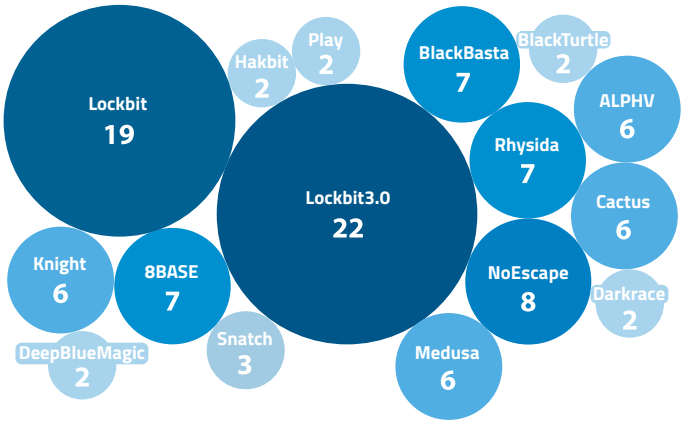


Figura 14 – Gruppi *ransomware* responsabili degli eventi trattati dall'ACN

Nel 2023 l'Italia è risultata il terzo Paese dell'Unione europea più colpito da *ransomware*, mentre a livello globale è stato il sesto Paese più colpito (Figura 15).

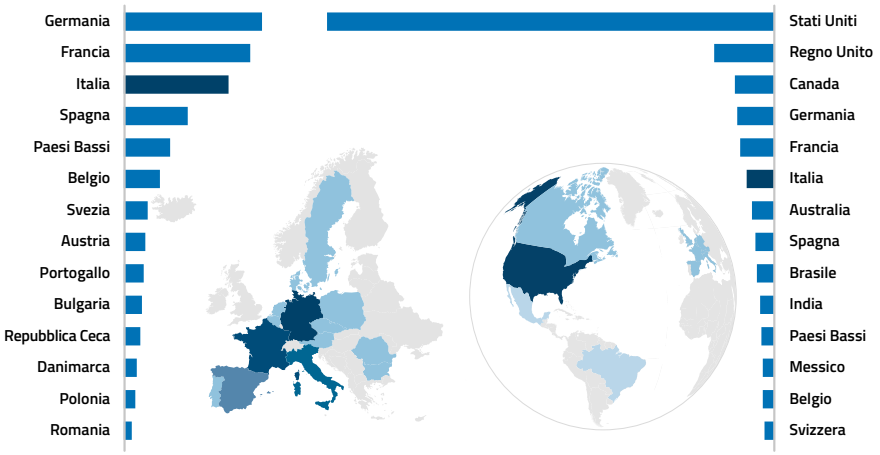


Figura 15 – *Ransomware* nell'UE e nel mondo

1.2.3 FOCUS SULLA PUBBLICA AMMINISTRAZIONE

Nel corso del 2023, l'ACN ha gestito 422 eventi *cyber* ai danni di istituzioni pubbliche nazionali, in sensibile aumento rispetto ai 160 del 2022. Di questi eventi, 85 sono stati classificati come incidenti (nel 2022 furono 57), procurando nella maggior parte dei casi il malfunzionamento dei sistemi e conseguenti blocchi o rallentamenti nell'erogazione dei servizi. La distribuzione di tali eventi nella Pubblica Amministrazione è rappresentata in Figura 16.

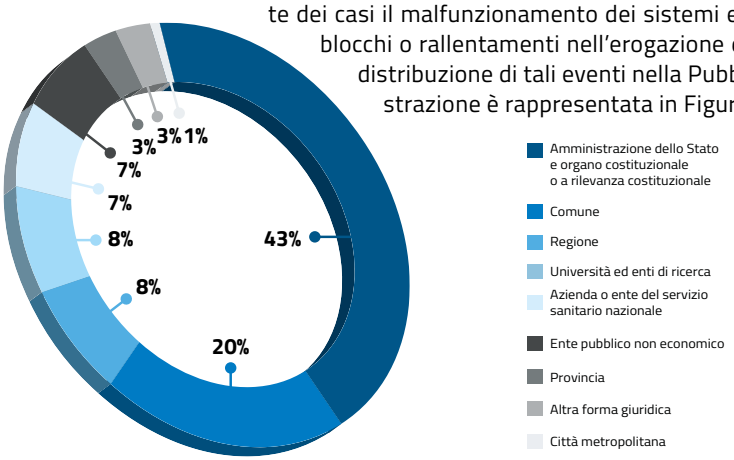


Figura 16 – Distribuzione degli eventi *cyber* contro la Pubblica Amministrazione

Considerando la frequenza e l'impatto (una media di oltre un incidente a settimana) delle diverse tipologie di eventi, emerge come nel 2023 sia stato il DDoS il fenomeno più frequente nei confronti delle istituzioni pubbliche, seguito dallo sfruttamento di vulnerabilità e dal *phishing* (Figura 17). Si registra, quindi, un parziale cambiamento di rotta rispetto al 2022, quando la minaccia preponderante nella Pubblica Amministrazione fu di tipo *ransomware*, seguita dal DDoS.

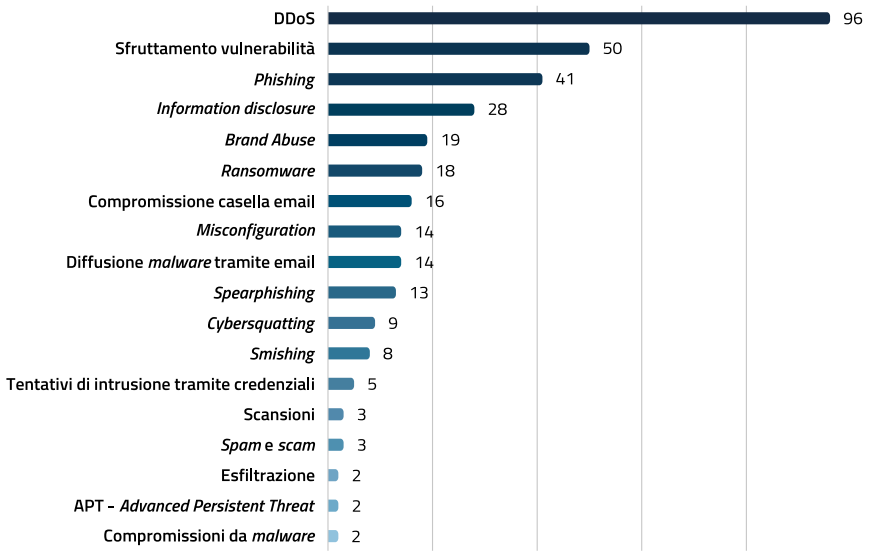


Figura 17 – Tipologie di eventi *cyber* contro la Pubblica Amministrazione

1.3 INTERVENTI A SUPPORTO DELLE VITTIME DI INCIDENTI

Tra i compiti attribuiti dalla legge all'Agenzia rientra il supporto alle vittime di incidenti di sicurezza cibernetica. Esso consiste principalmente nell'individuare e affiancare i soggetti nell'implementazione sia di azioni da compiere nell'immediato per il contenimento dell'incidente, sia di azioni volte al ripristino di una efficiente erogazione dei servizi.

Nei casi più complessi il supporto può avvenire tramite l'intervento *in loco* di un *team* di specialisti (*Deployable Digital Forensic Incident Response*-DDFIR). Nel corso del 2023 il personale specialistico dell'ACN è intervenuto, *in loco*, in 13 diversi casi, mentre in 31 casi ha fornito supporto da remoto (Figura 18) affiancando i soggetti nell'eradicazione della minaccia e nel ripristino delle condizioni di sicurezza con interventi della durata anche di diverse settimane.

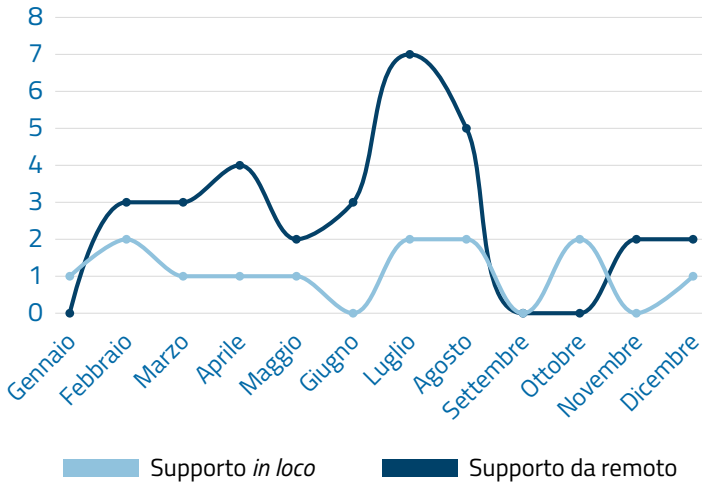


Figura 18 – Numero e tipologia di interventi a supporto diretto delle vittime di incidenti nel 2023

Per far sì che l'attività di supporto dell'Agenzia, sviluppata in occasione di eventi e incidenti cibernetici, possa dispiegarsi con la più ampia collaborazione da parte dei soggetti impattati, nel loro stesso interesse e in quello, più generale, della resilienza cibernetica del Paese, il 6 luglio 2023 il Presidente del Consiglio dei ministri, su proposta dell'Agenzia e sentito il Comitato interministeriale per la cybersicurezza (CIC), ha adottato una specifica Direttiva. Si è inteso rafforzare in particolare il quadro di cooperazione tra le Pubbliche Amministrazioni e l'ACN, onde ridurre i rischi di possibili propagazioni di conseguenze lesive dovute agli incidenti *cyber*, o il ripetersi di analoghi attacchi, ai danni di ulteriori soggetti pubblici e privati. La Direttiva stabilisce il quadro per una più efficace collaborazione con la PA[2], evidenziando come le conseguenze degli attacchi, se non gestite in modo coordinato ed efficace, potrebbero acquisire anche una rilevanza sistemica, sino a determinare un pregiudizio per la sicurezza nazionale. A tal fine, è richiesto alle amministrazioni pubbliche di operare garantendo:

- che l'Agenzia e, in particolare, gli operatori del CSIRT Italia dispongano del pieno supporto dei soggetti impattati, pure laddove gli stessi si dovessero avvalere di società *in house* o comunque a controllo pubblico;

[2] Nello specifico, le amministrazioni di cui all'art. 1, co. 2, del D.Lgs. n. 165/2001, con esclusione – in ragione delle specificità istituzionali e ordinamentali – degli organi dello Stato preposti alla prevenzione e accertamento dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché degli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.

- l'accesso ai locali, ai sistemi informativi e alle reti informatiche di pertinenza delle amministrazioni impattate, per tutto il tempo necessario al pieno esercizio delle competenze dell'Agenzia, compatibilmente con le prerogative dell'autorità giudiziaria.

Per dare cogenza a livello normativo a quanto previsto dalla citata Direttiva, nonché per assicurare che tale collaborazione si dispieghi quanto più possibile anche con i soggetti privati, nel mese di ottobre 2023 – in sede di conversione del D.L. n. 105/2023 – sono state introdotte nel D.L. n. 82/2021 alcune disposizioni volte a incrementare le capacità nazionali di prevenzione e di gestione degli incidenti e degli attacchi informatici.

In particolare, la previsione introdotta alla lettera n-*bis*), dell'art. 7, co. 1, del D.L. n. 82/2021 ha ampliato le funzioni dell'Agenzia, stabilendo che questa svolga ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici e privati che hanno subito incidenti o attacchi informatici. È quindi previsto che la mancata collaborazione da parte di alcune specifiche categorie di soggetti (soggetti Perimetro, NIS e Telco) sia valutata ai fini dell'applicazione delle sanzioni richiamate nella stessa disposizione.

Per altro verso, è stato previsto che l'Agenzia trasmetta al Procuratore nazionale antimafia e antiterrorismo i dati, le notizie e le informazioni rilevanti per l'esercizio delle funzioni e dei poteri di impulso e coordinamento delle indagini relative a gravi reati informatici di cui all'art. 371-*bis* del Codice di procedura penale[3].

Infine, sempre con il contributo dell'Agenzia, a fine anno (il 29 dicembre 2023) è stata adottata, sentito il CIC, una ulteriore Direttiva del Presidente del Consiglio dei ministri[4] volta a precisare alcuni aspetti applicativi del richiamato obbligo di collaborazione con l'ACN da parte dei Ministeri. In particolare, la Direttiva ha stabilito che tale obbligo potrà trovare puntuale attuazione in atti di intesa che dovranno declinare le attività che l'Agenzia e l'Amministrazione eventualmente colpita dall'attacco informatico saranno rispettivamente chiamati ad attuare. Vengono poi indicate le indispensabili misure che, in via prodromica e funzionale alla collaborazione prevista, dovranno essere messe in opera, ovvero implementate, anche per assicurare un più immediato ed efficace intervento dell'Agenzia in caso di incidente. Tra queste vi è la predisposizione di piani per la gestione delle vulnerabilità e della risposta in caso di incidente, nonché di un documento in cui siano definiti ruoli e responsabilità inerenti alla cybersicurezza, comprensivo dell'individuazione di un incaricato per la cybersicurezza (quale punto di contatto *cyber* ai fini delle comunicazioni e del necessario raccordo con l'ACN) e di un referente tecnico per la bersicurezza (da identificarsi tra il personale responsabile della gestione operativa dei sistemi IT).

---

[3] Comma 4-*bis* aggiunto all'art. 17 del D.L. n. 82/2021.

[4] Pubblicata nella Gazzetta Ufficiale del 16 febbraio 2024, n. 39.

1.4 ATTIVITÀ DI MONITORAGGIO PROATTIVO

L'Agenzia svolge, inoltre, attività di monitoraggio proattivo al fine di individuare e segnalare tempestivamente ai soggetti della *constituency* l'esposizione a specifiche minacce, rischi, vulnerabilità e criticità, che possono essere sfruttati, o che sono già in corso di sfruttamento, da parte degli attaccanti. A valle dell'individuazione, il CSIRT Italia entra in contatto con i soggetti a rischio e, qualora la criticità risulti particolarmente diffusa, svolge opera di diramazione pubblica degli *alert*, sia tramite portale pubblico sia attraverso i *social* dedicati (*Twitter/X, Telegram*).

Tramite queste attività sono stati segnalati, nel corso del 2023:

- **584 indirizzi web** di *phishing* contenenti riferimenti espliciti a 37 soggetti della *constituency*, per i quali sono state inviate **93 comunicazioni**;
- **2.822 dispositivi o servizi IT** potenzialmente affetti da vulnerabilità, per i quali sono state inviate **1.297 comunicazioni** ai 766 soggetti interessati;
- **802 dispositivi o servizi IT** potenzialmente compromessi afferenti a 210 soggetti nazionali, per i quali sono state inviate **241 comunicazioni**.

In Figura 19 sono sintetizzate, con riferimento ai 2.822 dispositivi o servizi IT, le tipologie di vulnerabilità rinvenute e segnalate ai soggetti, con la relativa gravità.

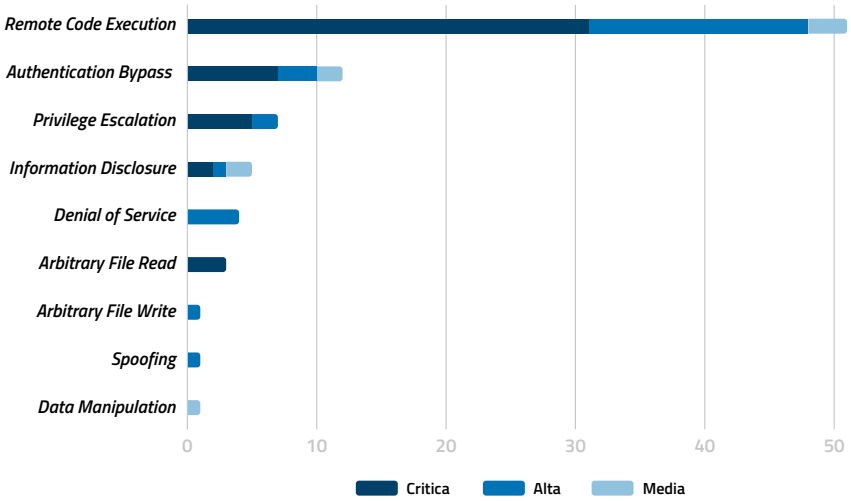


Figura 19 – Tipologia e gravità delle vulnerabilità rinvenute e segnalate dal CSIRT Italia

STUDIO DELLA SUPERFICIE D'ATTACCO

L'ACN studia la potenziale superficie di attacco nazionale, costituita dall'insieme di dispositivi e servizi esposti su Internet dai soggetti della *constituency*. Nel 2023 tale capacità di analisi è stata rafforzata, consentendo di individuare specifici fattori di rischio nello spazio di indirizzamento IP italiano.

A partire dal mese di luglio, attraverso la quotidiana analisi di circa 2,6 milioni di indirizzi IP, è stato possibile identificare, mediamente, ogni giorno:

- 753.468 indirizzi IP che presentano almeno un servizio o un dispositivo configurato erroneamente (c.d. *misconfiguration*);
- 167.663 indirizzi IP che presentano almeno un prodotto obsoleto e/o vulnerabile;
- 862.986 indirizzi IP che presentano almeno un servizio o un dispositivo che non dovrebbe essere esposto pubblicamente su Internet.

Infine, nel corso del 2023, il CSIRT Italia ha svolto diverse attività nell'ambito dello studio e dell'analisi. In particolare, sono stati condotti 472 approfondimenti su specifiche minacce *cyber* e, per ciascuna, è stata effettuata una stima del livello di rischio, predisponendo appositi bollettini contenenti gli esiti dell'analisi e le linee guida per la relativa mitigazione. Tale catalogo di bollettini "pronti all'uso" è utilizzato dal CSIRT Italia quale base per l'invio di comunicazioni ai soggetti che espongono la specifica minaccia, nonché all'interno del progetto HyperSOC (vds. capitolo 3).

Sempre in tale ambito, a partire dal mese di gennaio 2023, è stata avviata la redazione di un *report* di analisi dello stato della minaccia *cyber* in Italia, contenente i dati degli eventi e incidenti rilevati, l'analisi delle principali nuove vulnerabilità e gli approfondimenti sui *trend* della minaccia. Il documento, a diffusione limitata, a partire da giugno 2023 viene inviato mensilmente, tra gli altri, ai soggetti appartenenti al Perimetro di sicurezza nazionale cibernetica e alle Pubbliche Amministrazioni che partecipano al Nucleo per la cybersicurezza.

1.4.1 FOCUS SULLA MINACCIA APT

Nel corso del 2023 sono state riscontrate attività ostili da parte di attori cosiddetti *Advanced Persistent Threats* (APT), che conducono attacchi mirati, volti a installare *malware* nelle reti bersaglio per riuscire a mantenere attivi i canali impiegati per la fuoriuscita di informazioni di alto valore dalle infrastrutture IT della vittima. Tali attori hanno condotto tentativi di infezione tramite 9 campagne di *spearphishing* o tecniche di *social engineering*, 1 campagna di *password*

Spearphishing

Sottocategoria del phishing, è un attacco informatico contro obiettivi di specifico interesse che prevede l'invio di un messaggio da un account di posta elettronica apparentemente noto alla vittima, con l'intento di carpire informazioni sensibili o indurla ad aprire/scaricare allegati o link malevoli. Allo spearphishing sono associate tecniche di ingegneria sociale (social engineering), tra cui il monitoraggio delle relazioni e delle abitudini sui social media del soggetto d'interesse.

bruteforcing e 5 campagne di sfruttamento di vulnerabilità. La loro analisi ha portato a evidenziare dei collegamenti con attività pubblicamente attribuite a gruppi noti, come APT28, APT29, APT33, Storm-0558 e Lazarus.

In particolare, sono state colpite aziende e organizzazioni afferenti al settore diplomatico, governativo, della difesa, dei trasporti e dell'aerospazio, per un totale di 15 soggetti *target*.

Tra le tecniche più utilizzate per l'accesso iniziale alle reti delle vittime, si segnala l'utilizzo di e-mail di *spearphishing* con allegati o link malevoli, seguito dallo sfruttamento di vulnerabilità "recenti" o non note (*n-day, 1-day* e *0-day*) e dall'utilizzo di credenziali deboli tramite tecniche di *password bruteforcing* e *password spraying*.

Password bruteforcing

Consiste nel tentare il maggior numero possibile di password per forzare l'accesso ad una utenza.

Password spraying

Consiste nel provare la stessa password su tutti i possibili utenti.

Le infezioni condotte da questi particolari attori ostili hanno visto un ampio utilizzo di tecniche di persistenza, tra cui l'impiego di *webshell* sui portali pubblicamente accessibili, l'installazione di *malware* che si attivano all'avvio dei sistemi e che consentono il controllo remoto delle macchine *target* e l'utilizzo di strumenti leciti di amministrazione remota. Nella maggior parte dei casi sono stati utilizzati *malware* noti come appartenenti all'arsenale dell'attore, mentre in alcuni casi sono stati osservati e analizzati *malware* non pubblicamente documentati.

Webshell

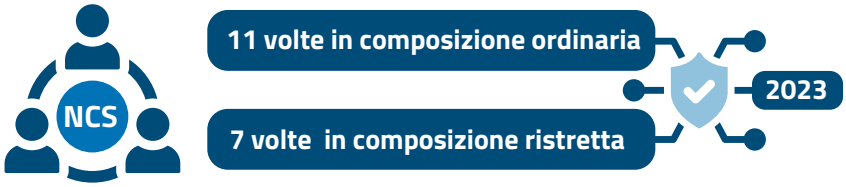
Programma malevolo solitamente installato dagli attaccanti al fine di consentire l'accesso da remoto a un server web.

Il principale intento percepito è stato quello del furto di informazioni presenti all'interno delle reti delle vittime, sfruttando servizi e applicativi leciti per la condivisione di dati e altre infrastrutture precedentemente compromesse.

1.5 PREVENZIONE E PREPARAZIONE A SITUAZIONI DI CRISI CIBERNETICA

Nel corso del 2023 il **Nucleo per la cybersicurezza** (NCS) ha continuato a consolidare il proprio ruolo, quale sede principale di coordinamento interministeriale a livello tecnico-operativo sulle questioni di cybersicurezza, al fine di sostenere l'azione del Presidente del Consiglio dei ministri. Nel 2023 il Nucleo si è riunito 11 volte in composizione ordinaria e 7 volte in composizione ristretta[5].

[5] Composizione del Nucleo che prevede la partecipazione alle riunioni delle sole amministrazioni e soggetti interessati.



NUCLEO PER LA CYBERSICUREZZA

Istituito in via permanente presso l'ACN, il Nucleo per la cybersicurezza opera a supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza per gli aspetti relativi alla prevenzione e preparazione a eventuali situazioni di crisi cibernetica e per l'attivazione delle procedure di allertamento.

L'NCS è presieduto dal Direttore generale dell'ACN, o dal Vice Direttore generale, ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del Dipartimento delle informazioni per la sicurezza (DIS), dell'Agenzia informazioni e sicurezza esterna (AISE), dell'Agenzia informazioni e sicurezza interna (AISI), di ciascuno dei Ministeri rappresentati nel Comitato interministeriale per la cybersicurezza e dal Dipartimento della Protezione civile della Presidenza del Consiglio dei ministri. Nel caso di trattazione di informazioni classificate, viene inoltre integrato da un rappresentante dell'Ufficio centrale per la segretezza del DIS.

Il Nucleo può essere convocato in composizione ristretta con la partecipazione delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi che coinvolgono aspetti di cybersicurezza. Per la gestione delle crisi cibernetiche, è prevista una composizione dell'NCS allargata ai rappresentanti del Ministero della salute e del Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile del Ministero dell'interno, nonché a quelli di ulteriori amministrazioni o di soggetti privati.

Dal 2023 per le riunioni in composizione ordinaria del Nucleo è stata prevista la partecipazione dei rappresentanti del Ministero della salute e del Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile del Ministero dell'interno – normativamente già disposta per le riunioni in situazioni di crisi cibernetica (*ex* art. 10, co. 3, D.L. n. 82/2021) – per una loro piena integrazione nei processi dell'NCS sin dalle fasi di normale operatività dello stesso.

L'NCS si è confermato il principale punto di raccordo informativo tra l'Agenzia e le diverse amministrazioni coinvolte che hanno potuto, ciascuna per gli ambiti di rispettiva competenza, condividere dettagli in merito allo stato della minaccia e alle attività di prevenzione e preparazione alle situazioni di crisi. Ciò ha permesso di mantenere un quadro situa-

zionale aggiornato e puntuale da poter riferire, con periodicità, al vertice politico così da assistere il processo decisionale del Governo.

In particolare, il Nucleo si è occupato di approfondire i riflessi in ambito nazionale delle situazioni di crisi internazionali, specialmente per quanto concerne l'acutizzarsi della minaccia cibernetica rivolta contro soggetti istituzionali italiani e di altri Paesi che hanno espresso solidarietà a Israele, a seguito degli eventi del 7 ottobre. In tale contesto internazionale, l'Agenzia ha fornito un costante aggiornamento sulla correlata minaccia *cyber*, invitando le amministrazioni NCS a mantenere elevati livelli di attenzione rispetto ai profili di cybersicurezza.

La valutazione tecnico-operativa sullo stato della minaccia ha portato a convocare una specifica riunione del **Comitato interministeriale per la cybersicurezza** per un esame a livello politico-strategico dello stato di sicurezza cibernetica, alla luce della situazione geopolitica internazionale relativa sia al conflitto in Medio Oriente che in Ucraina, oltre che delle misure di salvaguardia digitale necessarie alla protezione delle infrastrutture più critiche del Paese. Proprio in ragione dei temi trattati, la partecipazione al Comitato è stata estesa ad altri componenti del Consiglio dei ministri, nonché ad altre autorità.

COMITATO INTERMINISTERIALE PER LA CYBERSICUREZZA

Il CIC (istituito dall'art. 4 del D.L. n. 82/2021) ha funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

Il CIC è presieduto dal Presidente del Consiglio dei ministri ed è attualmente composto dall'Autorità delegata per la sicurezza della Repubblica e dai Ministri degli affari esteri e della cooperazione internazionale, dell'interno, della giustizia, della difesa, dell'economia e delle finanze, delle imprese e del *made in Italy*, dell'ambiente e della sicurezza energetica, dell'università e della ricerca e delle infrastrutture e dei trasporti. Le funzioni di segretario del CIC sono svolte dal Direttore generale dell'Agenzia.

Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare.

Nel 2023 si sono svolte, con il supporto dell'Agenzia, 5 riunioni, nel corso delle quali sono stati sottoposti all'attenzione del Comitato, in particolare: uno schema di DPCM di aggiornamento dell'elenco dei soggetti e dei settori inseriti nel PSNC (rispetto al quale il CIC è organo proponente ai sensi del D.L. Perimetro); due schemi di Decreti ministeriali sulla regolamentazione di dettaglio delle infrastrutture digitali per l'esecuzione e l'archiviazione delle intercettazioni (per l'adozione dei quali, ai sensi dell'art. 2, co. 9, del D.L. n. 105/2023, il Comitato si esprime per i profili di competenza); due Direttive adottate dal Presidente del Consiglio dei ministri in materia di cybersicurezza; nonché i bilanci dell'ACN.

In seno al Nucleo per la cybersicurezza l'Agenzia ha, inoltre, avuto modo di tenere aggiornate tutte le amministrazioni coinvolte sulle principali linee di azione portate avanti nel corso dell'anno per favorire la sicurezza e la resilienza *cyber* del Paese. In tale ambito, sono state infatti esaminate le attività di prevenzione e preparazione alle situazioni di crisi con risvolti per la cybersicurezza, come ad esempio la partecipazione a esercitazioni nazionali e multilaterali o le modifiche normative intervenute in materia, senza tralasciare la cooperazione internazionale, con particolare riferimento alla dimensione europea e al *capacity building*, in aggiunta ad approfondimenti su iniziative portate avanti dall'ACN in tema di innovazione tecnologica e ricerca.

Giova, infine, evidenziare che le sollecitazioni ricevute in relazione ad attacchi e incidenti rilevanti si sono tradotte in puntuali convocazioni del Nucleo in composizione ristretta con le amministrazioni interessate, per la gestione, condivisa e in funzione delle specifiche competenze, di incidenti *cyber* caratterizzati da maggiore rilevanza.

1.5.1 ISTITUZIONALIZZAZIONE E SVILUPPO DI CYCLONE

Il 2023 è stato il primo anno di esercizio istituzionale dello *European Cyber Crisis Liaison Organisation Network* (EU-CyCLONe o semplicemente CyCLONe) dopo l'entrata in vigore della Direttiva NIS 2 (Direttiva (UE) 2022/2555), che ne stabilisce formalmente il mandato e il ruolo all'interno dell'ecosistema di gestione crisi dell'Unione europea. CyCLONe, che nasce da un progetto promosso da Italia e Francia, ha lo scopo di sostenere la gestione coordinata degli incidenti e delle crisi *cyber* su vasta scala, garantendo il regolare scambio di informazioni tra gli Stati membri e le istituzioni, gli organi e le agenzie dell'Unione, ponendosi anche come elemento di collegamento tra la componente tecnica e il livello politico. La rete CyCLONe è composta dalle autorità per la gestione delle crisi *cyber* di ciascuno Stato membro e, in caso di incidente che possa avere un effetto sistemico per l'UE, dalla Commissione. All'Agenzia dell'Unione europea per la cibersicurezza (ENISA) è affidato il segretariato di CyCLONe, che viene presieduto dallo Stato membro che detiene la Presidenza di turno del Consiglio dell'Unione.

I lavori di CyCLONe, oltre a proseguire il monitoraggio delle evoluzioni del dominio *cyber* per intercettare eventuali segnali di una situazione di crisi, si sono incentrati sull'allineamento delle attività della rete stessa al mandato formale definito dalla Direttiva NIS 2, con particolare riferimento alla predisposizione della prima Relazione, che deve essere sottoposta al Parlamento europeo e al Consiglio UE entro giugno del 2024, nonché sul raccordo con il livello politico e sulle iniziative esercitative.

Nel corso del 2023, proseguendo nel suo ruolo di promotore del progetto, l'ACN ha partecipato alle attività di CyCLONe assicurando la presenza all'appuntamento annuale di

CYCLONE

A CyCLONe sono attribuiti i seguenti compiti:

- aumentare il livello di preparazione per la gestione di crisi e incidenti *cyber* su vasta scala;
- sviluppare una conoscenza situazionale condivisa in merito agli incidenti e alle crisi di cybersicurezza su vasta scala;
- valutare le conseguenze e l'impatto di incidenti e crisi di cybersicurezza su vasta scala e proporre possibili misure di attenuazione;
- coordinare la gestione degli incidenti e delle crisi di cybersicurezza su vasta scala e sostenere il relativo processo decisionale a livello politico;
- discutere, su richiesta di uno Stato membro interessato, i piani nazionali di risposta agli incidenti e alle crisi di cybersicurezza su vasta scala;
- cooperare con la rete di CSIRT.

vertice della rete, in linea anche con l'obiettivo di contribuire all'attivazione di meccanismi europei per il coordinamento della risposta a crisi *cyber* transnazionali.

Inoltre, è proseguita l'attività dell'ACN in seno al gruppo di lavoro per la redazione e l'affinamento della documentazione di base per il funzionamento di CyCLONe (*Working Group on Standard Operating Procedures*), specie in relazione al regolamento interno e alle procedure operative standard. A tale riguardo, l'Agenzia ha fornito impulso alla definizione delle modalità di supporto e raccordo con i gruppi del Consiglio UE di interesse. Nel mese di novembre è stata altresì assegnata all'Agenzia la presidenza del neocostituito gruppo di lavoro sulle esercitazioni (*Working Group on Exercises*).

1.5.2 ESERCITAZIONI INTERNAZIONALI E NAZIONALI

Le esercitazioni costituiscono uno strumento estremamente utile per innalzare la resilienza cibernetica del Paese, permettendo di simulare e testare meccanismi e procedure di gestione degli eventi e incidenti *cyber*, sia sul piano tecnico che su quello operativo. Tali attività rappresentano anche un utile momento per rafforzare la collaborazione interistituzionale, tanto tra i vari Ministeri e autorità impegnati sul piano nazionale, quanto tra diversi Stati e agenzie per quanto riguarda le attività in ambito internazionale.

In linea con l'impegno profuso nel 2022, anche nel 2023 l'Agenzia ha continuato ad assicurare la sua qualificata e attiva partecipazione alle esercitazioni caratterizzate da profili di cybersicurezza, tanto a livello nazionale quanto internazionale.

La principale esercitazione di carattere strategico-procedurale in ambito NATO è rappresentata dalla ***Crisis Management Exercise***, tenutasi nel 2023 dal 9 al 15 marzo. In tale ambito, l'ACN ha fornito, per la dimensione *cyber*, il supporto di propria competenza all'Ufficio del Consigliere militare del Presidente del Consiglio dei ministri, che coordina la partecipazione italiana all'iniziativa, assicurata tramite il Nucleo interministeriale situazione e pianificazione (NISP). Sempre in questo contesto, nel mese di dicembre l'Agenzia ha preso parte all'ulteriore esercizio NATO, noto come *Short Notice Exercise*.

A livello UE, l'Agenzia è stata impegnata nello svolgimento di **BlueOLEx**, attività annuale organizzata nell'ambito di CyCLONe per testare la preparazione dell'Unione in caso di crisi *cyber* e per potenziare la collaborazione tra le agenzie nazionali per la cybersicurezza degli Stati membri. L'edizione 2023, ospitata dal *National Coordinator for Security and Counterterrorism* dei Paesi Bassi, all'Aia (1° ottobre 2023), è stata condotta dalla Presidenza spagnola di turno del Consiglio dell'UE, sulla base dello scenario elaborato dalla Commissione europea con il supporto di ENISA.

In vista delle elezioni del Parlamento europeo di giugno 2024, inoltre, si è svolta a Bruxelles, il 21 novembre, la ***European Election Cyber Exercise 2023***, con l'obiettivo di garantire l'adeguata preparazione delle strutture nazionali ed europee responsabili dello svolgimento del processo elettorale, anche in relazione alla minaccia cibernetica. L'iniziativa, promossa dal Parlamento europeo, ha coinvolto i rappresentanti nazionali allo *European Cooperation Network on Elections* e al Gruppo di Cooperazione NIS (*NIS Cooperation Group*-NISCG), ovvero, per l'Italia, rispettivamente il Ministero dell'interno e l'ACN.

Inoltre, sempre a livello UE, si è conclusa la fase di pianificazione europea di ***Cyber Europe 2024*** (cui seguirà la fase di pianificazione nazionale), settima edizione della principale esercitazione di gestione crisi *cyber* dell'UE, che si tiene ogni due anni sotto il coordinamento di ENISA. L'iniziativa coinvolge gli Stati membri, le istituzioni, gli organi e le agenzie dell'Unione, nonché le strutture europee di gestione crisi, come CyCLONe, e di gestione degli incidenti, ovvero il *CSIRTs Network*. L'Agenzia ha dato il proprio contributo alla riorganizzazione e all'aggiornamento dell'esercitazione partecipando alle conferenze di pianificazione, nonché alla *task force* per la definizione degli obiettivi e l'elaborazione dello scenario.

Sul piano nazionale, al fine di rafforzare la capacità di gestione strategico-procedurale delle amministrazioni del Nucleo per la cybersicurezza e dei soggetti pubblici inseriti nel Perimetro di sicurezza nazionale cibernetica, sono state condotte 6 esercitazioni di tipo *table-top*

Cyber range

Ambienti virtuali nei quali possono essere simulati, a livello tecnico, reti e sistemi informativi oggetto di attacchi.

a favore di tali organizzazioni, nonché 2 esercitazioni di carattere tecnico a favore del CSIRT Italia, che ha previsto anche l'impiego di un *cyber range*.

ENISA CYBERSECURITY SUPPORT SERVICES

Nel contesto di CyCLONe, l'Agenzia ha preso attivamente parte ai c.d. *ENISA Cybersecurity Support Services,* una delle iniziative dell'Unione europea per il rafforzamento delle capacità *cyber* dei Paesi UE. Si tratta di una progettualità sperimentale avviata da ENISA per studiare, d'intesa con gli Stati membri, il ruolo che un fondo UE dedicato alle emergenze *cyber* possa svolgere.

Il progetto, sviluppato nel 2022 e proseguito nel 2023, prevede che le agenzie *cyber* nazionali dell'Unione possano usufruire di servizi di cybersicurezza erogati da ENISA al fine di rafforzare la resilienza delle strutture nazionali e, di conseguenza, dell'Unione. Il ventaglio di servizi offerti ricomprende la condotta di esercitazioni, *penetration test*, attività formative, monitoraggio e supporto alle attività di gestione degli incidenti.

2.

RESILIENZA DELLE INFRASTRUTTURE DIGITALI E SICUREZZA TECNOLOGICA

Il rafforzamento della resilienza *cyber* del Paese è tra i primari obiettivi dell'Agenzia, che contribuisce alla protezione degli *asset* critici nazionali attraverso un approccio sistemico orientato alla prevenzione, gestione e mitigazione del rischio. Ciò sia mediante il mantenimento di un quadro normativo aggiornato e coerente, sia con misure, strumenti e controlli che possano contribuire a rendere l'ecosistema digitale più sicuro e resiliente.

L'ACN, nel corso del 2023, è stata impegnata per rafforzare la capacità di far fronte alle minacce *cyber* attraverso il potenziamento della cybersicurezza e della resilienza, in particolare di quelle componenti più rilevanti per la tenuta del Paese. È proprio a questo obiettivo che si ispirano, pur nelle loro specificità, gli impianti normativi e regolatori relativi al Perimetro di sicurezza nazionale cibernetica e ad altre norme specifiche *cyber* quali, ad esempio, le Direttive NIS e NIS 2.

Infatti, in un'ottica di resilienza, riveste un ruolo fondamentale la garanzia che soprattutto i soggetti più sensibili utilizzino reti e sistemi digitali sicuri e resistenti alle intrusioni informatiche. A tale scopo rispondono le attività di scrutinio tecnologico, portate avanti dalle apposite articolazioni tecniche dell'Agenzia. Allo stesso tempo, l'ACN è stata impegnata anche in uno sforzo volto a ridurre i rischi connessi all'uso di strumenti digitali, tramite soluzioni di certificazione che garantiscano alti standard di sicurezza. A ciò si aggiunge, oltre al coinvolgimento dell'ACN nelle attività correlate all'esercizio dei poteri speciali (c.d. *Golden Power*), il ruolo svolto nei processi relativi alla transizione al *cloud* della PA e nella valorizzazione della crittografia come strumento di cybersicurezza.

LA CYBERSICUREZZA NEL CODICE DEI CONTRATTI PUBBLICI

Un elemento cruciale nel percorso verso la resilienza *cyber* è rappresentato dalla sicurezza degli strumenti tecnologici in uso. Per questo motivo, si evidenzia in particolare la sensibilità degli approvvigionamenti di tecnologie dell'informazione e della comunicazione (ICT). Al riguardo, il Piano di implementazione della Strategia, alla Misura #6, prevede proprio l'introduzione di disposizioni volte a valorizzare l'inclusione di elementi di sicurezza cibernetica nelle attività di *procurement* ICT della PA, fornendo indicazioni sia alla stessa PA che agli operatori di mercato per garantire che i beni e i servizi informatici acquistati da soggetti pubblici nell'ambito di gare d'appalto o di specifici accordi quadro rispondano – compatibilmente con la celere definizione delle procedure di aggiudicazione – ad adeguati livelli di cybersicurezza.

Sul punto, nell'ambito della predisposizione del nuovo Codice dei contratti pubblici (D.Lgs. n. 36/2023), si è intervenuto sulle modalità attraverso cui valorizzare gli aspetti legati alla cybersicurezza di prodotti e servizi acquisiti dalle Pubbliche Amministrazioni, anche al fine di contribuire a garantire la transizione digitale sicura del Paese. Tale riflessione, tra l'altro, è stata condotta, già a inizio 2023, anche in sede parlamentare dove, durante l'esame del testo del nuovo Codice, il Direttore

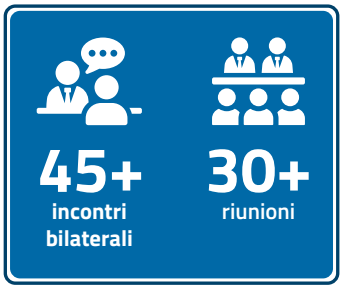
generale dell'ACN è stato invitato a svolgere un'audizione informale presso la VIII Commissione della Camera dei deputati (Ambiente, territorio e lavori pubblici).

Il legislatore della riforma ha quindi posto particolare attenzione alla *cybersecurity* che, anche grazie al contributo di competenza fornito dall'Agenzia nell'elaborazione delle specifiche disposizioni, trova per la prima volta un suo riconoscimento nel testo del Codice dei contratti pubblici. Nello specifico, tra le disposizioni riferite ai criteri di aggiudicazione degli appalti (art. 108), è stato previsto che le stazioni appaltanti, incluse le centrali di committenza, tengano sempre in considerazione gli elementi di cybersicurezza nell'approvvigionamento di beni e servizi informatici, in particolare quando il contesto d'impiego di tali beni e servizi risulti essere connesso alla tutela degli interessi nazionali strategici. In quest'ultimo caso, in particolare, la stazione appaltante deve stabilire un tetto massimo per il punteggio economico (entro il limite del 10%), risultando di tutta importanza attribuire un opportuno peso ai profili tecnico-qualitativi di cybersicurezza rispetto a quelli economici.

Sempre in tale ambito, l'ACN ha fornito il contributo di competenza all'elaborazione da parte del Governo (che l'ha approvata nel Consiglio dei ministri del 25 gennaio 2024) della proposta normativa, nota come D.D.L. "*Cyber*", nella quale si intende prevedere – tra le altre cose – che negli appalti pubblici per forniture di beni e servizi informatici destinati ad essere impiegati in un contesto connesso agli interessi nazionali strategici si osservino delle specifiche regole, che andranno definite con un apposito DPCM.

2.1 PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA: ATTUAZIONE DELLA NORMATIVA

Nel periodo di riferimento, l'Agenzia, nel proseguire le attività connesse all'attuazione della normativa Perimetro, ha avviato specifiche iniziative a supporto dei soggetti inseriti nel PSNC. In particolare, a partire da aprile è stato condotto un ciclo di oltre **30 riunioni** settoriali in cui sono stati invitati gruppi omogenei di soggetti inseriti nel Perimetro, alla presenza delle rispettive amministrazioni settorialmente competenti. Tale iniziativa ha permesso di stabilire un rapporto diretto con le articolazioni responsabili dell'adeguamento agli obblighi definiti dal D.L. Perimetro, fare il punto sulla documentazione condivisa dai soggetti, fornire chiarimenti di carattere generale sulle modalità attese di adozione delle misure di sicurezza e avviare un approfondimento circa alcune difficoltà registrate dai soggetti in fase attuativa. Ciò si rivela tanto più rilevante in conside-



razione del processo di periodico aggiornamento della disciplina, in via di programmazione per il 2024. A valle di queste riunioni sono stati inoltre condotti oltre **45 incontri bilaterali** al fine di approfondire alcune problematiche più specifiche di interesse dei singoli soggetti.

A livello istituzionale, il cosiddetto Tavolo Perimetro[6] si è riunito 3 volte (a febbraio, ottobre e dicembre) per deliberare in merito alle proposte di aggiornamento dell'elenco dei **soggetti Perimetro**. In particolare, sono state registrate variazioni di attribuzioni di funzioni e/o servizi essenziali dello Stato, che hanno portato a proporre al CIC alcune modifiche dell'elenco dei soggetti Perimetro, che a fine 2023 conta un totale di 118 soggetti.

Giova, inoltre, menzionare che a inizio anno (3 gennaio 2023) si è provveduto ad adottare la Determina del Direttore generale contenente la "Tassonomia degli incidenti che debbono essere oggetto di notifica", resasi necessaria a seguito dell'estensione degli **obblighi di notifica** introdotta dal comma 3-*bis* dell'art. 1 del D.L. Perimetro[7], alla cui elaborazione l'Agenzia ha fornito il proprio contributo. Infatti, tali obblighi, inizialmente previsti solo per gli incidenti aventi impatto su beni destinati a essere impiegati nel PSNC (c.d. beni ICT), sono stati estesi agli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (diversi quindi dai richiamati beni ICT), ma che sono comunque di pertinenza di soggetti inclusi nello stesso. L'intervento normativo è stato finalizzato a rafforzare il sistema di tutela della sicurezza nazionale nello spazio cibernetico posto in essere dal PSNC e ad avere un quadro tecnico-situazionale aggiornato sugli eventi in corso, anche al fine di prevenire possibili conseguenti impatti sui beni tecnologici rilevanti inseriti nel Perimetro.

La disposizione introdotta ha previsto un termine di notifica entro 72 ore, pertanto meno stringente rispetto a quelli previsti per i beni Perimetro (fissati in 1 ora e 6 ore, a seconda dell'entità dell'incidente). Inoltre, la stessa Determina, oltre a prevedere, per evitare ambiguità e duplicazioni, l'adozione di una tassonomia degli incidenti coerente con quella già familiare ai soggetti interessati e già prevista per gli incidenti aventi impatto sui beni ICT, nonché modalità di notifica in linea di continuità con quelle già operative, ha attribuito ai soggetti anche la facoltà di notificare attività di *spearphishing,* ritenendo utile poter acquisire anche tali informazioni ai fini di un più completo quadro informativo.

---

[6] Il Tavolo interministeriale per l'attuazione del Perimetro di sicurezza nazionale cibernetica ha il compito di proporre al CIC ogni variazione relativa all'individuazione delle funzioni e dei servizi essenziali dello Stato, nonché dei soggetti che li erogano. Tali variazioni vengono adottate, su proposta del CIC, con un atto amministrativo del Presidente del Consiglio dei ministri non soggetto a pubblicazione e per il quale è escluso il diritto di accesso.

[7] Comma inserito dall' art. 37-*quater*, co. 1, D.L. 9 agosto 2022, n. 115, convertito, con modificazioni, dalla legge 21 settembre 2022, n. 142.

2.2 DIRETTIVA NIS 2: STATO DEL RECEPIMENTO

Il percorso volto all'innalzamento dei livelli di sicurezza e resilienza *cyber* del Paese non passa solamente attraverso le prescrizioni del Perimetro di sicurezza nazionale cibernetica, ma anche attraverso quelle che discendono dalla normativa europea sulla sicurezza dei *Network and Information Systems*, e cioè dalla già citata Direttiva NIS del 2016 e dalla successiva Direttiva NIS 2 del 2022, che la sostituisce integralmente.

DIRETTIVA NIS 2

La Direttiva NIS 2 (Direttiva UE 2022/2555) supera e rafforza l'impianto normativo previsto dalla precedente Direttiva NIS (Direttiva (UE) 2016/1148), facendo tesoro dell'esperienza acquisita nella sua applicazione, in relazione ai seguenti ambiti:

- **introduzione del meccanismo di identificazione dei soggetti** in entità importanti o essenziali, per mezzo di un criterio omogeneo di identificazione basato sulla dimensione (c.d. *size-cap rule*), che estende l'applicazione della Direttiva a tutte le medie e grandi imprese che operano nei settori identificati dalla stessa. Inoltre, vengono ricomprese la Pubblica Amministrazione centrale (lasciando discrezionalità agli Stati membri su quella locale) e, indipendentemente dalle dimensioni, alcune specifiche categorie di soggetti individuate nella Direttiva;
- **allargamento dell'ambito di applicazione**, con un aumento significativo dei settori di applicazione e l'introduzione di un approccio "*all-hazards*" alla cybersicurezza, con l'inclusione di profili di sicurezza fisica delle infrastrutture ICT;
- **rafforzamento dei poteri di supervisione**, con indicazioni più dettagliate per la definizione delle misure di sicurezza e l'inasprimento delle sanzioni;
- **estensione delle funzioni dei CSIRT nazionali**, che fungeranno, tra l'altro, da intermediari di fiducia tra i soggetti segnalanti e i fornitori di prodotti e servizi ICT nell'ambito del quadro per la divulgazione coordinata delle vulnerabilità;
- **gestione delle crisi**, con la previsione di quadri nazionali in materia e l'istituzionalizzazione di EU-CyCLONe, per la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala.

Il passaggio dalla NIS alla NIS 2 prevede un aggiornamento del quadro regolatorio di tutti i Paesi dell'Unione europea, che dovranno recepire la nuova Direttiva entro il 17 ottobre 2024. A tal fine, l'Agenzia ha contribuito all'elaborazione del "Disegno di legge di delegazione europea 2022-2023", specie in relazione all'art. 3 che stabilisce specifici principi e criteri direttivi di delega per il recepimento della Direttiva NIS 2.

In particolare, il citato articolo di delega reca, tra gli altri, criteri finalizzati a:

- individuare i parametri in base ai quali un ente pubblico può essere considerato Pubblica Amministrazione ai fini dell'applicazione delle disposizioni della Direttiva NIS 2,

anche considerando la possibilità di applicazione della stessa Direttiva ai Comuni e alle Province secondo principi di gradualità, proporzionalità e adeguatezza;

- confermare la distinzione tra l'ACN, quale autorità nazionale competente e punto di contatto unico nazionale, e le autorità di settore;
- confermare le disposizioni del D.Lgs. n. 65/2018 in materia di istituzione del CSIRT Italia, prevedendo, inoltre, di ampliare la collaborazione, ivi prevista, tra tutte le strutture pubbliche con funzioni di *Computer Emergency Response Team* (CERT) coinvolte in caso di eventi malevoli per la sicurezza informatica;
- introdurre le modifiche necessarie alla legislazione vigente al fine di assicurare il corretto recepimento delle disposizioni della Direttiva in tema di divulgazione coordinata delle vulnerabilità;
- rivedere il sistema sanzionatorio e quello di vigilanza ed esecuzione, prevedendo sanzioni effettive, proporzionate e dissuasive rispetto alla gravità della violazione degli obblighi derivanti dalla Direttiva.

Divulgazione coordinata delle vulnerabilità (Coordinated Vulnerability Disclosure-CVD)

Processo volto a favorire la proficua interazione tra ricercatori che scoprono vulnerabilità e fabbricanti o fornitori di servizi o prodotti ICT, per il tramite di un intermediario di fiducia (che, ai sensi della NIS 2, deve essere un CSIRT formalmente designato da ciascuno Stato membro). Tale processo mira a garantire a fabbricanti e fornitori il tempo necessario a risolvere tali vulnerabilità prima che vengano rese pubbliche, mettendo al contempo al riparo il ricercatore da eventuali profili di responsabilità.

Nelle more dell'adeguamento alla NIS 2, tenuto conto del significativo impatto che la rinnovata disciplina avrà sul tessuto economico nazionale, l'Agenzia ha preso parte a diverse iniziative per sensibilizzare i soggetti che operano nei settori cui si applicherà la nuova Direttiva e avviare un dialogo con gli stessi soggetti volto a individuare ulteriori elementi da valutare nelle successive fasi dell'attività legislativa e regolamentare di attuazione. A tale riguardo l'ACN ha assicurato la propria partecipazione a eventi promossi da organismi europei come ENISA, così come a quelli organizzati dal tessuto imprenditoriale e da enti attivi nel partenariato pubblico-privato.

Al contempo, sono stati consolidati i rapporti con le 5 amministrazioni centrali, autorità di settore NIS (Ministero dell'economia e finanze-MEF, Ministero delle imprese e del *made in Italy*-MIMIT, Ministero dell'ambiente e della sicurezza energetica, Ministero delle infrastrutture e trasporti e Ministero della salute), attraverso periodiche riunioni, al fine di monitorare lo stato di attuazione della prima Direttiva NIS e avviare le discussioni relative agli aspetti pratici di recepimento della Direttiva NIS 2. In quel contesto è anche stata confermata la rilevanza del ruolo delle Regioni e delle Province autonome, in relazione ad alcuni settori che rientrano nell'ambito di applicazione della nuova Direttiva, portando ad avviare una interlocuzione con la Conferenza delle Regioni e delle Province autonome in vista di un suo prossimo coinvolgimento per le fasi attuative di rispettiva competenza.

2.3 LA CERTIFICAZIONE NEL MONDO DIGITALE

La costruzione di un ecosistema digitale sicuro richiede che siano adottati standard riconosciuti per garantire la resilienza delle soluzioni tecniche impiegate e la fiducia degli utenti nella corretta tutela del proprio patrimonio informativo. È questa la funzione primaria dei processi di certificazione che riguardano i prodotti e i servizi che compongono la trama dei moderni sistemi digitali complessi. Il ruolo dell'Agenzia in questo settore è quello di Autorità nazionale di certificazione della cybersicurezza, declinato a seconda che si tratti dell'applicazione di standard nazionali, europei o internazionali.

La certificazione ai sensi del Cybersecurity Act

Il Regolamento (UE) 2019/881, noto come Cybersecurity Act, comprende il Titolo III, dedicato al "Quadro europeo di certificazione della cybersicurezza", che definisce i sistemi europei di certificazione della cybersicurezza e i vari attori coinvolti, pubblici e privati.

Con il *Cybersecurity Act* o CSA (Regolamento (UE) 2019/881), l'Unione Europea, tra le altre cose, si è dotata di un quadro comune di certificazione della cybersicurezza con l'obiettivo di superare l'attuale frammentazione del mercato interno dei certificati di cybersicurezza e rendere maggiormente affidabili per il consumatore i prodotti e i servizi che utilizzano tecnologie dell'informazione e della comunicazione, a beneficio del mercato unico dell'UE.

Il CSA prevede l'adozione, tramite specifici regolamenti di esecuzione, di sistemi europei di certificazione della cybersicurezza per diversi ambiti, cioè regole armonizzate per l'emissione e gestione dei certificati di cybersicurezza per attestare la resistenza di prodotti, servizi e processi ICT ad attacchi e minacce informatiche. Nel 2023 si è lavorato all'elaborazione dei primi di tali sistemi, relativi alle certificazioni *Common Criteria* (EUCC), ai servizi *cloud* (EUCS) e alle reti 5G (EU5G).

European Common Criteria

Si tratta del primo sistema di certificazione europeo, che si ispira allo standard internazionale dei Common Criteria (ISO/IEC 15408). Una volta recepito abrogherà tutti gli schemi nazionali basati sullo stesso modello, incluso lo schema italiano attualmente applicato da OCSI (in base al DPCM 30 ottobre 2003).

Il CSA richiede, inoltre, a tutti gli Stati Membri di designare una o più Autorità nazionali di certificazione della cybersicurezza (***National Cybersecurity Certification Authority*-NCCA**) che vigilino a livello nazionale sull'applicazione del Regolamento e dei successivi sistemi di certificazione e cooperino con le autorità designate dagli altri Stati membri, la Commissione europea ed ENISA nella realizzazione e revisione del quadro europeo di certificazione.

Alle NCCA sono assegnate funzioni di vigilanza sugli organismi di valutazione della conformità e sui titolari dei certificati di cybersicurezza (vigilanza soggettiva), nonché sui certificati e sulle dichiarazioni di conformità (vigilanza oggettiva), con poteri ispettivi e sanzionatori. Le NCCA hanno anche il compito di rilasciare i certificati di cybersicurezza per il livello di affidabilità elevato.

In Italia, il ruolo di NCCA è stato assegnato all'Agenzia per la cybersicurezza nazionale dal D.L. n. 82/2021 e ulteriormente disciplinato dal D.Lgs. n. 123/2022.

Inoltre, sempre a livello nazionale, è operativo, da ormai vent'anni, lo schema nazionale di valutazione e certificazione ICT (definito con DPCM 30 ottobre 2003), che sarà superato dallo schema europeo EUCC. Nel 2023, in continuità con gli anni precedenti, l'Agenzia, in qualità di **Organismo di certificazione della sicurezza informatica (OCSI)**, ha portato avanti i compiti assegnati ai sensi dello schema nazionale, tra cui:

- l'emissione di 12 certificati di cybersicurezza in base allo standard *Common Criteria*, che sono riconosciuti a livello europeo e internazionale grazie agli accordi di mutuo riconoscimento (vds. box) ai quali OCSI aderisce;
- l'avvio di ulteriori processi di certificazione (al 31 dicembre 2023 ne risultano attivi 14);
- l'emissione di 3 attestazioni di conformità per dispositivi di firma/sigillo qualificato. OCSI, infatti, opera nell'ambito del Regolamento eIDAS (Regolamento (UE) 910/2014) in qualità di organismo di certificazione designato per l'Italia (ai sensi del Codice dell'amministrazione digitale).

L'ACN è attiva anche sul fronte della certificazione e valutazione di sicurezza di tecnologie emergenti, in particolare per quanto riguarda l'Intelligenza Artificiale (IA), ormai divenuta un ambito di interesse globale. Sul punto, oltre a contribuire a livello europeo al negoziato del relativo Regolamento, l'Agenzia partecipa a un gruppo di lavoro di ENISA ("*Thematic Group Artificial Intelligence*") volto a valutare le modalità con cui prodotti e servizi connessi a

Accordi di mutuo riconoscimento

A livello internazionale, gli organismi di certificazione aderiscono ad accordi di mutuo riconoscimento che consentono di attribuire validità comune ai certificati emessi dagli organismi aderenti. OCSI aderisce a:

- *CCRA (Common Criteria Recognition Arrangement): comprende 31 Paesi a livello globale;*
- *SOG-IS (Seniors Officials Group Information Systems Security): comprende 17 Paesi europei, anche extra-UE*

tecnologie di IA potrebbero essere oggetto di certificazione di cybersicurezza nell'ambito del *Cybersecurity Act*. L'Agenzia, inoltre, partecipa allo sviluppo di *framework* di controllo dell'IA nell'ambito dell'organizzazione internazionale *no-profit Cloud Security Alliance*, insieme a omologhe agenzie estere e *provider* globali di settore.

2.4 SCRUTINIO TECNOLOGICO PER IL PSNC

Dopo il suo avvio nella seconda parte del 2022, il **Centro di valutazione e certificazione nazionale (CVCN)** nel 2023 ha consolidato e ottimizzato le proprie procedure al fine di garantire l'applicazione della specifica normativa, tenendo comunque in debita considerazione le esigenze dei soggetti Perimetro di tempi di scrutinio commisurati alle loro esigenze di funzionamento operativo.

Centro di valutazione e certificazione nazionale

La struttura dell'ACN che riceve le comunicazioni da parte dei soggetti inclusi nel Perimetro concernenti l'intenzione di impiegare particolari categorie di componenti ICT all'interno di reti, sistemi informativi e servizi informatici da cui dipendano funzioni o servizi essenziali dello Stato e dal cui malfunzionamento, interruzione, o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Il CVCN può disporre l'esecuzione di test di corretta implementazione delle funzioni di sicurezza e penetration test su quei componenti e negarne o autorizzarne la messa in esercizio, con eventuali prescrizioni.

Come mostrano i dati riportati in Figura 20, il 2023 ha visto il CVCN impegnato nell'esame di un numero considerevole di procedimenti. Per una corretta lettura di tali dati, si noti che alcuni procedimenti esaminati nel corso del 2023 sono stati avviati nell'anno precedente.

Anche nel caso di autorizzazione senza esecuzione dei test, il CVCN ha fornito raccomandazioni o condizioni volte a prevedere l'adozione di buone pratiche di sicurezza, mirate sul particolare oggetto di fornitura e sullo specifico contesto d'impiego. Queste sono elaborate sulla scorta dell'analisi del rischio prodotta dal soggetto e valutata dal CVCN nella fase delle verifiche preliminari. Nei casi in cui, invece, è stata imposta l'esecuzione di test di sicurezza, gli stessi sono stati tutti condotti dai laboratori del CVCN, che ha poi fornito, al soggetto, al fornitore e/o allo sviluppatore, delle prescrizioni, raccomandazioni o indicazioni per il miglioramento della sicurezza del prodotto e delle sue condizioni di impiego.

L'esecuzione dei test ha consentito di alimentare e mettere a disposizione dei soggetti del Perimetro un catalogo di prodotti valutati; il che risponde anche a esigenze di velocizzazione e semplificazione procedurale, tendente a valorizzare il disposto normativo (art. 6 del DPR n. 54/2021) a mente del quale occorre "*evitare la duplicazione di test eventualmente già eseguiti*". Il catalogo rappresenta uno strumento utile per tali soggetti che intendano acquisire apparati ICT, potendosi così ragionevolmente aspettare un processo di valutazione più snello per prodotti che abbiano già superato i test di sicurezza del

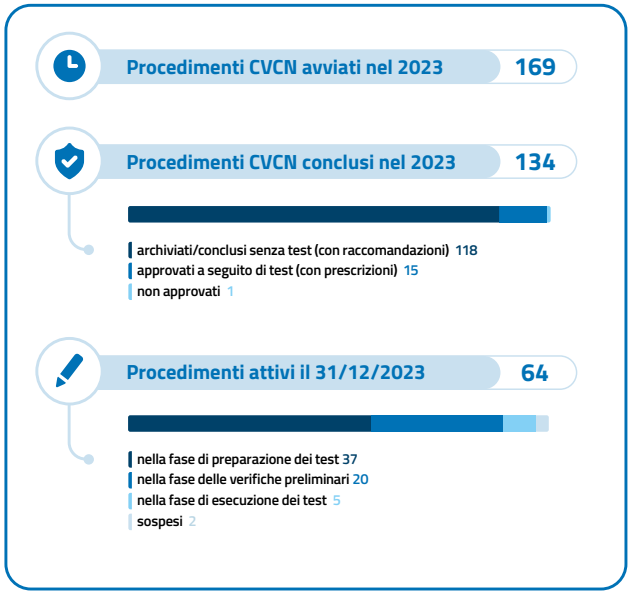


Figura 20 – Stato dei procedimenti in esame da parte del CVCN nel 2023

CVCN. In ragione, però, della necessità di valutare di volta in volta i prodotti in relazione allo specifico contesto d'impiego, resta comunque ferma l'obbligatorietà della comunicazione al CVCN da parte dei soggetti Perimetro.

Nel corso del 2023 il CVCN si è impegnato per contenere i tempi e i costi delle procedure di valutazione dei procedimenti amministrativi, quantomeno delle fasi su cui esso ha un controllo diretto. Si è riusciti, così, a raggiungere una significativa contrazione delle tempistiche tra il 2022 e il 2023, nello specifico di circa il 30%, sia per i procedimenti conclusi con test, sia per quelli senza test.

In diversi casi i procedimenti sono stati sospesi e/o conclusi senza l'adozione di provvedimenti perché la documentazione fornita risultava parziale oppure perché l'oggetto della fornitura era escluso dall'obbligo di comunicazione al CVCN.

L'esecuzione dei test, talvolta, ha risentito di alcune criticità ricorrenti, come la non corretta definizione dell'oggetto della comunicazione al CVCN, non circoscritta a uno specifico componente ma a infrastrutture complesse, nonché la difficoltà nel reperire la documentazione necessaria per condurre efficientemente i test, specie nel caso in cui fornitore e produttore non coincidano. Questi aspetti, unitamente all'impatto delle procedure del

CVCN sui soggetti Perimetro e sui loro fornitori, sono stati oggetto di numerose occasioni di confronto e approfondimento.

> ***Vulnerabilità***
>
> *Una falla di un sistema informatico, hardware o software, che, qualora sfruttata, consentirebbe a un malintenzionato di comprometterne la disponibilità, l'integrità o la riservatezza.*

Nell'ambito delle attività di test e analisi di sicurezza, nonostante lo stringente vincolo temporale (60 giorni), gli esperti dei laboratori del CVCN hanno individuato anche diverse vulnerabilità informatiche non note (c.d. vulnerabilità *zero-day*). In particolare, sono state individuate **38 vulnerabilità *zero-day***, di cui **22 di livello critico o alto**, per le quali è stato attuato un processo di divulgazione responsabile (c.d. *responsible disclosure*), attraverso il quale, in stretta collaborazione con i produttori dei software o dei dispositivi oggetto di test, viene concordata la pubblicazione dei dettagli della vulnerabilità solo quando questa è stata corretta.

Di queste vulnerabilità, 9 sono già state corrette dal produttore (e i dettagli tecnici sono stati pubblicati online), 9 sono state riconosciute dai produttori e saranno corrette, per le restanti vulnerabilità le interlocuzioni sono ancora in corso.

> ***Vulnerabilità zero-day***
>
> *Per zero-day si intende una vulnerabilità non ancora pubblicamente nota e per la quale, di conseguenza, non sono state rese disponibili mitigazioni dal produttore. Il termine zero-day si riferisce al fatto che il produttore ha avuto a disposizione zero giorni di preavviso per predisporre una correzione o mitigazione della vulnerabilità stessa.*

Per quanto riguarda i Centri di valutazione (CV) presso il Ministero della difesa e il Ministero dell'interno, anche nell'ottica di raggiungere i relativi obiettivi PNRR (vds. al riguardo il capitolo 3), è stato istituito un Comitato di attuazione, presieduto da ACN, che si è riunito 3 volte nel corso del 2023 e ha monitorato lo stato di avanzamento dell'attivazione dei due CV, al fine di omogeneizzare le iniziative di sviluppo.

Particolarmente sfidante si è rivelato il processo di accreditamento di laboratori di prova (Laboratori accreditati di prova-LAP) in ragione dei rigorosi requisiti strumentali, professionali e documentali richiesti agli aspiranti LAP per operare a supporto del CVCN nell'ambito del Perimetro. Proprio per tali ragioni l'Agenzia, tramite il CVCN, ha, da un lato, fornito supporto ai laboratori che intendano accreditarsi (anche attraverso indicazioni puntuali sulla redazione della documentazione e con la messa a disposizione, sulla pagina web

> ***Laboratori accreditati di prova***
>
> *Il CVCN può delegare l'esecuzione di test a laboratori di prova preventivamente accreditati ai sensi del DPCM n. 92/2022 e delle discendenti determinazioni tecniche adottate da ACN.*
>
> *È possibile richiedere l'accreditamento per l'area "Software e Network" (che comprende un sottoinsieme delle categorie di beni ICT del DPCM 15 giugno 2021), fino a un livello di severità dei test medio-alto.*

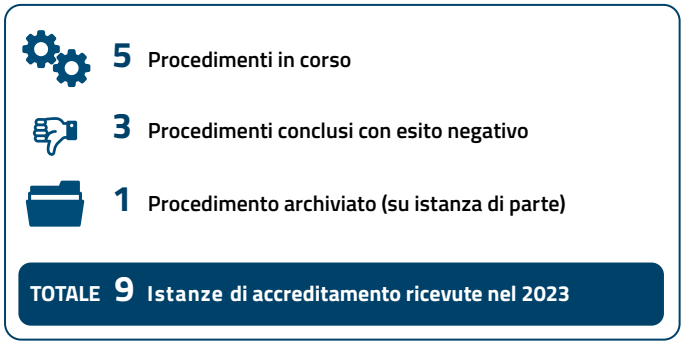


Figura 21 – Stato di avanzamento dell'accreditamento dei LAP nel 2023

del CVCN, di una raccolta di FAQ sui requisiti necessari per l'accreditamento), dall'altro, ha curato un processo di aggiornamento delle modalità d'esame.

La situazione al 31 dicembre 2023 rispetto all'accreditamento di LAP è sintetizzata in Figura 21[8].

2.5 ATTIVITÀ ISPETTIVE E DI VERIFICA

Da ottobre 2022, in seno all'ACN opera un'articolazione deputata allo svolgimento delle attività di verifica tecnico-documentale e ispezione, per gli adempimenti di cybersicurezza attribuiti all'Agenzia dalla normativa vigente, nei confronti dei soggetti sia pubblici che privati.

Tale articolazione, che nel 2024 vedrà un ulteriore rafforzamento delle proprie capacità operative anche in ragione del piano di reclutamento dell'Agenzia (vds. capitolo 7), ha continuato nel 2023 a sviluppare un sistema di gestione della qualità in conformità a quanto previsto per gli organismi di ispezione (UNI CEI EN ISO/IEC 17020). Ciò al fine di stabilire una struttura logica e coerente per tutte le procedure (istruzioni operative, modelli, registri, liste di riscontro), di consentire una gestione, documentale e operativa, efficace ed efficiente, nonché di offrire garanzie di imparzialità, indipendenza e riservatezza rispetto alle attività ispettive.

Laboratori di valutazione della sicurezza

Laboratori accreditati dall'OCSI che effettuano le valutazioni finalizzate alla certificazione di dispositivi ICT secondo lo schema nazionale di cui al DPCM 30 ottobre 2003.

[8] Nel corso del 2023 è stato anche concluso, con esito negativo, un ulteriore procedimento di accreditamento avviato nel 2022.

Nel corso dell'attività di verifica e ispezione dei Laboratori di valutazione della sicurezza (LVS) e dei LAP, propedeutica al loro accreditamento, è stata esaminata la documentazione presentata da 8 laboratori, fornendo le relative non conformità e osservazioni necessarie all'adeguamento ai requisiti previsti dalle norme di riferimento.

Nel corso del 2023 sono state inoltre condotte 4 attività ispettive nei confronti di altrettanti soggetti appartenenti al PSNC e 1 relativa a un laboratorio di valutazione della sicurezza LVS.

2.6 *CLOUD* PER LA PUBBLICA AMMINISTRAZIONE

I servizi digitali, erogati tramite le relative infrastrutture, rappresentano la modalità primaria di fornitura delle prestazioni al cittadino da parte delle Pubbliche Amministrazioni, richiedendo, per tale ragione, affidabilità, sicurezza e sostenibilità nel tempo. A tali principi si ispira il processo di transizione al *cloud* della PA[9]. Al riguardo, l'impianto normativo specifica le modalità per la migrazione e per la qualificazione dei servizi *cloud,* di cui la PA può approvvigionarsi ricorrendo al libero mercato, oltre a prescrivere le misure e i requisiti per il raggiungimento dei livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e delle caratteristiche di qualità, sicurezza, *performance*, scalabilità e portabilità dei servizi *cloud* per la Pubblica Amministrazione.

L'iter di transizione verso il *cloud* inizia con la fase di classificazione**,** mediante la quale viene stabilito l'impatto dei servizi e dei dati trattati da una PA in relazione al loro livello di criticità. A tal fine, già nel 2022 l'ACN, con Determina del Direttore generale (n. 306/2022), ha descritto i criteri con cui ogni Amministrazione stabilisce la rilevanza di ciascun dato e servizio trattato, sui tre livelli: strategico (la cui compromissione può avere un impatto sulla sicurezza nazionale), critico (la cui compromissione può determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese) e ordinario (i rimanenti dati e servizi).

Al fine di fornire una protezione adeguata a seconda del livello di classificazione, i citati livelli minimi per le infrastrutture digitali e le caratteristiche dei servizi *cloud*, siano essi erogati direttamente dalla PA o acquisiti dal mercato, sono stati definiti in maniera incrementale. Per preservarne l'efficacia e l'opportuna gradualità, è necessario provvedere al loro aggiornamento nel tempo, anche in relazione all'evoluzione dello scenario di rischio.

Il processo di qualificazione consente all'Agenzia di svolgere le verifiche preventive sul livello di conformità dei servizi *cloud* offerti da operatori privati dei quali si possono av-

[9] Processo che si è strutturato a partire dal c.d. "Regolamento *Cloud* per la PA", nonché con le Determine ACN 306 e 307 del 2022.

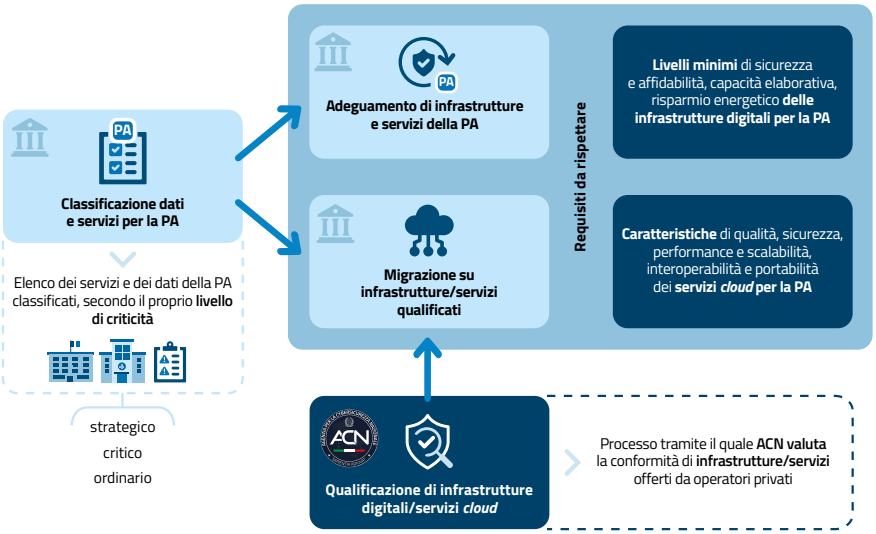


Figura 22 – Processo di transizione al *cloud* per la PA

valere le Pubbliche Amministrazioni in alternativa all'erogazione in proprio dei servizi. I requisiti di qualificazione sono anch'essi coerentemente organizzati su livelli crescenti, per un maggior controllo sui dati e sui servizi.

Le Pubbliche Amministrazioni che vogliono procedere all'acquisizione di un servizio *cloud* possono accedere a un catalogo (Catalogo *Cloud* per la PA), disponibile sul sito web dell'Agenzia, e verificare quali servizi *cloud* abbiano ricevuto la qualificazione da parte dell'ACN (unitamente al livello concesso), al fine di assicurarsi in via preventiva che questi siano conformi al livello di classificazione necessario per gestire i loro dati o servizi.

Nel corso del primo anno di gestione ACN, sono state ricevute oltre 500 istanze di qualificazione da parte di circa 300 fornitori differenti. Si è potuto tuttavia accogliere solo una parte delle istanze a causa di incoerenze sul completo adempimento dei requisiti previsti o carenze formali che ne pregiudicavano la corretta valutazione. Inoltre, nel solo 2023, sono state fornite risposte a circa 1.000 richieste di informazioni, spesso prodromiche alla vera e propria istanza di qualificazione.

In stretta collaborazione con il Dipartimento per la trasformazione digitale (DTD) della Presidenza del Consiglio dei ministri – nell'ambito delle relazioni del Dipartimento con la Commissione per l'innovazione tecnologica e la digitalizzazione della Conferenza delle Regioni e delle Province autonome – è stata avviata un'attività di coordinamento per

entità regionali e provinciali, coinvolgendo, altresì, le relative società *in house*. Ciò ha consentito di rilevare le peculiarità di ciascuna realtà territoriale e di contribuire, già in questa fase, a indirizzare correttamente le attività di adeguamento dei *data center* e servizi, nonché quelle relative alla migrazione.

A seguito del trasferimento delle funzioni dall'Agenzia per l'Italia digitale (AgID) all'ACN in tema di qualificazione, nel corso del 2023 quest'ultima ha effettuato alcuni interventi regolatori specifici, d'intesa con il DTD, al fine di gestire il periodo di transizione, integrando le previsioni del "Regolamento *Cloud* per la PA" (vds. box).

DECRETI ACN IN MATERIA DI *CLOUD*

Con il **Decreto direttoriale ACN del 2 gennaio 2023** è stato regolamentato il **regime transitorio** per la qualificazione dei fornitori, in modo da garantire la continuità dei servizi qualificati già in uso, gestendo, con gradualità, il passaggio di funzioni da AgID. In particolare, per le infrastrutture e i servizi *cloud* precedentemente qualificati da AgID, è stata rilasciata una nuova qualifica, valida fino al 18 gennaio 2024, di livello minimo, utile cioè per trattare esclusivamente dati e servizi classificati come ordinari. È stato quindi previsto che, nello stesso periodo, i fornitori potessero richiedere, attraverso modalità semplificate, il rinnovo, la promozione a un livello superiore per tali infrastrutture e servizi, o il rilascio di una qualifica per nuove infrastrutture e servizi *cloud*.

Il **Decreto direttoriale ACN dell'8 febbraio 2023** ha specificato i **termini** per la comunicazione dell'avvenuto adeguamento delle infrastrutture digitali e dei servizi *cloud* per le PA che gestiscono "*on premises*" le proprie infrastrutture, che affidano dati e servizi a società *in house*, nonché per quelle che li affidano a società a controllo pubblico per espressa previsione normativa. È stato così chiarito che tali infrastrutture e servizi non sono soggetti al citato processo di qualificazione, ma devono comunque essere conformi, entro il 18 gennaio 2024, ai requisiti contenuti nella Determina ACN n. 307/2022, termine entro il quale è necessario dichiararne l'adeguamento, con l'invio all'Agenzia della relativa autodichiarazione.

Con il **Decreto direttoriale del 28 luglio 2023**, sono stati aggiornati al 31 gennaio 2024 i termini per il **completamento del regime transitorio** (precedentemente fissati al 31 luglio 2023). Ciò ha risposto all'esigenza di garantire la necessaria gradualità al passaggio al nuovo regime e per razionalizzare alcuni requisiti tecnici previsti per le infrastrutture e i servizi *cloud* per la PA. Sono stati, inoltre, rivisti i termini per l'adeguamento relativi a interventi di particolare complessità. In tali casi l'Amministrazione avrà, infatti, a disposizione (ove abbia già formalizzato il relativo *iter* amministrativo entro il 30 settembre 2023) una diluizione dei termini fino al 18 ottobre 2024.

Durante il 2023, l'Agenzia ha quindi elaborato un documento unitario per razionalizzare e armonizzare la disciplina vigente in materia, la cui adozione è prevista per la prima metà del 2024. Questo aggiornerà i livelli minimi e le caratteristiche in materia al mutato scenario di rischio, chiarendo altresì alcuni profili di non agevole applicazione, emersi anche a seguito dei confronti con gli *stakeholder*.

European Cybersecurity Certification Scheme for Cloud Services

Sistema di certificazione europeo in tema di servizi cloud che sarà adottato dalla Commissione europea, ai sensi del Cybersecurity Act.

Inoltre, l'Agenzia sta lavorando per la definizione della certificazione europea sul *cloud* (EUCS), processo che presenta profili di particolare complessità e delicatezza, anche in considerazione del fatto che lo schema dovrà contemperare le esigenze di mercato con le istanze di autonomia e di non dipendenza da tecnologie extra-UE. In questo ambito, peraltro, si colloca il simultaneo impegno dell'ACN di assicurare che lo schema di certificazione europeo e il sistema di qualificazione nazionale dei fornitori di servizi *cloud* e di infrastrutture digitali siano coerenti.

Oltre a seguire il processo di evoluzione normativa in tema di *cloud* per la PA, l'Agenzia ha dedicato uno sforzo significativo per accrescere l'efficacia dei processi e degli strumenti in uso. Nello specifico, al fine di migliorare l'interazione con i fornitori di servizi *cloud* e con le amministrazioni, sono state avviate progettualità volte ad affinare gli strumenti tecnologici e informativi, anche attraverso la pubblicazione dell'apposita sezione sul sito web dell'Agenzia (sostitutiva dell'attuale *Marketplace Cloud* ereditato da AgID). Sono state inoltre definite tutte le metodologie di verifica, tanto quelle da adottare per il regime ordinario di qualificazione, quanto quelle necessarie per le dichiarazioni di conformità da trasmettere entro il 18 gennaio 2024, nonché quelle per il mantenimento dei requisiti da parte dei fornitori qualificati.

L'Agenzia è stata infine impegnata a fornire supporto al DTD nelle attività di verifica dei requisiti su infrastrutture e servizi *cloud* nell'ambito dei rilevanti progetti finanziati tramite il PNRR (Investimenti 1.1 "Infrastrutture digitali" e 1.2 "Abilitazione al *cloud* per le PA locali", a titolarità DTD). In particolare, l'Agenzia viene coinvolta primariamente in fase di vaglio preventivo delle istanze di finanziamento, fornendo le informazioni relative al processo di qualificazione delle infrastrutture digitali e dei servizi *cloud* al fine di verificare i requisiti di accesso al finanziamento.

2.7 CONTRIBUTO DELL'ACN IN MATERIA DI *GOLDEN POWER*

Nell'ambito delle attività correlate all'esercizio dei poteri speciali di cui al D.L. n. 21/2012, l'ACN partecipa ai procedimenti *Golden Power* in duplice veste:

- membro del **Gruppo di coordinamento**, che analizza le notifiche e le prenotifiche inviate dai soggetti in relazione a operazioni rientranti nell'ambito di applicazione del *Golden*

Power. In tale contesto, si distinguono un Gruppo di coordinamento "ordinario", competente sulle notifiche *ex* artt. 1 e 2 del D.L. 21/2012[10], e un Gruppo di coordinamento "ristretto", responsabile per le notifiche *ex* art. 1-*bis*, relative, attualmente, alla tecnologia 5G e, in prospettiva, a ulteriori tecnologie, a partire dalle infrastrutture *cloud*;

- membro del **Comitato di monitoraggio** sull'ottemperanza alle prescrizioni imposte sulle notifiche *ex* art. 1-*bis* (tecnologia 5G).

Per quanto riguarda le notifiche analizzate dal Gruppo di coordinamento, delle 577 pervenute nel 2023, 12 hanno riguardato i piani annuali e relativi aggiornamenti in materia di tecnologia 5G (ai sensi dell'art. 1-*bis*) e 565 le materie di cui ai richiamati articoli 1 e 2. Sono, inoltre, pervenute 150 prenotifiche[11]. In tale contesto, l'Agenzia è stata coinvolta nella valutazione di tutte le "notifiche 5G", e in circa il 30% delle "notifiche tradizionali" che presentavano profili di cybersicurezza. Ha, inoltre, esaminato il 23% delle prenotifiche.

I casi trattati sono stati particolarmente complessi, tanto che in circa un terzo dei procedimenti in cui l'ACN è stata coinvolta, è stato necessario un supplemento istruttorio mediante quesiti o audizioni. In relazione alle notifiche per cui l'Agenzia ha fornito supporto, l'esito del procedimento è riportato nella Figura 23.

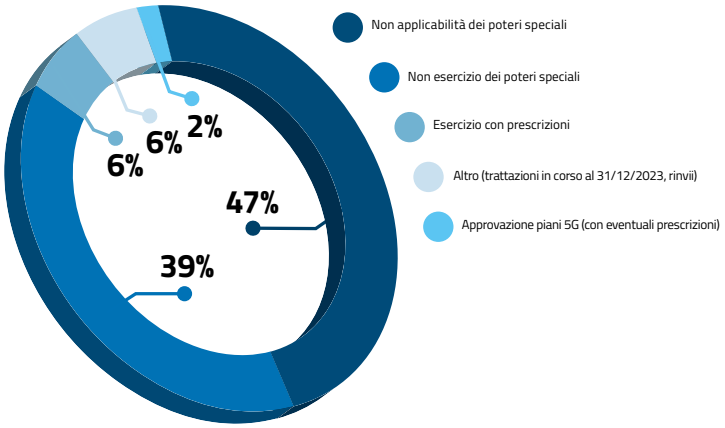


Figura 23 – Esito dei procedimenti su notifiche *Golden Power* in cui l'ACN è stata coinvolta

[10] Relativamente all'esercizio dei poteri speciali, rispettivamente, nei settori della difesa e della sicurezza nazionale, e quelli inerenti agli attivi strategici nei settori dell'energia, dei trasporti e delle comunicazioni.

[11] Le prenotifiche riguardano solo le trattazioni relative agli artt. 1 e 2 del D.L. n. 21/2012 e consentono l'esame da parte del Gruppo di coordinamento (o, nelle ipotesi previste, del Consiglio dei ministri) delle operazioni, anteriormente alla formale notifica, al fine di ricevere una valutazione preliminare sulla applicabilità dei citati articoli e sulla autorizzabilità dell'operazione.

Tra i casi trattati dal Gruppo di coordinamento nel corso del 2023, vi sono state notifiche che, seppur afferenti a settori non direttamente riconducibili a quello della cybersicurezza, quanto invece a contesti manufatturieri o relativi alle telecomunicazioni, per la natura degli assetti tecnologici interessati hanno reso necessaria la richiesta di un parere tecnico dell'ACN, rivelatosi determinante nell'adozione di provvedimenti di esercizio dei poteri speciali.

Per quanto attiene alle attività del Comitato di monitoraggio, previsto in ambito 5G, l'ACN ha ricevuto e analizzato 60 relazioni di ottemperanza. Il 2023 è stato un anno particolarmente rilevante da questo punto di vista, poiché sono state oggetto di monitoraggio le prescrizioni imposte agli operatori di telecomunicazione rispetto ai primi piani annuali presentati nel corso del 2022 (a seguito delle modifiche operate con il D.L. n. 21/2022). L'attività di monitoraggio si è concentrata, in particolare, sulla valutazione delle attività di diversificazione dei fornitori nella componente di accesso radio, in ottemperanza alle misure del *Toolbox* europeo sul 5G, al quale si sono ispirati i decreti di approvazione dei piani.

Per superare incertezze applicative, emerse a seguito della ridefinizione della disciplina dei poteri speciali inerenti, tra gli altri, ai servizi di comunicazione elettronica a banda larga con tecnologia 5G, e di contatti con gli operatori economici, l'Agenzia ha promosso la modifica normativa che ha portato all'abrogazione dell'art. 3 del D.L. n. 105/2019.

La disciplina prevede ora che:

- i soggetti inclusi nel Perimetro inviino le comunicazioni al CVCN (*ex* art. 1, co. 6, lettera a), del D.L. Perimetro) a prescindere dai procedimenti *Golden Power*, i quali, peraltro, attualmente afferiscono a piani annuali di sviluppo e non più a singoli contratti;
- le imprese non incluse nel Perimetro rispettino l'obbligo di notificare i propri piani di sviluppo di reti 5G al Gruppo di coordinamento *Golden Power*.

2.8 CRITTOGRAFIA E CYBERSICUREZZA

Vista la rilevanza che la crittografia ha già assunto e continuerà ad avere per il futuro della sicurezza informatica, l'ACN – già dalla seconda metà del 2022 – si è dotata di una struttura dedicata che agisce per la diffusione della crittografia quale strumento di cybersicurezza.

Coerentemente con le iniziative dei gruppi internazionali e delle omologhe istituzioni estere, l'ACN ha voluto ovviare alla totale assenza di documenti tecnici sulla crittografia a livello nazionale, tramite la pubblicazione di 3 documenti relativi alle **"Linee Guida delle Funzioni Crittografiche",** che forniscono dettagli tecnici e raccomandazioni riguardo gli algoritmi crittografici, e i relativi parametri, da adottare fin dalle prime fasi di progettazione di reti, applicazioni e servizi.

Il primo documento della serie, che nasce da un confronto tra l'Agenzia e l'Autorità Garante per la protezione dei dati personali (GPDP), risponde alle gravi lacune in termini di sicu-

rezza informatica nell'ambito della conservazione delle password, presenti in numerose imprese e amministrazioni titolari o responsabili del trattamento di dati personali. Gli archivi che contengono le password degli utenti, infatti, vengono spesso violati a causa di varie tipologie di attacchi informatici, per cui è di fondamentale importanza che le informazioni degli utenti siano cifrate in modo corretto. Nella pubblicazione **"Conservazione delle Password"**, redatta congiuntamente da ACN e GPDP e pubblicata il 12 dicembre 2023, sono presentate utili raccomandazioni sugli algoritmi crittografici più sicuri e sui parametri da utilizzare, in modo da raggiungere gli standard minimi di sicurezza.

Sempre il 12 dicembre 2023, l'ACN ha pubblicato altri due documenti della serie, intitolati rispettivamente **"Funzioni di *Hash*"** e **"Codici di Autenticazione del Messaggio"**, che approfondiscono temi prioritari, poiché strettamente collegati alla conservazione delle password. Il primo documento è dedicato alle funzioni di *hash* crittografiche, algoritmi largamente impiegati in ambito informatico per garantire l'integrità dei dati trasmessi. Il secondo tratta i codici di autenticazione del messaggio (MAC-*Message Authentication Code*), uno strumento crittografico ampiamente utilizzato che garantisce simultaneamente autenticazione e integrità dei dati.

L'Agenzia provvederà alla continua espansione della serie di Linee Guida, che in conclusione conterrà tutte le raccomandazioni dell'ACN in merito ai diversi ambiti della crittografia. Sarà inoltre necessaria una continua azione di aggiornamento di tali documenti, al fine di mantenere i contenuti sempre al passo con gli sviluppi nazionali e internazionali in termini di crittografia e cybersicurezza.

Sotto il profilo della ricerca, l'Agenzia sta analizzando con particolare attenzione la minaccia presentata dai computer quantistici per gli attuali schemi di crittografia a chiave pubblica. Nonostante al momento non esistano macchine o strumentazioni in grado di effettuare attacchi quantistici sugli attuali sistemi crittografici, è di fondamentale importanza prepararsi all'avvento dei computer quantistici nei prossimi decenni. Questa urgenza è prioritaria non solo per resistere a futuri attacchi diretti ai sistemi informatici in uso, ma anche per contrastare la strategia nota come "*harvest now, decrypt later*", che prevede di intercettare dati ora, per poi decifrarli in un futuro, quando saranno disponibili computer quantistici adatti. Per arginare tale minaccia, la comunità scientifica ha ideato nuovi algoritmi che possano resistere ad attacchi quantistici, dando vita alla cosiddetta **crittografia *post-quantum***.

Gli esperti dell'ACN stanno seguendo da vicino gli sviluppi internazionali, con particolare riguardo al processo di standardizzazione *post-quantum* del *National Institute of Standards and Technology* statunitense, e si stanno confrontando con i loro omologhi nei gruppi istituzionali europei. L'obiettivo è fornire consigli e direttive su una strategia di transizione verso i nuovi algoritmi *post-quantum*, passando per una fase intermedia di tipologia ibrida. Le raccomandazioni nazionali a tal riguardo saranno oggetto di un nuovo documento della serie "Linee Guida delle Funzioni Crittografiche" previsto per il 2024. Per restare aggiornati rispetto agli sviluppi europei, si è inoltre aderito all'invito a far parte dell'*Institutional and Industrial Advisory Board* per un progetto sulla transizione alla crittografia resistente ad attacchi quantistici ("*Quantum-oriented Update to Browsers and Infrastructures for the PQ Transition"),* nell'ambito del programma di ricerca *Horizon Europe*.

Oltre alle diverse interlocuzioni istituzionali, su base nazionale e internazionale, l'Agenzia è stata coinvolta anche in un confronto diretto con la comunità di ricerca nazionale, affiliandosi, in quanto ente pubblico, all'Associazione di promozione sociale "*De Componendis Cifris*", che vede partecipi professori universitari, aziende, studenti ed enti statali al fine di incentivare l'utilizzo della crittografia come strumento di cybersicurezza e diffondere i più recenti sviluppi in materia.

3.

INVESTIMENTI PNRR PER LA CYBERSICUREZZA

Nel quadro delle riforme per la digitalizzazione dell'Italia, il Piano nazionale di ripresa e resilienza (PNRR) dedica significativa attenzione alla sicurezza cibernetica, proponendo, tra le varie attività, un percorso di miglioramento della postura di sicurezza del sistema Paese nel suo insieme, a partire dalla Pubblica Amministrazione.

L'Investimento 1.5 *"Cybersecurity"* della Missione 1 – Componente 1 – Asse 1 del PNRR, a titolarità DTD e di cui l'Agenzia è Soggetto attuatore, prevede una dotazione di 623 milioni di euro al fine di migliorare le difese del Paese ponendo la cybersicurezza e la resilienza a fondamento della trasformazione digitale della PA, così come del settore privato. Ciò mira a rafforzare l'ecosistema digitale nazionale potenziando le capacità dell'Agenzia e sostenendo la crescita dell'autonomia tecnologica nazionale.

In quest'ottica, l'ACN sta coordinando diverse progettualità dedicate principalmente a potenziare la resilienza *cyber* delle PA, sviluppare servizi *cyber* nazionali e sostenere la creazione di una rete nazionale di laboratori di scrutinio e certificazione tecnologica.

L'Investimento 1.5 è declinato in *milestone* e *target* europei, organizzati secondo le due scadenze di dicembre 2022 e dicembre 2024. Le iniziative coordinate dall'Agenzia hanno permesso di raggiungere tutti gli obiettivi previsti per il 2022 (come riportato nel box).

MILESTONE E *TARGET* DELL'INVESTIMENTO 1.5 "*CYBERSECURITY*"

Obiettivi previsti entro dicembre 2022:

- ***milestone* UE M1C1-5**: attivazione dell'**Agenzia per la cybersicurezza nazionale**;
- ***milestone* UE M1C1-6**: dispiego **iniziale** dei **servizi *cyber* nazionali**;
- ***milestone* UE M1C1-7**: attivazione di almeno **1 laboratorio** di **scrutinio tecnologico e certificazione**;
- ***milestone* UE M1C1-8**: attivazione di **un'unità centrale di ispezione** per le misure di sicurezza PSNC e NIS;
- ***target* intermedio UE M1C1-9**: potenziamento delle capacità cyber. Realizzazione di almeno **5 interventi di potenziamento** *cyber* per le PA. In questo caso, il *target* è stato raggiunto grazie al completamento di 7 interventi di potenziamento, valutati positivamente dalla Commissione europea.

Nel corso del 2023 sono, quindi, proseguite le attività intraprese dall'Agenzia per conseguire gli ulteriori obiettivi previsti entro il 2024, quali:

- ***target* finale UE M1C1-19**: potenziamento delle capacità *cyber*. Realizzazione di almeno **50 interventi di potenziamento** *cyber* per le PA. In quest'ambito sono continuate le azioni

di monitoraggio e gestione delle attività degli Avvisi già attivati nel 2022 (Avvisi 1, 2 e 3) e degli Accordi di collaborazione in materia di c.d. "*cyber defence*". Inoltre, è stato pubblicato l'Avviso 7/2023, per il potenziamento della resilienza *cyber* delle PA centrali, ed è stato predisposto un ulteriore nuovo Avviso rivolto alle PA locali.

- ***milestone* UE M1C1-20**: dispiego **integrale** dei servizi ***cyber* nazionali**. In quest'ambito, è stato pubblicato l'Avviso 6/2023 per il finanziamento di CSIRT regionali, al fine di supportarne l'attivazione. Sono stati inoltre attivati i primi servizi dell'HyperSOC (un sistema di monitoraggio della minaccia *cyber* centralizzato) ed è in fase di attivazione l'ISAC Italia (centro per la diffusione capillare di informazioni sul rischio *cyber*, *Information Sharing and Analysis Centre*-ISAC). È stato, inoltre, stipulato un accordo con il consorzio CINECA a cui l'Agenzia ha conferito il mandato per l'espletamento della procedura di gara per realizzare una piattaforma di *High Performance Computing* (HPC) che, mediante strumenti di Intelligenza Artificiale e *machine learning* (ML), potenzierà le capacità dei servizi *cyber* nazionali.
- ***Milestone* UE M1C1-21**: attivazione di almeno **10 laboratori** di scrutinio tecnologico e certificazione, del **CVCN** e dei **Centri di valutazione dei Ministeri dell'interno e della difesa.** In quest'ambito sono proseguite le attività per realizzare dei CV per l'attivazione e l'accreditamento dei laboratori di scrutinio tecnologico dei soggetti interessati, individuati anche con la pubblicazione dell'Avviso 5/2022.
- ***Milestone* UE M1C1-22**: esecuzione di almeno **30 ispezioni** per le misure di sicurezza PSNC e NIS. In quest'ambito, a seguito dell'attivazione dell'unità centrale ispettiva, sono stati consolidati i sistemi interni di gestione e sono in corso di svolgimento le ispezioni.

3.1 INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA *CYBER* PER LA PA

L'obiettivo del potenziamento della resilienza *cyber* delle Pubbliche Amministrazioni è un fattore chiave per la trasformazione digitale sicura e resiliente del Paese ed è stato perseguito dall'Agenzia mediante interventi volti a valutare il livello di maturità della postura di sicurezza delle amministrazioni interessate e, conseguentemente, a delineare una strategia evolutiva per migliorarne organicamente il livello di maturità *cyber*. A tal fine, l'Agenzia ha proseguito l'approccio multilivello, coinvolgendo tutti i principali attori nazionali, pubblici e privati, del mondo della *cybersecurity*.

Il modello di analisi della postura di sicurezza è stato definito in linea con il "*Framework nazionale per la cybersecurity e la data protection*"[12]. Ciò ha consentito di avere una sostanziale uniformità nei risultati, valorizzando la rilevanza e la maturità delle prassi di

[12] Per maggiori informazioni si rimanda a https://www.cybersecurityframework.it/

sicurezza, responsabilizzando maggiormente le PA alla gestione di eventuali rischi e criticità. La predisposizione di specifici piani di potenziamento strategico ha consentito di raggiungere anche l'obiettivo di tracciare le vulnerabilità identificate in fase di analisi, nonché di pianificare organicamente gli investimenti a medio-lungo termine da realizzare.

3.1.1 ACCORDI STIPULATI E AVVISI FINALIZZATI NEL 2022. SVILUPPI

Gli Accordi stipulati e gli Avvisi pubblicati nel corso del 2022 sono stati gli strumenti con cui, nel 2023, sono state gestite le numerose progettualità dell'Agenzia in tale ambito.

In particolare, è proseguita l'azione dell'Agenzia per l'attuazione degli Accordi *Cyber Defence*, stipulati nel 2022, al fine di potenziare le capacità nazionali di difesa informatica di 6 entità istituzionali: Ministero dell'interno, Ministero della giustizia, Ministero della difesa, Arma dei Carabinieri, Guardia di Finanza e Consiglio di Stato. All'importo complessivo pari a 150 milioni di euro finalizzato al miglioramento della postura *cyber*, sono state aggiunte ulteriori risorse PNRR (18,5 milioni) per attività di progettazione e implementazione dei CV dei Ministeri dell'interno e della difesa. In merito, nel 2023 sono state ricevute richieste di anticipo (massimo 10% del totale) per un importo complessivo di 16,25 milioni di euro, accolte dall'Agenzia.

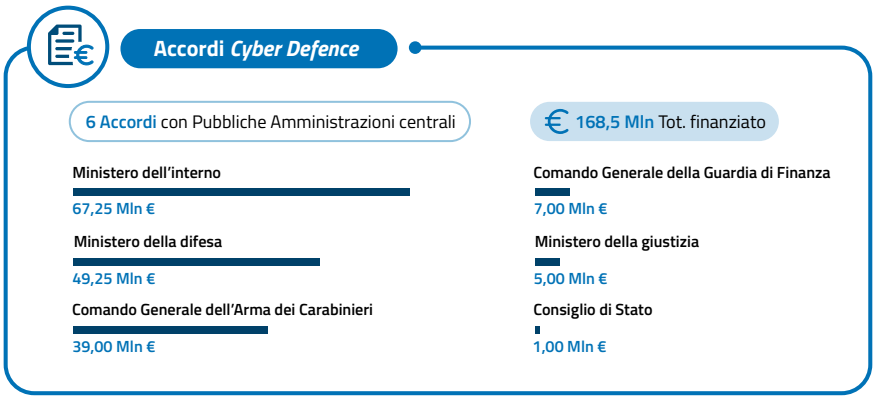


Figura 24 – Accordi *Cyber Defence*

L'Agenzia ha inoltre provveduto a seguire gli sviluppi degli Avvisi emessi nel 2022 (1, 2 e 3/2022), riassunti nel box.

SVILUPPI RELATIVI AGLI AVVISI PER IL POTENZIAMENTO DELLA RESILIENZA *CYBER* DELLA PA PUBBLICATI NEL 2022

Avviso Pubblico 1/2022: per il potenziamento della resilienza *cyber* degli Organi costituzionali e di rilievo costituzionale, delle Agenzie fiscali e delle amministrazioni facenti parte del Nucleo per la cybersicurezza.

- Aperto il 3 marzo 2022 | Chiuso il 7 aprile 2022.
- Nel 2022: finanziati 20 progetti di 12 amministrazioni per un totale di 15 milioni di euro.
- Nel 2023: rifinanziamento di 1,15 milioni di euro (portando il totale a 22 progetti) e anticipi nei limiti del 10%.

Avviso Pubblico 2/2022: per il potenziamento della resilienza *cyber* degli Organi costituzionali e di rilievo costituzionale, delle Agenzie fiscali e delle amministrazioni facenti parte del Nucleo per la cybersicurezza.

- Aperto il 3 marzo 2022 | Chiuso il 23 marzo 2022.
- Nel 2022: finanziati 57 interventi erogati dall'Agenzia per 12 amministrazioni per un totale di 7,85 milioni di euro.
- Nel 2023: portati a completamento la quasi totalità degli interventi finanziati sulle 12 amministrazioni.

Avviso Pubblico 3/2022: per il potenziamento della resilienza *cyber* di Regioni, Province autonome e Comuni capoluogo facenti parte di Città metropolitane.

- Aperto il 2 agosto 2022 | Chiuso il 17 ottobre 2022.
- Nel 2022: finanziati 51 progetti di 35 amministrazioni per un totale di 45 milioni di euro.
- Nel 2023: rifinanziamento di 18,7 milioni di euro (portando il totale a 63,7 milioni per 75 progetti) e anticipi nei limiti del 10%.

Nell'Avviso 3/2022 si considera preferenziale lo sviluppo di progetti in uno o più settori ritenuti strategici, permettendo ai soggetti realizzatori di coinvolgere ulteriori PA (ad esempio alcune Aziende sanitarie locali).

Il coinvolgimento di ulteriori Pubbliche Amministrazioni locali ha rappresentato criterio preferenziale ed è stato utilizzato per 63 dei 75 progetti ammessi a finanziamento. Per una corretta lettura del dato, si noti che in taluni casi un progetto può essere afferente a diversi settori. Particolarmente virtuoso è stato il caso di un soggetto realizzatore che ha

coinvolto oltre 40 tra amministrazioni locali e *in-house*, operanti nei settori raccolta e igiene ambientale, trasporti e approvvigionamento di acqua potabile.

SETTORE	PROGETTI
Sanitario	41
Utilities (acque reflue, gestione rifiuti, acqua potabile)	20
Energia	7
Trasporti	6
Finanziario	6
Aerospazio e difesa	4
Telecomunicazioni	1

Analisi della postura di sicurezza della PA. Le iniziative finanziate con gli Avvisi 1, 2 e 3/2022 hanno permesso di fotografare lo stato di maturità della postura di sicurezza *cyber* delle Pubbliche Amministrazioni coinvolte. Al fine di monitorare tale maturità (e individuare come migliorarla), l'Agenzia ha identificato 6 diversi livelli (Figura 25) e le seguenti 6 dimensioni di intervento:

- ***governance* e programmazione *cyber***: coordinamento, supervisione e gestione della *cybersecurity*, attraverso la programmazione strategica di investimenti e iniziative;
- **gestione del rischio *cyber* e della continuità operativa**: individuazione, valutazione e trattamento sistematico dei rischi associati all'ambito *cyber* e implementazione di un piano di potenziamento volto a garantire la resilienza di funzioni e servizi critici in caso di eventi avversi;
- **gestione e risposta agli incidenti di sicurezza**: monitoraggio, identificazione e gestione degli incidenti *cyber* e ripristino dei sistemi impattati;
- **gestione delle identità digitali e degli accessi logici**: gestione delle identità e definizione dei permessi di accesso alle risorse, al fine di autenticare e autorizzare correttamente persone, gruppi e servizi in base agli attributi specifici e ai principi di "*need to know*", "*least privilege*" e "*segregation of duties*";
- **formazione e consapevolezza *cyber***: definizione e attuazione di piani strutturati per il miglioramento delle conoscenze in ambito *cyber*;

- **sicurezza delle applicazioni, dei dati e delle reti**: protezione dell'infrastruttura applicativa e di rete, e regolamentazione dei processi di protezione dei dati, al fine di prevenire potenziali incidenti *cyber* e di ridurne gli impatti.

LIVELLI DI MATURITÀ

MATURITÀ		DESCRIZIONE
INCOMPLETO	0	*Controlli non implementati o parzialmente implementati*
CONSIDERATO	1	*L'implementazione dei controlli è affidata a processi, procedure e soluzioni tecniche con risultati non prevedibili e non documentati. La gestione è affidata alle singole competenze del personale e non all'uso comprovato di processi ben definiti*
DEFINITO	2	*L'implementazione dei controlli si avvale di processi, procedure e soluzioni tecniche ben definiti e documentati nelle funzioni dell'organizzazione coinvolta, ma ciascuna funzione gestisce i propri processi, procedure e soluzioni tecniche in modo indipendente.*
AVVIATO	3	*L'implementazione dei controlli si avvale di processi, procedure e soluzioni tecniche ben definiti, documentati e standardizzati a livello di normativa interna dell'Amministrazione.*
IMPLEMENTATO	4	*Oltre a includere gli aspetti del livello di maturità "Avviato", sono fissati degli obiettivi quantitativi per quanto riguarda le performance dei processi, delle procedure e delle soluzioni tecniche alla base dell'implementazione dei controlli.*
OTTIMIZZATO	5	*Oltre a includere gli aspetti del livello di maturità "Implementato", i processi, le procedure e le soluzioni tecniche alla base dell'implementazione dei controlli sono sottoposti a miglioramento continuo in risposta a cambiamenti nell'Amministrazione e considerando le esperienze passate.*

Figura 25 – Livelli di maturità della postura di sicurezza *cyber* della PA

L'Agenzia, valutando per ciascuna dimensione di intervento il relativo livello di maturità, mette a disposizione di ciascuna Amministrazione un documento di analisi finalizzato a individuare con immediatezza lo stato di maturità, quello auspicato e le attività necessarie per potenziarlo. Tale documento è corredato di un grafico (esemplificato in Figura 26) che riassume visivamente i risultati dell'analisi: la maturità *"as is"* rappre-

senta l'effettivo stato dei presidi organizzativi, di processo e tecnologici della postura di cybersicurezza dell'organizzazione; quella *"quick win"* identifica gli obiettivi raggiungibili nel breve termine; il "*target*" è il livello di maturità auspicabile a esito di un piano pluriennale di potenziamento.

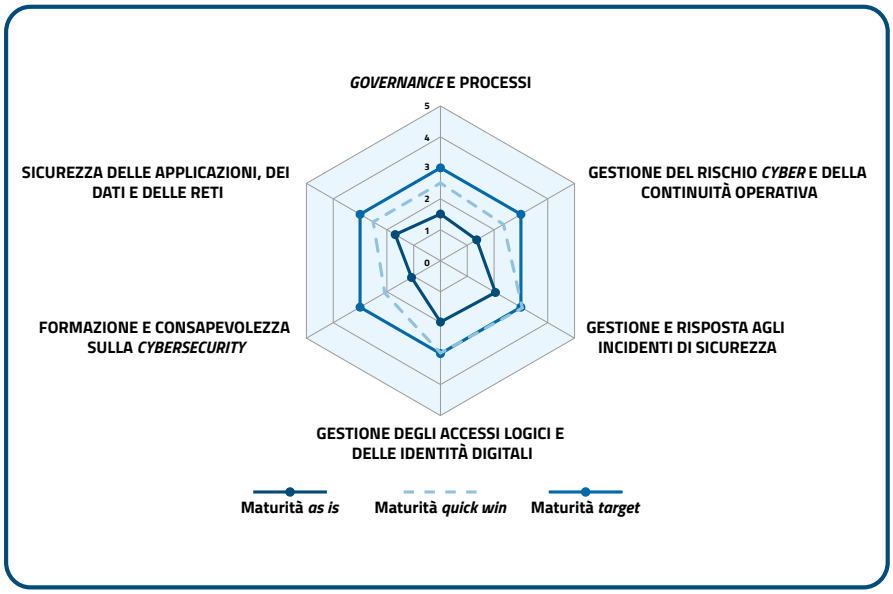


Figura 26 – Strumento esemplificativo

Grazie a tale analisi l'Agenzia ha accompagnato le amministrazioni coinvolte in un processo che ha consentito di intraprendere – e in taluni casi anche portare a termine – i primi interventi di potenziamento, raggiungendo, tra gli altri, i seguenti obiettivi:

- adottare una gestione centralizzata della cybersicurezza con la relativa definizione formale dei processi *cyber* (*governance* e programmazione *cyber*);
- definire la strategia e i relativi piani di continuità operativa, realizzare o, in taluni casi, ingegnerizzare i siti di *disaster recovery* e gli strumenti di *backup*, valutare i rischi *cyber* relativi alla gestione delle terze parti (gestione del rischio *cyber* e della continuità operativa);
- definire le modalità di gestione degli incidenti informatici e, contestualmente, formalizzare le procedure di *log management*, definire presidi h-24 per la gestio-

ne degli eventi di sicurezza, acquisire o realizzare strumenti adeguati a supporto della gestione degli incidenti informatici (gestione e risposta agli incidenti di sicurezza);

- definire e rendere attuabili i processi di gestione degli accessi logici, realizzare o acquisire soluzioni tecnologiche a supporto del suddetto processo, formalizzare i modelli operativi alla base della cybersicurezza (gestione degli accessi logici e delle identità digitali);
- implementare attività di sensibilizzazione del personale, acquisire strumenti informatici a supporto dei programmi formativi, definire piani di formazione diversificati per ruoli e posizioni organizzative (formazione e consapevolezza sulla *cybersecurity*);
- regolamentare i processi di protezione dei dati e di verifica dell'integrità dei sistemi informativi, adottare strumenti di *data loss prevention* e di *asset inventory* (sicurezza delle applicazioni dei dati e delle reti).

3.1.2 AVVISI PUBBLICATI NEL 2023 E PROSSIMI PASSI

Gli Avvisi pubblicati nel 2023 hanno permesso di proseguire quanto avviato dall'Agenzia nel corso del 2022, ampliando la platea dei soggetti potenzialmente interessati, in virtù dei positivi risultati riscontrati sia per la Pubblica Amministrazione centrale che locale.

In particolare, nel mese di ottobre del 2023 è stato pubblicato l'Avviso Pubblico 7/2023 che mira a dare seguito alle attività di potenziamento della capacità *cyber* offerte mediante l'Avviso 2/2022, concorrendo quindi al raggiungimento del *target* finale UE M1C1-19. L'Avviso 7/2023 prevede, infatti, interventi erogati dall'Agenzia a favore di ulteriori PA centrali, cioè tutte le amministrazioni che non hanno partecipato all'Avviso 2/2022 e altri soggetti destinatari (Organi costituzionali e a rilevanza costituzionale, Ministeri, Agenzie fiscali, Enti di regolazione dell'attività economica, Autorità amministrative indipendenti ed Enti a struttura associativa).

L'Avviso, con una dotazione finanziaria di 15 milioni di euro, si è chiuso il 5 dicembre e ha trovato ampia adesione. Gli interventi che saranno finanziati rientrano nelle seguenti tipologie:

- analisi della postura di sicurezza e piano di potenziamento;
- miglioramento dei processi e dell'organizzazione di gestione della *cybersecurity*;
- miglioramento della consapevolezza delle persone.

Ulteriori opportunità di finanziamento si apriranno nel corso del 2024, andando ad allargare la platea dei potenziali beneficiari delle attività di potenziamento della resilienza *cyber* a Pubbliche Amministrazioni locali al fine di sostenere la gestione del rischio *cyber*

di grandi Comuni, Città Metropolitane, Agenzie regionali sanitarie e aziende ed enti di supporto al Servizio sanitario nazionale, attraverso l'emanazione di apposito Avviso.

3.2 FOCUS SUI SERVIZI *CYBER* NAZIONALI

Fra gli obiettivi dell'Investimento 1.5 rientra la creazione e lo sviluppo di un insieme di servizi *cyber* nazionali, ovvero un gruppo organico di iniziative che mirano a mettere a disposizione strumenti all'avanguardia per la gestione del rischio cibernetico a livello nazionale, anche mediante sinergie con la Pubblica Amministrazione e il settore privato.

Fra le azioni e gli investimenti realizzati dall'Agenzia nel corso del 2023 si segnalano, in particolare, i seguenti:

- **CSIRT Italia e costruzione di una rete di CSIRT regionali**;
- **HyperSOC, infrastruttura HPC e strumenti di IA e ML**;
- **ISAC Italia e rete di ISAC settoriali**.

La realizzazione dei servizi *cyber* nazionali si accompagna necessariamente allo sviluppo delle piattaforme informatiche che, attraverso l'elaborazione delle informazioni di *cyber threat intelligence* dell'Agenzia e l'integrazione automatizzata dei *Security Operation Centre* (SOC) pubblici/privati sul territorio, permettono di calcolare e monitorare l'esposizione al rischio *cyber* della *constituency*. In particolare, a sostegno delle elevate capacità di scambio che dovrà gestire la piattaforma HyperSOC, è stata progettata, sviluppata e messa in produzione una *Cyber Data Platform* in grado di acquisire, archiviare, preparare e distribuire i dati raccolti, garantendo opportuna *governance* di sicurezza, *compliance* e *performance* per tutti i diversi livelli di utenti e fruitori della piattaforma. Inoltre, al fine di favorire l'utilizzo di tali servizi, l'ACN ha progettato e implementato un sistema centralizzato per la gestione dell'accreditamento dei soggetti e per la fruizione di specifiche informative *cyber*.

3.2.1 CSIRT ITALIA E COSTRUZIONE DI UNA RETE DI CSIRT REGIONALI

L'Agenzia sta lavorando alla creazione e al rafforzamento di una rete territoriale di CSIRT che si integrerà con il CSIRT Italia. A tale obiettivo, nel corso del 2023, è stato indirizzato uno specifico avviso (Avviso Pubblico 6/2023) che ha finanziato progetti volti a istituire o potenziare i CSIRT costituiti presso le Regioni o le Province autonome. Si tratta di squadre per la risposta agli incidenti informatici su base locale, deputate alla prevenzione e alla mitigazione del rischio *cyber*, che supportino il CSIRT Italia nella gestione delle vulnerabilità, nella condivisione di informazioni e della *situational awareness*, nel monitoraggio

del livello di protezione e rilevamento, nell'analisi e risposta degli incidenti di sicurezza informatica.

In linea con gli obiettivi trasversali del PNRR, tra cui quello della "doppia transizione verde e digitale", i progetti proposti hanno beneficiato di finanziamenti aggiuntivi nel caso in cui includessero anche attività di potenziamento dei servizi dei CSIRT regionali nei settori sanitario, dell'efficientamento energetico e della tutela del territorio e delle risorse idriche.

L'Avviso ha permesso di finanziare, con una dotazione complessiva di circa 28,5 milioni di euro, i progetti presentati da 19 amministrazioni, come riportato nella Figura 27.

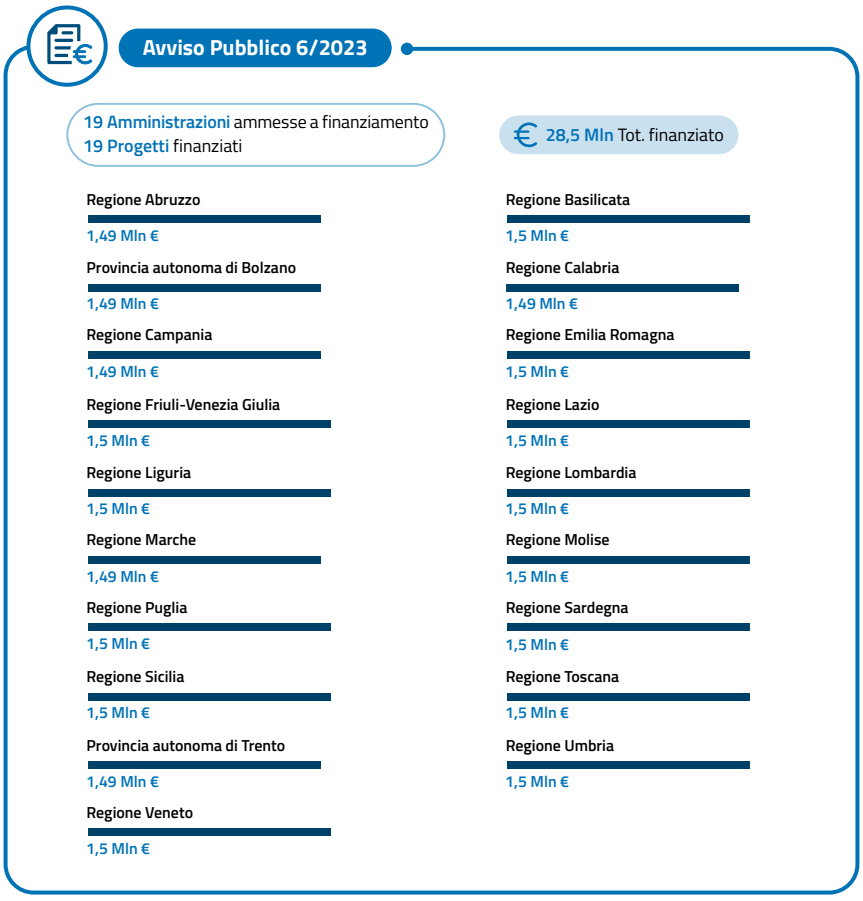


Figura 27 – Avviso 6/2023 Ammissione a finanziamento

A sostegno delle funzioni dei CSIRT regionali saranno realizzati degli ambienti specifici, dedicati alle attività di analisi forense, utili alla risposta e alla gestione degli incidenti informatici, allo scopo di sostenere le Pubbliche Amministrazioni nella mitigazione dei rischi e nella prevenzione di future intrusioni.

3.2.2 HYPERSOC, INFRASTRUTTURA HPC E STRUMENTI DI IA/ML

Un secondo ambito di intervento principale riguarda la creazione di un *Security Operations Centre* nazionale (HyperSOC), dedicato al monitoraggio degli eventi *cyber,* specie in ottica preventiva e di azione integrata. L'HyperSOC interagirà con i diversi SOC pubblici/privati presenti sul territorio, permettendo di calcolare e monitorare l'esposizione al rischio *cyber* del perimetro esposto della *constituency*. Per fare fronte a scenari di complessità crescente, si rende inoltre necessario il ricorso a piattaforme di calcolo e strumenti algoritmici innovativi, tramite la creazione di una infrastruttura di *High Performance Computing*, accompagnata da strumenti di simulazione basati su Intelligenza Artificiale e *machine learning* per una più efficace analisi della minaccia.

Il sistema di HPC che sosterrà le esigenze computazionali dell'HyperSOC si collocherà presso il nuovo centro di calcolo del consorzio CINECA, a Napoli, grazie alla firma di uno specifico accordo in base al quale il Consorzio realizzerà per conto dell'ACN l'HPC dedicato all'ecosistema nazionale della cybersecurity. L'investimento dell'Agenzia ammonta a oltre 20 milioni di euro a valere sui fondi PNRR. Sempre il medesimo accordo prevede la progettazione di un *data center* per l'HPC dell'Agenzia, anche con lo sviluppo dei primi prototipi in ambito di intelligenza artificiale generativa, che andrà altresì a potenziare l'HyperSOC con avanzati algoritmi di IA e *machine learning*.

3.2.3 ISAC ITALIA E RETE DI ISAC SETTORIALI

Il terzo pilastro dei servizi *cyber* nazionali – cui è dedicata una dotazione di 12,3 milioni di euro – è rappresentato dalla costituzione di una rete di ISAC settoriali, da integrare con le strutture dell'ACN, per diffondere su tutto il territorio informazioni sullo stato della minaccia *cyber* così da consentire lo scambio di raccomandazioni e buone pratiche a sostegno della resilienza complessiva del Paese. Presso l'Agenzia verrà quindi istituito ISAC Italia, che permetterà di raccogliere e condividere informazioni di tipo strategico, tattico e operativo in risposta all'evoluzione del panorama globale e settoriale della minaccia. Questo sarà collegato, da un lato, alla rete di ISAC settoriali, da costituire tramite iniziative pubblico-private coordinate dall'ACN, e, dall'altro, con la rete europea degli ISAC, contribuendo alla creazione dello *European CyberShield* previsto dal *Cyber Solidarity Act*.

Nel corso del 2023, le attività svolte hanno riguardato sia il lavoro in vista dell'istituzione di ISAC Italia, sia quello rivolto alla facilitazione della costituzione di una rete nazionale di ISAC settoriali. Quanto al primo filone, è stato intrapreso un esame dettagliato delle comparabili realtà internazionali, sulla cui base identificare le capacità da espandere e progettare le attività da sviluppare, anche in relazione alla relativa *governance*. In merito al secondo punto, sono stati identificati i settori di riferimento per la futura costituzione dei relativi ISAC e, in particolare: spazio, aerospazio e difesa; energetico; servizi finanziari; sanitario; manufatturiero; tecnologie critiche e infrastrutture digitali; telecomunicazioni e servizi digitali; trasporti; gestione di acque reflue, rifiuti e acqua potabile.

È stato, inoltre, realizzato un programma pilota a supporto degli *stakeholder* interessati alla costituzione di un ISAC di settore, attraverso il quale ISAC Italia coinvolgerà inizialmente determinati soggetti attivi nel settore di riferimento, supportandoli quindi nel processo di creazione del relativo ISAC e della conseguente associazione alla rete nazionale di ISAC.

3.3 LABORATORI DI SCRUTINIO E CERTIFICAZIONE TECNOLOGICA

L'Agenzia è impegnata, inoltre, a sostenere la costituzione di una rete di laboratori di scrutinio tecnologico a supporto del CVCN, che dovranno conseguire l'accreditamento come Laboratori accreditati di prova (vds. capitolo 2). A tal fine, è stato promosso l'Avviso 5/2022, per individuare progetti di creazione o rafforzamento di laboratori dedicati alla valutazione e allo scrutinio tecnologico della sicurezza degli apparati elettronici

e delle applicazioni utilizzate per reti, sistemi informativi e servizi informatici da cui dipendano funzioni o servizi essenziali dello Stato e dal cui malfunzionamento, interruzione, o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Mediante tale Avviso sono stati stanziati 5 milioni di euro per progetti di soggetti, sia pubblici che privati, prevedendo l'erogazione di contributi finanziari ai sensi del Regolamento "*de minimis*", (UE) n. 1407/2013. Conseguentemente, nella prima metà del 2023 l'Agenzia ha individuato le proposte ammissibili al finanziamento, svolgendo i controlli previsti per legge sui soggetti partecipanti, insieme ai necessari adempimenti sul Registro nazionale degli aiuti di Stato, determinando infine la concessione del finanziamento a 27 soggetti, che sarà poi perfezionato solo all'esito positivo del processo di accreditamento (Figura 28).

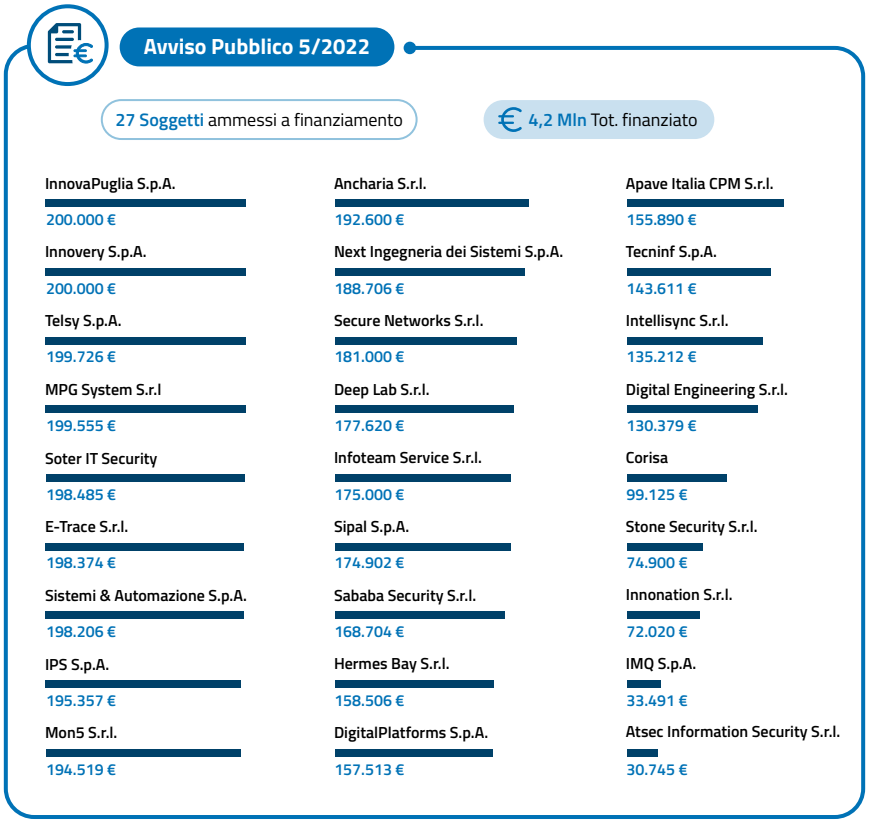


Figura 28 – Avviso 5/2022 Ammissione a finanziamento

4.

COOPERAZIONE INTERNAZIONALE

Il 2023 ha visto un'intensa attività internazionale dell'ACN, che ha approfondito le proprie relazioni in molteplici direzioni, sia a livello bilaterale che multilaterale, oltre che nell'articolato quadro della *governance cyber* dell'Unione europea. In costante raccordo con il Ministero degli affari esteri e della cooperazione internazionale (MAECI), le attività dell'Agenzia hanno sostenuto la più ampia proiezione internazionale, privilegiando il rafforzamento dei rapporti non solo con omologhe agenzie dei Paesi *like-minded*, ma anche con quelle del vicinato strategico, in particolare del Mediterraneo allargato e dei Balcani.

Il potenziamento del ruolo internazionale dell'ACN, a tutti i livelli, ha permesso di consolidare un rapporto di fiducia e collaborazione con altri Paesi, con un impatto diretto sugli obiettivi di resilienza e sicurezza *cyber*, ad esempio attraverso il dialogo e lo scambio informativo e di buone prassi per affrontare sfide comuni e transnazionali. A livello bilaterale, l'Agenzia ha condotto incontri al vertice con autorità competenti sulla cybersicurezza, oltre a interlocuzioni con Ambasciate e delegazioni estere, anche finalizzate alla sottoscrizione di protocolli di intesa. In ambito europeo, al contributo sui negoziati in corso per rafforzare l'impianto regolatorio dell'UE, si sono accompagnate molteplici attività – a livello tecnico e operativo oltre che di *policy* – volte a rafforzare la postura di sicurezza e resilienza *cyber* dell'Unione. Infine, l'Agenzia ha favorito la partecipazione italiana in diversi consessi multilaterali che trattano tematiche *cyber* per la definizione di politiche comuni che promuovano l'interesse nazionale.

4.1 COOPERAZIONE BILATERALE

L'estensione dei rapporti bilaterali si è rilevata strumentale per assicurare la missione dell'Agenzia. Nel corso del 2023 sono stati effettuati incontri al vertice con le corrispondenti agenzie di Belgio, Romania, Francia, Israele, Lussemburgo, Tunisia e Stati Uniti. Di notevole rilievo è stata la visita a Washington del novembre 2023, nel corso della quale gli incontri, in particolare, con la Direttrice della *Cybersecurity and Infrastructure Security Agency* (CISA) e il Vice Consigliere del Presidente USA per la Sicurezza Nazionale, hanno messo in luce gli elementi di convergenza che esistono tra USA, Italia e UE nello sforzo collettivo di assicurare la gestione della sicurezza digitale, anche attraverso la cooperazione internazionale e l'impegno nelle sedi multilaterali. Si è potuta, inoltre, registrare una forte convergenza sull'iniziativa dell'ACN di costituire un gruppo di lavoro in ambito G7 fra le agenzie e i centri responsabili per la cybersicurezza, durante la Presidenza italiana del 2024. Infine, la condivisione con la CISA delle valutazioni sul nesso fra Intelligenza Artificiale e cybersicurezza, in linea con l'indirizzo politico del Presidente del Consiglio dei

ministri espresso al Summit di Bletchley Park su *AI Safety* di novembre, ha favorito l'adesione dell'ACN al documento sulle "Linee guida per uno sviluppo sicuro dell'Intelligenza Artificiale", adottato da agenzie di 18 Paesi (di cui si parlerà più approfonditamente nel prosieguo).

Sono stati, inoltre, avviati negoziati per rafforzare la cooperazione attraverso protocolli d'intesa con agenzie per la cybersicurezza di Albania, Giordania, Israele, Romania, Ruanda, Slovenia, Spagna e Stato della Città del Vaticano. Il 28 settembre a Tunisi, in occasione della missione del Direttore generale, è stato firmato il protocollo d'intesa fra l'ACN e l'Agenzia nazionale per la cybersicurezza tunisina (l'ANCS-*Agence Nationale de la Cybersécurité*). La collaborazione prevede lo scambio di informazioni sugli attacchi informatici e l'organizzazione di attività di formazione, ricerca e scambio di esperti. Si è trattato del primo accordo stipulato dall'ACN con una omologa agenzia estera, la cui particolare valenza è rappresentata anche dalla collocazione della Tunisia in un quadrante altamente strategico per il Paese.

L'intensificazione dei rapporti con omologhe agenzie europee, quali ad esempio il BSI tedesco, l'ANSSI francese, l'INCIBE spagnola, il CCB belga, ha consentito all'ACN uno scambio di esperienze sulle minacce cibernetiche e un maggior dialogo sui principali negoziati in ambito UE, nonché su aspetti rilevanti per l'operatività dell'Agenzia, quali la proposta di schema europeo di certificazione per i servizi *cloud*.

Sono stati anche intensificati i rapporti in tema di cybersicurezza con Ambasciate e delegazioni di Canada, Danimarca, Emirati Arabi Uniti, Giordania, Israele, Lituania, Regno Unito, Repubblica Ceca, San Marino, Slovacchia, Stato della Città del Vaticano, Stati Uniti e Ucraina con autorità governative di Albania, Germania, Grecia, Libia, Romania, Slovenia, Spagna.

4.2 ATTIVITÀ IN AMBITO EUROPEO

4.2.1 NORMATIVE E *POLICY* UE IN MATERIA *CYBER*

L'Agenzia ha continuato ad assicurare – in stretto raccordo con il MAECI e, in particolare, con la Rappresentanza Permanente d'Italia presso l'Unione europea – la propria partecipazione ai lavori dell'*Horizontal Working Party on Cyber Issues* (HWPCI), per la trattazione di questioni relative a *policy* e atti normativi in materia di resilienza e sicurezza *cyber*.

Horizontal Working Party on Cyber Issues

HWPCI è il gruppo orizzontale, istituito nel 2016, responsabile del coordinamento dei lavori del Consiglio dell'UE sulle questioni relative alla cybersicurezza, in particolare le politiche e le attività legislative in materia. Ha il fine di assicurare un approccio unitario e armonizzato alle politiche cyber, che tenga conto delle evoluzioni della minaccia, nonché di definire le priorità dell'UE in materia di cybersicurezza e di garantire la condivisione informativa all'interno del Consiglio e tra gli Stati membri.

Nello specifico, durante il 2023 l'ACN si è dedicata principalmente alle seguenti proposte di Regolamento:

- Regolamento per la cybersicurezza dei diversi organismi UE, che stabilisce misure per un livello comune elevato di cybersicurezza nelle istituzioni, negli organi, negli uffici e nelle agenzie dell'Unione e che è stato pubblicato sulla Gazzetta Ufficiale dell'Unione europea a dicembre per la sua entrata in vigore a gennaio 2024 (Regolamento (UE, Euratom) 2023/2841);
- *Cyber Resilience Act* (CRA), sui requisiti di cybersicurezza dei prodotti con componenti digitali e per il quale è stato raggiunto l'accordo sul testo in occasione del trilogo politico del 30 novembre 2023;
- *Cyber Solidarity Act* (CSoA), che introduce misure per rafforzare la solidarietà e le capacità dell'UE di individuazione, preparazione e risposta alle minacce e agli incidenti di cybersicurezza, i cui negoziati in ambito HWPCI sono stati avviati a settembre 2023;
- emendamenti al *Cybersecurity Act* con riguardo ai servizi di sicurezza gestiti per i quali, dopo un rapido negoziato in seno al HWPCI, avviato anch'esso nel settembre 2023, è stato raggiunto l'accordo sul testo a seguito del trilogo politico del 4 dicembre 2023.

CYBER SOLIDARITY ACT

Il 18 aprile 2023 la Commissione europea ha presentato la proposta di Regolamento sul *Cyber Solidarity Act*, che prevede:

- la creazione di una infrastruttura di SOC nazionali, integrati a livello paneuropeo, tenuti alla condivisione delle informazioni all'interno della UE per sviluppare e potenziare capacità comuni in materia di rilevamento e conoscenza situazionale di minacce e incidenti *cyber*;
- la definizione di "procedure di emergenza *cyber*", che contemplano, fra l'altro, un meccanismo di riserva di capacità nella gestione degli incidenti *cyber* su larga scala, garantito da operatori fiduciari del settore privato, che potranno essere dispiegate su richiesta dello Stato membro interessato ovvero di istituzioni, organismi e agenzie UE. Tali operatori dovranno essere certificati sulla base dello schema che sarà adottato per la certificazione dei servizi di sicurezza gestiti, ai sensi del *Cybersecurity Act* (Regolamento (UE) 2019/881);
- la realizzazione di un "meccanismo di esame degli incidenti *cyber*" per valutare ed esaminare specifici incidenti di cybersicurezza. Su richiesta della Commissione o delle autorità nazionali nell'ambito della rete CyCLONe o della rete dei CSIRT, l'ENISA è chiamata a esaminare specifici incidenti *cyber* significativi o su larga scala e a presentare una relazione che includa lezioni apprese e raccomandazioni per migliorare la risposta dell'Unione.

I fondi per realizzare tali iniziative proverranno dall'obiettivo strategico *"cybersecurity"* del *Digital Europe Programme* e saranno gestiti attraverso il Centro europeo di competenze in *cybersecurity*.

EMENDAMENTI AL *CYBERSECURITY ACT*

Il 18 aprile 2023 la Commissione europea ha presentato la proposta di Regolamento contenente emendamenti al *Cybersecurity Act* finalizzati all'adozione di sistemi europei di certificazione della cybersicurezza anche per i "servizi di sicurezza gestiti", in aggiunta ai prodotti, processi e servizi ICT già coperti dal CSA. In particolare, la proposta prevede l'introduzione di specifici obiettivi di sicurezza degli schemi europei di certificazione della cybersicurezza per i richiamati servizi.

Tale certificazione dovrà attestare che anche i predetti servizi soddisfino i requisiti di sicurezza specificati, al fine di proteggere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati cui si accede, che si elaborano, si conservano o si trasmettono in relazione alla fornitura di tali servizi, e che gli stessi siano forniti in modo continuativo con la competenza e l'esperienza richieste da personale con un livello molto elevato di conoscenze tecniche e integrità professionale.

Rispetto alle ultime due proposte (CSoA ed emendamenti al CSA), il Direttore generale dell'ACN ha avuto, altresì, modo di illustrare in sede parlamentare, nell'ambito dell'audizione informale svolta il 26 ottobre 2023, presso la 4ª Commissione (Politiche dell'Unione europea) del Senato della Repubblica, le diverse attività che l'Agenzia sta portando avanti a livello UE sui temi del rafforzamento dello spazio cibernetico, in collaborazione con gli altri Stati membri e le istituzioni europee. Il Direttore generale ha svolto, inoltre, un'ulteriore audizione informale, il 19 aprile 2023, presso la XIV Commissione (Politiche dell'Unione europea) della Camera dei deputati, nell'ambito dell'esame della Comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo e al Consiglio "La politica di ciberdifesa dell'UE".

Audizione del Direttore generale dell'ACN al COPASIR

Oltre alle audizioni parlamentari richiamate nel testo, il Direttore generale dell'Agenzia è stato udito il 18 aprile dal Comitato parlamentare per la sicurezza della Repubblica (COPASIR) nell'ambito delle funzioni di controllo svolte dal Comitato sulle attività dell'Agenzia concernenti la tutela della sicurezza nazionale nello spazio cibernetico.

Sempre in ambito HWPCI, inoltre, l'Agenzia ha provveduto a fornire pareri anche per la definizione di *dossier* politici quali le Conclusioni del Consiglio sulla politica dell'Unione in tema di *cyber defence*, adottate nel novembre 2023, e la revisione delle Linee guida sul *Cyber Diplomacy Toolbox*. In aggiunta, contributi sono stati forniti anche nel corso dei negoziati di altri atti normativi dell'Unione con un *focus* più ampio rispetto alla materia *cyber*, come la proposta di Regolamento che stabilisce regole armonizzate sull'Intelligenza Artificiale (*Artificial Intelligence Act* o *AI Act*) e le modifiche al Regolamento sull'identificazione elettronica e i servizi fiduciari (eIDAS2).

PROPOSTA DI REGOLAMENTO *AI ACT*

La proposta di Regolamento che stabilisce regole armonizzate sull'Intelligenza Artificiale (*AI Act*) mira a garantire il buon funzionamento del mercato interno per lo sviluppo, la commercializzazione e l'utilizzo dei sistemi di Intelligenza Artificiale e a sostenere la *leadership* dell'Unione europea in materia. La proposta, adottando un approccio proporzionato basato sul rischio, prevede la proibizione delle applicazioni dell'IA contrarie ai valori dell'Unione e responsabilità crescenti per i fornitori di sistemi maggiormente rischiosi. Stabilisce, inoltre, degli obblighi di trasparenza nell'impiego di alcuni sistemi specifici di IA – in particolare quando vengono utilizzati *chatbot* o *deep fake* – e introduce misure aggiuntive per favorire l'innovazione, prevedendo specifiche misure per sostenere i fornitori di piccole dimensioni. A livello di *governance*, la proposta introduce l'istituzione di un Comitato europeo per l'Intelligenza Artificiale costituito da rappresentanti degli Stati membri e della Commissione. Gli Stati membri designano una o più autorità competenti, tra cui un'autorità di controllo.

Nel trilogo sulla proposta di Regolamento, Consiglio, Parlamento e Commissione hanno raggiunto l'accordo politico sulle norme fondamentali il 9 dicembre 2023.

4.2.2 RAFFORZAMENTO DELLA POSTURA DI SICUREZZA DELL'UE

L'ACN ha attivamente preso parte alle numerose attività di **ENISA.** In particolare, oltre all'incontro bilaterale a livello di vertice, è stato dato il contributo di competenza sia all'interno del *Management Board*, organo di governo interno, sia nella rete dei funzionari di collegamento (*National Liaison Officer*-NLO). Nel corso dell'anno l'ACN, pertanto, ha preso parte alle riunioni del *Management Board* e agli incontri della rete dei NLO, oltre che a quelli dei relativi sottogruppi di lavoro, quali:

- *"EU Cybersecurity Index"*, nel cui ambito si è contribuito ad affinare tale strumento e a partecipare al secondo esercizio pilota, in vista dell'ufficializzazione dell'Indice, che avverrà nel 2024. Tale Indice è volto a valutare e a incrementare i livelli di maturità dell'Unione e degli Stati membri nelle seguenti aree: *policy*, capacità, operatività, sviluppo del mercato e del settore industriale. Il contributo nazionale per la corrente edizione è stato elaborato grazie anche alla proficua collaborazione con altre amministrazioni (Ministeri dell'interno, della giustizia, dell'impresa e del *made in Italy*, dell'università e della ricerca, dell'istruzione e del merito e DTD);
- *"National Cybersecurity Strategies"*, portando come caso-studio l'esperienza maturata nell'ambito dell'attuazione della Strategia nazionale di cybersicurezza 2022-2026.

Da segnalare, inoltre, la designazione, nel corso del 2023, di un osservatore permanente dell'Agenzia nell'ambito dell'"*Ad Hoc Working Group on Cybersecurity Skills*", con l'obietti-

vo di supportare ENISA nelle attività di *governance*, implementazione e futuro sviluppo dell'*European Cybersecurity Skills Framework* (ECSF). Rileva, infine, che per le attività di promozione della cultura della cybersicurezza l'ACN funge da *National Campaign Coordinator* per le iniziative relative al mese europeo della cybersicurezza (vds. capitolo 5).

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Il Quadro europeo per le capacità di cybersicurezza è il punto di rifermento dell'Unione per la definizione e valutazione delle capacità *cyber* per i diversi profili professionali in materia. Lo strumento mira a:

- sviluppare uno standard comune, a livello europeo, di ruoli, capacità, competenze e conoscenze nel settore della *cybersecurity*, ad uso di organizzazioni, pubbliche e private, che necessitano di reclutare specifiche professionalità;
- agevolare la predisposizione di programmi di formazione in tale ambito e, conseguentemente, la creazione di una forza-lavoro europea specializzata;
- facilitare l'orientamento nel percorso di studi per i giovani che intendono intraprendere una carriera nel campo;
- costituire un utile strumento per attività di *capacity building*.

L'Agenzia svolge inoltre le funzioni di **Centro nazionale di coordinamento** (NCC), interfacciandosi con il **Centro europeo di competenze in cybersicurezza** (*European Cybersecurity Competence Centre*-**ECCC**) per supportarlo nell'attuazione di iniziative volte a rafforzare lo sviluppo industriale, in tecnologia e ricerca in *cybersecurity*. In particolare, l'ECCC è chiamato a gestire le opportunità di finanziamento in ambito industriale, di investimento e di innovazione in cybersicurezza, offerte dai programmi *Digital Europe Programme* (DEP) e *Horizon Europe*.

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE ITALY

Nel 2023, l'ACN ha partecipato a due bandi DEP, aggiudicandosi in entrambi i casi il finanziamento. Tramite uno di tali bandi, diretto allo sviluppo dei diversi Centri nazionali di coordinamento, è stato avviato a partire da novembre 2023 il progetto NCC-IT, volto a sostenere la piena capacità operativa dell'NCC italiano con un *budget* di 2 milioni di euro. Per quanto riguarda il secondo, l'ACN partecipa, all'interno di un consorzio che include rilevanti amministrazioni di altri 6 Stati membri, al progetto ENSOC che partirà nei primi mesi

del 2024 e mira a sviluppare la rete europea dei SOC con un *budget* di 24 milioni di euro, contribuendo a mettere a sistema le iniziative già avviate a livello nazionale con il PNRR.

PROGRAMMI *DIGITAL EUROPE* E *HORIZON EUROPE*

L'Agenzia, nel ruolo di NCC, ha monitorato e promosso le opportunità di finanziamento in ambito industriale, di investimento e di innovazione in cybersicurezza, offerte dai programmi *Digital Europe Programme* e *Horizon Europe*, gestite dall'ECCC.

- Il DEP – con un budget, per l'anno 2023, di 161 milioni di euro – ha finanziato bandi che hanno riguardato, in particolare: il rafforzamento dei SOC nazionali e dell'ecosistema SOC europeo; lo sviluppo di capacità delle piattaforme transfrontaliere di *cyber threat detection*; l'attuazione del *Cybersecurity Emergency Mechanism*; il coordinamento e le sinergie tra la sfera *cyber* civile e militare; il supporto alla definizione degli standard armonizzati per l'applicazione del *Cyber Resilience Act*; il *capacity building* e la cooperazione nell'ambito delle norme europee in materia di cybersicurezza.
- Il fondo *Horizon Europe* – con un budget, per il 2023, di 58,7 milioni di euro – ha finanziato progetti relativi alla sicurezza dei sistemi, delle piattaforme e delle infrastrutture digitali, allo sviluppo di tecnologie in ambito *identity management* e *privacy,* nonché alla sicurezza dei sistemi di Intelligenza Artificiale.

L'Agenzia rappresenta l'Italia nel *Governing Board* dell'ECCC, che definisce gli indirizzi di investimento in cybersicurezza e la gestione delle relative opportunità. Tra questi, l'adozione della *ECCC Strategic Agenda,* documento strategico contenente gli obiettivi che il Centro europeo intende raggiungere entro il 2027. Nella sua seduta di ottobre il *Governing Board* ha eletto il Direttore Esecutivo del Centro, scegliendo il dott. Luca Tagliaretti, la cui candidatura è stata fortemente sostenuta dal Governo e dalla ACN stessa.

Un ulteriore filone di attività in ambito UE che ha coinvolto attivamente l'Agenzia è costituito dal **Gruppo di cooperazione NIS** (*NIS Cooperation Group*-NISCG), istituito dalla già richiamata Direttiva NIS e confermato dalla NIS 2, con un mandato più esteso, quale snodo centrale per assicurare un'efficace e armonizzata implementazione della disciplina. In tale contesto, l'Agenzia ha assicurato la partecipazione alle riunioni plenarie annuali, oltre che ai periodici punti di situazione e delibere sulle attività dei gruppi di lavoro del NISCG, che hanno consentito un confronto sul Programma di lavoro biennale 2024-2026.

I lavori del NISCG sono infatti organizzati in 16 gruppi di lavoro, c.d. *Work Streams*, nei quali gli esperti delle autorità competenti NIS si confrontano su temi orizzontali e setto-

riali. L'Agenzia segue i lavori di tutti i gruppi di lavoro (nel 2023 ha partecipato a oltre 43 incontri), e detiene la co-presidenza di 3. Tra le numerose iniziative condotte nel 2023, sono di particolare rilievo i lavori del:

- *Work Stream on Telecom Cybersecurity* e del *Work Stream on Risk Evaluation,* nell'ambito dei quali l'ACN, in qualità di co-presidente, ha svolto un ruolo propulsore: nel primo *Work Stream,* in relazione al dibattito sulla pubblicazione della seconda relazione sullo stato di attuazione del *Toolbox on 5G Cybersecurity* e alle attività volte a finalizzare l'analisi del rischio nel settore delle telecomunicazioni dell'UE; nel secondo gruppo di lavoro, per lo sviluppo delle analisi e degli scenari di rischio per l'intera Unione;
- *Work Stream on Cybersecurity Risk and Vulnerability Management*, che ha portato alla pubblicazione delle linee guida per la definizione delle *policy* nazionali di divulgazione coordinata delle vulnerabilità. Inoltre, importante è stato il contributo dell'ACN per l'elaborazione degli elementi tecnici necessari per l'adempimento degli obblighi in materia di misure di sicurezza per le categorie di soggetti considerate intrinsecamente transfrontaliere[13], che sono stati forniti alla Commissione UE in vista dell'adozione del relativo atto di esecuzione, prevista entro ottobre 2024;
- *Work Stream on Incident Notification* e *Work Stream on Digital Infrastructure and Service*, nell'ambito dei quali l'ACN ha contribuito a precisare gli elementi tecnici necessari per l'elaborazione dell'atto di esecuzione sugli obblighi di notifica per i soggetti che erogano servizi intrinsecamente transfrontalieri.

Per altro verso, l'Agenzia ha partecipato intensamente agli incontri periodici della rete di collaborazione europea ***CSIRTs Network***, che riunisce i diversi CSIRT degli Stati membri, oltre al CERT-EU, per uno scambio informativo a livello di Unione e per l'esame delle eventuali risposte agli incidenti. L'ACN è stata presente nei diversi gruppi di lavoro nati in questo ambito, come il gruppo di lavoro che produce, con cadenza quadrimestrale, il *EU Joint Cyber Assessment Report* di ENISA[14], quello dedicato al supporto degli CSIRT degli Stati membri per la definizione delle procedure di diffusione coordinata delle vulnerabilità, previste dalla Direttiva NIS 2, partecipando anche ad altri gruppi, di natura più tecnica, sulle procedure operative, sulla strumentazione e sulla valutazione del livello di maturità *cyber*.

---

[13] Si fa, in particolare, riferimento ai fornitori di servizi di sistemi di nomi di dominio, ai registri dei nomi di dominio di primo livello, ai fornitori di servizi di *cloud computing*, ai fornitori di servizi di *data center,* ai fornitori di reti di distribuzione dei contenuti, ai fornitori di servizi gestiti, ai fornitori di servizi di sicurezza gestiti, ai fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di *social network,* nonché ai prestatori di servizi fiduciari.

[14] Si tratta del rapporto sull'andamento degli incidenti e delle minacce nell'Unione, redatto congiuntamente da ENISA, EUROPOL e CERT-EU, a partire dai contributi degli CSIRT degli Stati membri e destinato al Consiglio europeo, alla Commissione e all'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza.

È stata inoltre parte attiva nello scambio di informazioni di natura tecnica tramite i canali messi a disposizione dal *CSIRTs Network*, proprio al fine di consentire la collaborazione con gli CSIRT degli altri Stati membri. Sempre in tale ambito, sono stati, altresì, condotti diversi incontri con omologhe agenzie e strutture estere con lo scopo di attivare nuovi canali di scambio informativo.

Nell'ambito delle attività per l'elaborazione degli schemi europei di certificazione della cybersicurezza, l'ACN ha assicurato la propria partecipazione alle riunioni dello ***European Cybersecurity Certification Group*** (ECCG), comitato consultivo della Commissione europea per l'attuazione del *Cybersecurity Act*, che emette pareri obbligatori e vincolanti sui sistemi di certificazione europea. Ha inoltre partecipato ai lavori del comitato che assiste la Commissione europea nella procedura d'esame per l'adozione degli atti esecutivi relativi agli schemi di certificazione, attivato, per la prima volta, alla fine del 2023 in vista dell'adozione del già citato schema di certificazione europeo *Common Criteria* (vds. capitolo 2).

Tra i vari tavoli europei, l'ACN dedica particolare attenzione agli sviluppi delle nuove tecnologie, partecipando ad esempio al *Crypto Subgroup* dell'ECCG, sulla validazione di algoritmi crittografici supportati dallo schema di certificazione EUCC, che nei prossimi anni lavorerà alla redazione di documenti condivisi contenenti le liste delle soluzioni crittografiche supportate dall'EUCC e le modalità di test per la loro corretta implementazione e validazione.

Da ultimo, si richiama il lavoro condotto dall'Agenzia in seno alla ***European Competent Authority on Secure Electronic Communications***, nata con lo scopo di agevolare le interazioni tra le autorità nazionali responsabili dell'integrità delle reti di telecomunicazione, di cui al Codice europeo delle comunicazioni elettroniche. In tale consesso, vengono discussi gli approcci di supervisione nel settore delle telecomunicazioni e definiti gli oneri in materia di misure di sicurezza e obblighi di notifica armonizzati. L'adozione della Direttiva NIS 2, che prevede l'assorbimento degli aspetti di cybersicurezza del citato Codice, ha innescato un rafforzamento del confronto tra questo consesso e i gruppi di lavoro del NISCG in tale ambito, per definire i rispettivi aspetti di competenza, favorendo sinergie ed evitando sovrapposizioni.

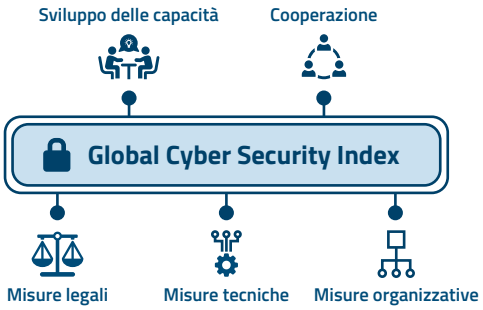
Sempre in ambito UE, nel luglio 2023 l'Agenzia ha aderito all'iniziativa denominata *Cyber Capacity Building Network* (*CyberNet*), avviata nel 2019 al fine di assicurare il coordinamento tra le diverse attività di *capacity building* realizzate dagli Stati membri a beneficio di Paesi terzi, rafforzando al contempo la capacità di fornire assistenza tecnica nel settore della cybersicurezza e nel contrasto della criminalità informatica. In particolare, l'ACN ha aderito alla *"Stakeholder community"* con l'obiettivo di condividere le relative esperienze e capacità in materia di *cyber capacity building*. La comunità è costituita da più di 60 membri tra autorità nazionali *cyber*, Ministeri, organizzazioni non governative,

think tank e istituzioni accademiche dei Paesi UE e di Stati *partner*, nonché di organismi internazionali.

4.3 AMBITO MULTILATERALE

L'Agenzia è presente anche nei competenti consessi multilaterali in ambito ONU, NATO, OSCE, G20 e G7.

In particolare, a livello **ONU** l'ACN ha partecipato ai due gruppi di lavoro istituiti per la definizione della quinta edizione del *Global Cyber Security Index*, il cui obiettivo è consentire ai Paesi aderenti di accrescere il proprio complessivo livello di cybersicurezza, identificando le aree di possibile miglioramento. Tale esercizio prevede, infatti, la predisposizione di contributi nazionali su 5 aree tematiche – misure legali, misure tecniche, misure organizzative, sviluppo delle capacità e cooperazione – in relazione alle quali hanno fornito un contributo anche Ministero dell'interno, MIMIT, Ministero dell'università e della ricerca (MUR) e Ministero dell'istruzione e del merito (MIM).



Inoltre, sempre in ambito ONU, l'Agenzia ha seguito i lavori per la definizione di una "*Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*", partecipando agli incontri del gruppo di lavoro coordinato dalla Farnesina e composto dagli esperti del Ministero della giustizia e del Ministero dell'interno, per assicurare la coerenza dell'architettura nazionale di cybersicurezza e del relativo quadro normativo e di *policy*, cercando anche di mantenere, per quanto possibile, l'impianto della Convenzione del Consiglio d'Europa sulla criminalità informatica (c.d. Convenzione di Budapest), ampiamente applicata a livello internazionale.

Con riguardo alle attività in ambito **NATO**, l'Agenzia ha continuato a seguire l'evoluzione delle politiche in materia di *cyber defence*, relativamente agli aspetti di resilienza e sicurezza cibernetica, in raccordo con la Rappresentanza Permanente d'Italia presso il Consiglio Atlantico, nell'ambito del *Cyber Defence Committee*. In particolare, l'ACN ha contribuito allo sviluppo della "*Virtual Cyber Incident Support Capability*", strumento di assistenza reciproca a sostegno degli sforzi nazionali di mitigazione degli effetti di significative attività *cyber* malevole, lanciato in occasione del Vertice dei Capi di Stato e di Governo tenutosi a

Vilnius a luglio 2023. L'Agenzia ha partecipato, inoltre, assieme al MAECI e al Ministero della difesa, alla prima edizione della *Annual Cyber Defence Conference* che, nel mese di novembre, ha riunito rappresentanti in ambito politico, militare e tecnico per una discussione sulle priorità e sull'impegno della NATO in materia di difesa *cyber*, in vista del prossimo Vertice dell'Alleanza, che si terrà a Washington nel luglio 2024.

In ambito **OSCE**, è proseguito il supporto fornito dall'Agenzia al MAECI nell'attuazione delle *Confidence-Building Measure* (CBM) e, specialmente, della CBM n. 14 in materia di *partnership* pubblico-privato (PPP)[15], contribuendo, sotto il profilo contenutistico, alla predisposizione del rapporto *"Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE Participating States"* (pubblicato a marzo 2023). Inoltre, il CSIRT Italia, unitamente alle omologhe strutture di Spagna, Albania e Romania, ha approfondito, nel corso di un *workshop* su "Risposta a incidenti informatici significativi: una prospettiva di settore", la collaborazione PPP nella gestione di incidenti *ransomware*.

Nell'ambito della Presidenza indiana del **G20**, nel corso della riunione ministeriale del 19 agosto 2023, sono stati discussi tre settori chiave dell'economia digitale – infrastrutture pubbliche digitali per l'inclusione e l'innovazione digitali, la costruzione di un'economia digitale sicura e resiliente, lo sviluppo di competenze digitali per creare una forza lavoro pronta per il futuro a livello globale – nel cui contesto, l'ACN ha fornito il proprio contributo con riguardo a svariate tematiche, tra cui il rafforzamento della cooperazione in materia di cybersicurezza, la promozione del *capacity building* della cittadinanza per rispondere agli incidenti informatici nell'economia digitale e lo sviluppo di un ambiente di sicurezza e consapevolezza informatica, soprattutto per i più piccoli e per le giovani generazioni.

Per quel che concerne il **G7**, nel 2023 la Presidenza giapponese ha riattivato il c.d. *Ise-Shima Cyber Group*, che era stato avviato in occasione del Summit di Ise-Shima del 2016 e le cui attività erano poi cessate al termine del relativo turno di presidenza. In tale ambito sono state discusse, a livello Ambasciatori, 2 delle 11 norme sul comportamento responsabile degli Stati nello spazio cibernetico, adottate dall'Assemblea Generale dell'ONU nel 2015, con l'obiettivo di addivenire a un'interpretazione condivisa tra i *partner* G7. Le norme in questione sono:

- quella che proibisce agli Stati di porre in essere o sostenere attività *cyber* malevole volte a danneggiare intenzionalmente le infrastrutture critiche di un altro Paese o tali da comprometterne l'operatività e la conseguente erogazione di servizi pubblici;

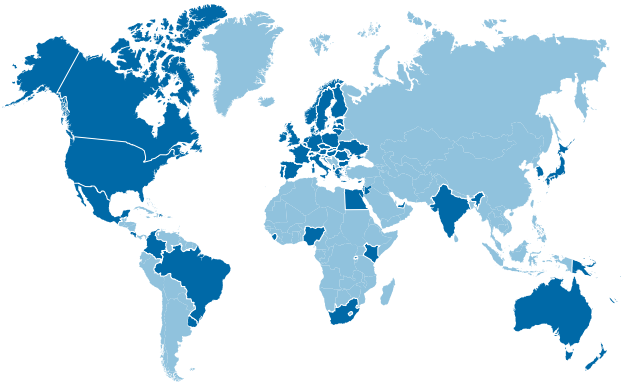
[15] «Gli Stati partecipanti, su base volontaria e conformemente alla legislazione nazionale, promuoveranno partenariati pubblico-privati e svilupperanno meccanismi per lo scambio di migliori prassi per quanto concerne le risposte alle sfide comuni alla sicurezza derivanti dall'uso delle TIC». L'Italia, insieme ad Austria, Belgio, Estonia, Finlandia e Svezia, si è impegnata nello sviluppo di tale CBM, nell'ambito di un apposito gruppo di lavoro.

- quella che richiede agli Stati di rispondere alle richieste di assistenza da parte di Stati le cui infrastrutture critiche siano oggetto di tali attività, nonché alle richieste di mitigazione delle stesse, laddove l'attività promani dal proprio territorio.

In particolare, l'Agenzia ha fornito un supporto tecnico alla Farnesina, in merito alle circostanze al verificarsi delle quali tali norme troverebbero applicazione a fronte di operazioni *cyber* ritenute inammissibili.

Nell'ambito di una collaborazione continuativa con il gruppo di lavoro G7 per la sicurezza e l'integrità della ricerca (*G7 Working Group on the Security and Integrity of the Global Research Ecosystem*), l'Agenzia ha intensificato anche la collaborazione con il MUR, partecipando, tra l'altro, alla "Giornata Nazionale della Cybersicurezza", organizzata dal Dicastero.

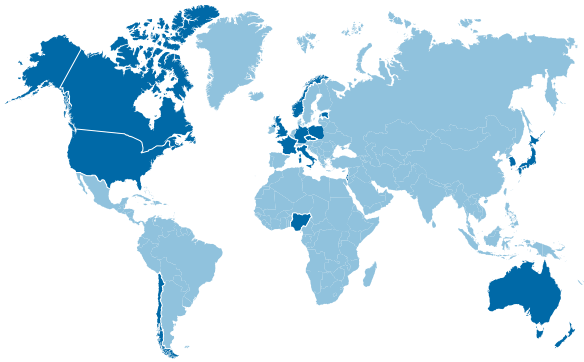
Inoltre, in preparazione della Presidenza italiana del G7 nel 2024, l'Agenzia, come anticipato, ha proposto l'istituzione di un gruppo di lavoro con le autorità nazionali per la cybersicurezza dei Paesi del G7 (oltre all'Italia, Canada, Francia, Germania, Giappone, Regno Unito e Stati Uniti).



Sempre sul piano multilaterale, sono proseguiti i lavori nell'ambito della ***Counter Ransomware Initiative*** **(CRI)**, avviata su impulso del *National Security Council* statunitense nell'ottobre del 2021 quale foro per promuovere la cooperazione e lo scambio di esperienze tra gli Stati partecipanti[16] sul tema del contrasto agli attacchi *ransomware*. In tale ambito, l'ACN ha assicurato la propria partecipazione agli incontri strategici che si sono focalizzati sul contrasto del modello imprenditoriale dei *ransomwa-*

[16] Attualmente il consesso è formato da 50 membri, tra Paesi e organizzazioni: Unione europea, Interpol, Albania, Australia, Austria, Belgio, Brasile, Bulgaria, Canada, Colombia, Costa Rica, Croazia, Egitto, Emirati Arabi Uniti, Estonia, Francia, Germania, Giappone, Giordania, Grecia, India, Irlanda, Israele, Italia, Kenya, Lituania, Messico, Nigeria, Norvegia, Nuova Zelanda, Paesi Bassi, Papua Nuova Guinea, Polonia, Portogallo, Regno Unito, Repubblica Ceca, Repubblica di Corea, Repubblica Dominicana, Romania, Ruanda, Sierra Leone, Singapore, Slovacchia, Spagna, Stati Uniti, Sud Africa, Svezia, Svizzera, Ucraina e Uruguay.

re e sulla costruzione di una base comune di evidenze, continuando a svolgere un ruolo di coordinamento nazionale tra le altre amministrazioni con competenza in materia, segnatamente il MAECI per la componente *cyber diplomacy*, il Ministero dell'interno per gli aspetti di criminalità informatica e il MEF per quel che concerne il contrasto al finanziamento illecito. L'Agenzia ha partecipato inoltre al terzo Summit CRI, svoltosi a Washington dal 31 ottobre al 1° novembre 2023, nel corso del quale è stata approvata la dichiarazione congiunta che impegna le amministrazioni dei Paesi aderenti a non pagare riscatti ai cybercriminali. I membri si sono, inoltre, assunti l'onere di fornire assistenza reciproca nella risposta a un incidente in caso di attacco *ransomware* che colpisca i governi o settori vitali dei Paesi coinvolti. Sempre in tale sede, l'ACN ha potuto presentare la propria proposta, denominata *Cybersecurity Authorities Network* (CyAN), volta ad ampliare il meccanismo di CyCLONe, istituendo la rete delle autorità di cybersicurezza, attraverso una piattaforma su base volontaria tra Paesi *like-minded* per la trattazione di molteplici tematiche relative al *ransomware,* ma anche ad altre minacce di cybersicurezza.



Come anticipato precedentemente, l'Agenzia ha aderito alle **"Linee guida per uno sviluppo sicuro dell'Intelligenza Artificiale"**, promosse dal *National Cyber Security Centre* del Regno Unito in collaborazione con la CISA degli Stati Uniti sottoscritte da 23 Agenzie di 18 Paesi (Australia, Canada, Cile, Corea del Sud, Estonia, Francia, Germania, Giappone, Israele, Italia, Nigeria, Norvegia, Nuova Zelanda, Polonia, Regno Unito, Repubblica Ceca, Singapore e Stati Uniti). L'iniziativa emana dalla prima conferenza internazionale sull'Intelligenza Artificiale, il cosiddetto "*AI Safety Summit*" del 1 e 2 novembre che si è tenuto nel Regno Unito, a Bletchley Park. Durante tale incontro esperti governativi e del settore privato hanno elaborato una linea di indirizzo comune per supportare gli sviluppatori di qualsiasi sistema basato sull'IA, al fine di innalzare i livelli di cybersicurezza dell'Intelligenza Artificiale per assicurare che sia progettata, sviluppata e impiegata in maniera sicura. La sicurezza è, infatti, una precondizione essenziale allo sviluppo dell'IA, per garantire resilienza, *privacy*, correttezza e affidabilità, cioè in ultima analisi un cyberspazio più sicuro per tutti.

Un ultimo filone di attività in ambito multilaterale è costituito dalla collaborazione a livello tecnico dell'Agenzia con organismi internazionali.

Per quanto riguarda il settore delle certificazioni, nel 2023 l'ACN in qualità di OCSI ha avuto una rilevante proiezione internazionale, a partire da un importante risultato ottenuto nel mese di settembre con il superamento di una valutazione tra pari, nota come *Voluntary Periodic Assessment*, condotta da referenti degli omologhi organismi di certificazione spagnolo, polacco, svedese e turco. Il positivo esito della valutazione consentirà a OCSI di mantenere il suo stato di organismo di certificazione qualificato nell'ambito dei già citati accordi di mutuo riconoscimento con organismi di certificazione europei (SOG-IS) e internazionali (CCRA), consentendo ai certificati emessi da OCSI di continuare a essere validi in Europa e nel mondo (vds. capitolo 2). Rappresentanti dell'Agenzia hanno inoltre partecipato a 6 diversi incontri – di cui uno svoltosi proprio a Roma – a livello di SOG-IS e CCRA ed esprimendo la presidenza di uno dei comitati direttivi del CCRA per tutto il 2023.

L'ACN è stata, inoltre, presente ai principali tavoli multilaterali sull'utilizzo consapevole della crittografia all'interno dei processi di certificazione internazionale. Tra questi, giova menzionare il *Crypto Group* del SOG-IS, che sta lavorando a un elenco di algoritmi crittografici raccomandati per la protezione dei dati sensibili all'interno dei prodotti da certificare, nonché il processo di revisione all'interno del *Common Criteria Development Board* per l'introduzione di funzioni di sicurezza dedicate alla crittografia all'interno delle certificazioni *Common Criteria*, con la prossima pubblicazione di un documento dedicato ("*Specification of Functional Requirements for Cryptography*").

In tema di risposta agli incidenti, il CSIRT Italia, già accreditato nella rete globale di *Trusted Introducer*, è entrato a far parte, da ottobre 2023, del FIRST (*Forum of Incident Response and Security Teams*), la più importante comunità mondiale di *incident responders*. Tale processo ha richiesto la revisione interna delle procedure di gestione di eventi, strumenti, dati e personale, nonché la sponsorizzazione da parte di due *team* già affiliati al FIRST, ovvero il CERT di Banca d'Italia e la CISA, l'autorità *cyber* statunitense con la quale l'ACN ha costanti interlocuzioni in virtù di una relazione sempre più stretta. Infine, è stato superato con successo un *audit* approfondito, condotto *in loco* dal personale del CERT di Banca d'Italia, con lo scopo di verificare la conformità delle politiche e dei processi operativi in uso al CSIRT Italia ai requisiti richiesti per l'ingresso al FIRST.

Si tratta di un risultato importante che consentirà al CSIRT Italia di beneficiare delle evidenze condivise tra i membri che, dalla sua fondazione nel 1990, compongono la *community* del FIRST, fatta di squadre di risposta agli incidenti informatici sia pubbliche che private di tutto il mondo. La nuova affiliazione al FIRST, infatti, permette al nostro Paese di contribuire sempre meglio alla resilienza complessiva dell'ecosistema cibernetico

nazionale, consentendo al CSIRT Italia di aumentare lo standard generale di sicurezza, tanto in termini di risposta agli incidenti, quanto di condivisone di informazioni relative a minacce emergenti.

Infine, con l'obiettivo di sviluppare le capacità nazionali in materia di *capacity building* e di realizzare il relativo ecosistema nazionale, l'Agenzia ha seguito, tra le altre cose, i lavori del Gruppo degli *stakeholder* in ambito *Global Forum on Cyber Expertise* (GFCE).

5.

RICERCA E INNOVAZIONE, FORMAZIONE, CONSAPEVOLEZZA

Un ulteriore indispensabile snodo della strategia dell'ACN per affrontare le sfide di cybersicurezza riguarda la necessità di dotare Pubbliche Amministrazioni, imprese e cittadini di un'adeguata capacità per cogliere al meglio le opportunità dischiuse dalle evoluzioni tecnologiche. Sotto questo aspetto, sono chiamati a svolgere un ruolo di primo piano il tessuto imprenditoriale e il mondo della ricerca, indispensabili per rafforzare l'ecosistema digitale italiano e per produrre innovazione sicura. Altrettanto imprescindibile è il contributo del sistema universitario e scolastico nel suo complesso, dal quale dovranno emergere non solo i professionisti della cybersicurezza del domani, ma anche cittadini più informati dei rischi *cyber* e dunque più capaci di porvi rimedio. Si tratta di uno sforzo a tutto tondo e i cui risultati saranno apprezzabili appieno solo nel lungo periodo, ma che l'ACN considera prioritario nel percorso di rafforzamento delle difese *cyber* del Paese.

5.1 RICERCA E INNOVAZIONE

5.1.1 PROGRAMMI INDUSTRIALI, DI INVESTIMENTO E DI INNOVAZIONE

Nell'ottica di rafforzare l'ecosistema digitale del Paese, indispensabile per potenziare l'autonomia tecnologica in ambito *cyber*, l'Agenzia è impegnata per accelerare l'intera filiera dell'innovazione.

A tal fine, nel 2023 è stato avviato il *Cyber Innovation Network* (CIN), il primo programma strategico di sostegno allo sviluppo di imprenditorialità innovativa e alla valorizzazione dei risultati della ricerca. Il CIN prevede schemi di finanziamento relativi a specifici filoni tecnologici definiti dall'Agenda di Ricerca e Innovazione (esaminata più estesamente di seguito). Nel dettaglio, l'Agenzia ha avviato le progettualità relative alla prima area di intervento, focalizzata sulla nuova imprenditorialità, e identificato le attività propedeutiche allo sviluppo della seconda, dedicata al trasferimento dei risultati della ricerca (Figura 29).

Figura 29 – Aree di intervento CIN

Nell'ambito della **prima area di intervento** è stato pubblicato uno specifico Avviso per selezionare operatori qualificati (in particolare, incubatori e acceleratori di *startup*), con cui progettare e introdurre programmi operativi congiunti per sostenere la crescita di *startup* ad alto contenuto innovativo.

Per tale selezione, l'Agenzia ha definito una rigorosa metodologia di analisi tenendo in considerazione: l'esperienza maturata dall'operatore nell'ambito di programmi di incubazione e/o accelerazione per *startup*, con particolare riferimento alla loro esperienza in ambito di *cybersecurity*; la struttura e le caratteristiche del programma di incubazione/accelerazione proposto dall'operatore, con particolare riguardo alla *governance* e al livello di coerenza e impatto del programma; il numero complessivo di *startup* nell'ambito della cybersicurezza.

All'esito dell'attività di selezione, è stata riconosciuta l'idoneità per 19 programmi dei 24 considerati ammissibili (Figura 30). L'Agenzia ha dunque proposto la sottoscrizione di un accordo di collaborazione ai primi **6 operatori selezionati**, riservandosi la possibilità di ampliare il numero di soggetti a cui proporre la sottoscrizione dello stesso accordo.

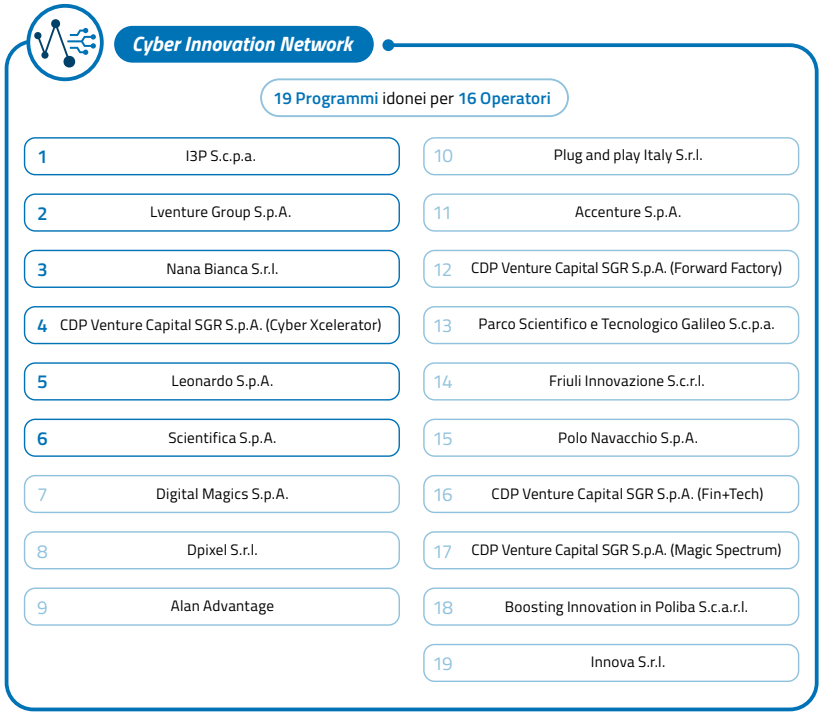


Figura 30 – Graduatoria CIN

Le candidature ricevute nell'ambito della selezione per il CIN hanno, peraltro, permesso di effettuare una prima fotografia dell'ecosistema italiano dell'innovazione della *cybersecurity*, che coinvolge in diversa misura l'intero territorio nazionale e che può contare, tra gli altri, operatori attivi nel campo del *venture capital*, dell'accelerazione e dell'incubazione di *startup*, nonché in quello della consulenza.

A valle degli accordi di collaborazione, l'Agenzia selezionerà, tra le *startup* italiane costituite da non oltre 60 mesi e che hanno partecipato o parteciperanno ai programmi degli operatori selezionati, quelle che riterrà più meritevoli di ricevere un finanziamento. Ciò permetterà di identificare *startup* che lavorino sulle tecnologie emergenti con elevato potenziale di innovazione e scalabilità nell'ambito della cybersicurezza, valorizzando in maniera prioritaria tecnologie quali scienza dei dati, Intelligenza Artificiale, robotica, *Internet of things*, *blockchain*, computazione quantistica e crittografia.

In particolare, l'Agenzia ha avviato le interlocuzioni per strutturare i programmi congiunti con gli operatori selezionati e predisposto gli atti per la selezione e il finanziamento delle *startup* con due diverse misure, in linea con la disciplina in materia di aiuti di Stato (regime *"de minimis"*):

- per il sostegno delle attività di validazione della soluzione innovativa proposta, dell'interesse di mercato verso la soluzione e della sostenibilità del modello di *business*, fino a un massimo di 50.000 euro per *startup*;
- per supportare lo sviluppo e lo *scale-up* di mercato del progetto imprenditoriale e della soluzione già validata, fino a un massimo di 150.000 euro per *startup*.

La **seconda area di intervento** è dedicata alla valorizzazione dei risultati della ricerca pubblica in collaborazione con i *Technology Transfer Offices* (TTO) di università ed enti pubblici di ricerca, il cui compito è aggregare i risultati della ricerca pubblica per favorirne la valorizzazione commerciale. Al riguardo, l'ACN ha lavorato per definire la metodologia volta a mappare il panorama italiano dei TTO. Ciò permetterà di ampliare il *Cyber Innovation Network*, consentire l'accesso a risultati della ricerca già strutturati e sostenerne la validazione, rispetto alle esigenze del mercato.

5.1.2 PROGRAMMI DI SOSTEGNO ALLA RICERCA

Nel 2022 l'ACN aveva delineato una tabella di marcia per il perseguimento degli obiettivi strategici in materia di ricerca e innovazione tecnologica articolata in tre fasi che, a partire dalla definizione di una base di conoscenza condivisa per orientare la ricerca e l'innovazione, consentisse la creazione di una rete di soggetti di ricerca, pubblici e privati, cui destinare investimenti in ricerca applicata in ambiti per i quali risulti necessario o strategico un potenziamento delle capacità nazionali.

A completamento della prima fase, a giugno 2023 l'Agenzia e il MUR hanno pubblicato l'***Agenda di Ricerca e Innovazione per la Cybersicurezza 2023-2026***, risultato di un'intensa attività congiunta. L'Agenda, mirando a promuovere la ricerca sulla cybersicurezza e a valorizzarne i risultati, è rivolta a tutti gli attori che operano direttamente o beneficiano della ricerca sulla cybersicurezza in Italia, incluse università, amministrazioni pubbliche, imprese e consorzi pubblici e privati.

Il documento contiene una lista di 60 argomenti prioritari per l'ecosistema pubblico-privato nazionale della ricerca, con un orizzonte temporale che guarda al 2026. Gli argomenti sono raggruppati in 18 subaree che afferiscono alle seguenti 6 aree della conoscenza condivise sulla sicurezza cibernetica:

1. *sicurezza dei dati e privacy*, focalizzata sulle *privacy-enhancing technology* e le sfide più attuali nell'ambito della crittografia e della condivisione sicura delle informazioni;
2. *gestione delle minacce cibernetiche*, che include la ricerca di tecniche di attacco e difesa, la *cyber threat intelligence*, la gestione degli incidenti e operazioni di sicurezza, nonché le scienze forensi digitali;
3. *sicurezza dei software e delle piattaforme*, che tratta la sicurezza nello sviluppo e test del software, la sicurezza nei sistemi operativi e tecnologie di virtualizzazione, nonché nelle *blockchain*;
4. *sicurezza delle infrastrutture digitali*, che approfondisce la sicurezza degli apparati hardware e di rete che compongono le infrastrutture digitali per assicurarne la resilienza cibernetica;
5. *aspetti della società*, che indaga i risvolti umani, formativi e legali della cybersicurezza;
6. *aspetti di governance*, che approfondisce le questioni organizzative, di gestione del rischio e di standardizzazione.

Inoltre, il documento identifica 19 tecnologie emergenti, tra cui l'Intelligenza Artificiale, il calcolo quantistico e i sistemi di controllo industriale, ritenute rilevanti per lo studio dei vari argomenti delle citate aree.

Considerato il ritmo serrato di avanzamento di ricerca e innovazione, nonché delle politiche nel campo della cybersicurezza, saranno rilasciati aggiornamenti periodici per spiegare come gli argomenti di ricerca individuati si possano adattare all'evolversi dello scenario.

L'ACN ha, inoltre, posto le basi per le fasi successive partecipando a eventi e conferenze di settore, attivando nuove collaborazioni su progettualità specifiche e dando avvio alla progettazione di programmi di promozione e valorizzazione della ricerca sulla sicurezza cibernetica.

Infine, nell'ottica di creare una rete di collaborazioni stabili nell'ecosistema nazionale della ricerca, nel corso del 2023 sono state intensificate le interlocuzioni con il Consorzio interuniversitario nazionale per l'informatica (CINI). Tra le varie aree di cooperazione, considerata l'importanza degli aspetti di cybersicurezza dell'Intelligenza Artificiale, l'Agenzia ha aderito, assieme al Garante per la protezione dei dati personali, all'azione progettuale promossa dal *Laboratory of Artificial Intelligence and Intelligent Systems* del CINI, per l'armonizzazione nazionale delle metodologie di valutazione e dei processi di gestione del rischio dell'IA, nel cui ambito l'ACN è impegnata, approfondendo gli aspetti relativi al rischio *cyber*.

5.1.3 IL COMITATO TECNICO-SCIENTIFICO

Al fine di promuovere la collaborazione con il sistema dell'università e della ricerca oltre che con il sistema produttivo nazionale, è istituito presso l'Agenzia, e presieduto dal suo Direttore generale, il Comitato tecnico-scientifico (CTS) che svolge funzioni di consulenza e proposta.

Nel corso del 2023, i temi trattati dal CTS sono stati:

- l'Agenda di Ricerca e Innovazione per la Cybersicurezza, presentata al CTS, prima della sua pubblicazione, per raccogliere orientamenti e revisioni. Il CTS si è espresso positivamente sul documento finale e ha sottolineato l'importanza di approfondire le tematiche dell'Intelligenza Artificiale, della sperimentazione pratica del *quantum computing*, della *cyberbiosecurity* e dei sistemi di controllo industriale, avendo cura di coinvolgere le Fondazioni SERICS, FAIR e NQSTI nell'ambito di partenariati estesi relativi, rispettivamente, alla cybersicurezza, all'IA e al *quantum computing*;
- il Programma di *awareness* della cybersicurezza, predisposto dall'Agenzia per promuovere la consapevolezza e diffondere comportamenti responsabili tra gli utenti. Il CTS ne ha condiviso l'impostazione e le finalità generali, fornendo alcuni utili spunti di integrazione (vds. oltre, nella sezione dedicata alla consapevolezza, per ulteriori dettagli);

- il Piano di comunicazione orientato a far conoscere e comprendere il ruolo dell'ACN all'interno del mondo istituzionale, anche estero, della comunità professionale e della società italiana. Ciò è volto a promuovere il consolidamento di una identità riconoscibile e coerente dell'Agenzia, anche per accrescerne la reputazione, per farne conoscere le attività progettuali, le opportunità per imprese e centri di ricerca, nonché, in raccordo con il citato Programma di *awareness*, per favorire la diffusione della cultura *cyber* nella società;
- le implicazioni dell'Intelligenza Artificiale sul fronte della *cybersecurity*, con particolare riferimento alle necessità di sviluppo delle capacità di ricerca e industriali in materia. Il CTS ha fornito importanti indicazioni rispetto alle possibili attività che l'ACN può intraprendere nel campo dell'IA a supporto della cybersicurezza, di *cybersecurity* dell'IA e di contrasto alla minaccia cibernetica basata su IA.

5.2 FORMAZIONE, SVILUPPO DELLA FORZA LAVORO E CAPACITÀ NAZIONALI

Un ecosistema digitale solido non può prescindere da un capitale umano adeguatamente formato, nonché da una conoscenza in materia *cyber* quanto più diffusa possibile. Pertanto, l'Agenzia ha proseguito, anche nel 2023, le iniziative di sviluppo di percorsi formativi nel settore della cybersicurezza. Ciò al fine, da un lato, di incrementare la disponibilità della forza lavoro da impiegare in futuro e, dall'altro, di migliorare la risposta degli operatori già attivi per aggiornarne la preparazione rispetto alle crescenti minacce alla sicurezza informatica. Infatti, solo con un appropriato percorso formativo si possono creare le professionalità più adatte per il campo sempre più ampio e in costante evoluzione delle professioni ICT, nonché radicare la cultura della sicurezza informatica. Si registra, nel Paese, una significativa carenza di esperti in cybersicurezza a ogni livello, così come risulta limitato il possesso di competenze anche fra coloro che hanno responsabilità decisionali.

Con riferimento agli interventi di formazione, l'Agenzia sta curando la programmazione di varie iniziative, con l'obiettivo di rendere ordinato e congruente il percorso di crescita di nuova forza lavoro, di pari passo con lo sviluppo delle competenze appropriate. Ciò deve partire dalla formazione a tutti i livelli (scolastico, universitario, di formazione professionale) e includere percorsi differenziati per focus e per livello di approfondimento tecnico, a seconda dei destinatari, tra i quali non possono essere tralasciate le figure con responsabilità non strettamente specialistiche. Nell'ambito della formazione dei professionisti nei settori tecnologici, è emersa la necessità di combinare diversi approcci, sia teorici (formale per scuole e università, informale per mondo aziendale), che pratici, questi ultimi volti a costruire un quadro di riferimento su cui innestare azioni concrete.

Nella sua collaborazione con il Ministero dell'istruzione e del merito, l'Agenzia ha posto uno specifico focus sulla scuola primaria, avviando interlocuzioni volte a far rientrare la cybersicurezza tra i contenuti delle attività formative finalizzate alla cittadinanza digitale nell'ambito dell'educazione civica.

Una particolare attenzione è stata riservata, già dagli anni passati, al sistema degli Istituti tecnologici superiori (ITS *Academy* o semplicemente ITS), scuole di eccellenza ad alta specializzazione tecnologica post-diploma, che permettono di conseguire il titolo di tecnico superiore, basate sulla connessione delle politiche d'istruzione, formazione e lavoro con le politiche industriali. Tali Istituti sono realizzati da fondazioni costituite *ad hoc*, su base regionale, da soggetti di diverse categorie (istituti scolastici, atenei, enti di formazione professionale, enti locali e aziende) per portare avanti percorsi formativi in settori tecnologicamente avanzati e facilitare l'inserimento nel mondo del lavoro di figure professionali di livello intermedio. Sebbene tali percorsi coinvolgano per ora poche centinaia di studenti, sono di grande importanza per far fronte alla carenza di specialisti nelle discipline informatiche e, in particolare, nella cybersicurezza.

Per questa ragione, l'Agenzia nel 2023 ha continuato a dedicare una specifica attenzione agli ITS ampliando la rete di collaborazione con le amministrazioni interessate (MIM, MUR, DTD) e con i diversi interlocutori (Regioni, Confindustria e altri soggetti). Al fine di sostenere i percorsi ITS in materia di cybersicurezza e *cloud computing*, l'Agenzia ha approvato la creazione di borse di studio per la frequenza degli Istituti, che saranno assegnate a partire dall'anno scolastico 2024/2025.

Sempre con l'obiettivo di stimolare l'interesse specifico da parte dei giovani e di contribuire alla diffusione di una maggiore consapevolezza del rischio e della minaccia *cyber,* l'Agenzia ha continuato a offrire il proprio contributo a varie iniziative mirate, tra cui quelle promosse dal *Cybersecurity National Lab* del CINI. Tra queste ultime, giova ricordare i programmi di formazione e competizione che rientrano sotto il nome complessivo di *Big Game: CyberChallenge, OliCyber e CyberTrials*. Quest'ultima, in particolare, è rivolta specificamente a studentesse, senza prerequisiti tecnici, e risponde all'obiettivo dell'Agenzia di ridurre il *gender gap*, sollecitando l'attenzione delle ragazze per le discipline scientifico-tecnologiche.

Nel corso del 2023, si è proseguito a consolidare le relazioni con il sistema universitario – Ministero dell'università e della ricerca, Conferenza dei rettori delle università italiane (CRUI), atenei e Agenzia nazionale di valutazione del sistema universitario e della ricerca – al fine di sostenere le attività didattiche nel settore della cybersicurezza e contribuendo attivamente alla loro definizione, anche tramite la sottoscrizione di specifici accordi (vds. oltre). In particolare, è stato deciso di istituire delle borse di studio volte a incoraggiare la frequenza di corsi universitari

nell'ambito della cybersicurezza, che saranno assegnate a partire dall'anno accademico 2024/2025.

L'Agenzia ha, inoltre, effettuato una ricognizione dell'offerta formativa, con particolare riguardo alle lauree magistrali, in modo da definire – insieme agli altri soggetti competenti per l'approvazione e l'accreditamento – una modalità di riconoscimento dei corsi di studio in cybersicurezza, o in altre discipline con contenuti significativi di cybersicurezza (in particolare informatica e ingegneria informatica).

A livello post-laurea, l'ACN ha continuato a fornire il proprio sostegno al primo dottorato nazionale in cybersicurezza, partito a febbraio 2023 presso la Scuola IMT Alti Studi di Lucca, con la quale è stata sottoscritta un'apposita convenzione. Sempre in tale direzione si colloca il programma a sostegno della promozione e del rafforzamento dei corsi di dottorato, accreditati dal MUR, che saranno avviati a partire dall'anno accademico 2024/2025. Tale programma si rivolge alle università italiane – statali e non, ivi compresi gli istituti di istruzione universitaria a ordinamento speciale – che verranno invitate a manifestare il proprio interesse a collaborare con l'Agenzia per la promozione di percorsi di dottorato in ambito *cyber*. Verranno così individuati 30 progetti di ricerca proposti dalle università, alle quali offrire la sottoscrizione di un accordo di collaborazione che consentirà, tra l'altro, di mettere a disposizione una borsa di dottorato per ciascun progetto selezionato. Ciò va sia nel senso di una più approfondita formazione, sia di creare una rete di soggetti di ricerca, pubblici e privati, con cui l'Agenzia possa cooperare per lo sviluppo di competenze nell'ambito della cybersicurezza e, in particolare, su temi inerenti alle aree, alle sub-aree e agli argomenti prioritari della citata Agenda di Ricerca e Innovazione.

Per quanto riguarda l'affinamento delle competenze in ambito *cyber* delle professionalità impiegate nel settore pubblico, l'Agenzia ha stretto un accordo con la Scuola nazionale dell'amministrazione (SNA) che consentirà di collaborare concretamente a sostegno della formazione del personale. In particolare, in continuità con le iniziative formative già avviate nel precedente anno, nel 2023 sono state realizzate delle sessioni formative *ad hoc* destinate ai dipendenti della Pubblica Amministrazione. Sempre in tale contesto di collaborazione, è stata programmata la promozione e lo sviluppo di una *Comunità di Pratica* specificatamente dedicata ai temi della cybersicurezza, importante strumento per la condivisione e lo scambio di esperienze tra pari, apprendimento collaborativo e disseminazione di conoscenza, aperto a contributi della società civile e finalizzato alla realizzazione di buone pratiche e all'illustrazione di esperienze rilevanti.

La promozione della formazione e l'attività di divulgazione nel settore della cybersicurezza è stata, inoltre, portata avanti attraverso la partecipazione di rappresentanti dell'Agenzia a numerosi eventi, convegni e seminari presso istituzioni

nazionali e internazionali. Tra questi, si segnalano in particolare i gruppi di lavoro in ambito ENISA ed ECCC (vds. capitolo 4), nonché quello della *Coalizione Nazionale per le competenze digitali*, afferente all'iniziativa nota come *Repubblica Digitale*, promossa dal DTD**.**

5.3 CONSAPEVOLEZZA E CULTURA DELLA CYBERSICUREZZA

Alla necessaria attività di sostegno per la formazione degli specialisti con competenze anche di tipo non tecnico sulle questioni *cyber*, si affianca un ulteriore, importante filone relativo alla promozione della consapevolezza in materia di cybersicurezza (c.d. *cybersecurity awareness*). A tale riguardo, l'Agenzia ha predisposto il menzionato **Programma di *awareness* della cybersicurezza** quale strumento di *governance* per la pianificazione nel medio e lungo periodo delle iniziative e delle campagne di sensibilizzazione che l'Agenzia ha già iniziato a promuovere verso i cittadini, le imprese e i soggetti pubblici, anche in sinergia con altri attori a livello nazionale ed europeo.

Il Programma, soggetto ad aggiornamenti periodici, comprende una lista di macroprogetti strategici, attuati tramite iniziative articolate per piani operativi annuali, ed è corredato di un quadro di riferimento (che sarà pubblicato nel corso del 2024) per la sistematizzazione dei temi e contenuti prioritari per l'Agenzia, dei *target* da raggiungere e dei relativi strumenti e canali di realizzazione.

Nell'ambito delle iniziative previste dal Programma si segnalano:

- il mese europeo della cybersicurezza (ottobre): principale progetto di consapevolezza sulla cybersicurezza a livello europeo che prevede la cooperazione degli Stati membri, della Commissione e di ENISA per la realizzazione coordinata di campagne annuali e di specifici eventi. L'ACN, dal 2023, rappresenta l'Italia al gruppo di coordinamento del progetto e, in occasione della campagna di ottobre 2023, ha pubblicato, in raccordo con ENISA, un mini-sito con pillole video e infografiche in lingua italiana per introdurre gli scenari tipici del *social engineering* e aiutare a riconoscerne i segnali di allarme;

- nella cornice dell'accordo siglato nel dicembre 2022 tra l'Agenzia e la Banca d'Italia, che prevede la definizione di campagne di sensibilizzazione sulle tematiche di *cybersecurity*, sono state avviate alcune iniziative congiunte. In particolare, sono stati organizzati un seminario frequentato da rappresentanti di entrambe le istituzioni, seguito da un corso rivolto al personale dirigenziale della Banca d'Italia. L'Agenzia ha collaborato con il CERT istituzionale della Banca per la predisposizione di documentazione utile sulle buone pratiche per minimizzare o arginare gli impatti degli attacchi cibernetici, anche in relazione ai nuovi profili di rischio relativi alle piattaforme di condivisione e comunicazione digitali e all'Intelligenza Artificiale;
- in seguito alle riflessioni già avviate nel corso del precedente anno, nel 2023 l'ACN ha avviato la progettazione di una campagna interistituzionale, in collaborazione con il Dipartimento per l'informazione e l'editoria della Presidenza del Consiglio dei ministri, per la sensibilizzazione in favore delle piccole e medie imprese, che si svolgerà nel corso del 2024. Le PMI rappresentano, infatti, un *target* particolarmente rilevante per l'Agenzia[17] alla luce del numero di eventi *cyber* di cui sono oggetto (vds. capitolo 1) e del livello di maturità *cyber* mediamente non particolarmente elevato di tali aziende. L'Agenzia, anche in vista dei recenti sviluppi normativi europei in materia di cybersicurezza[18], ha voluto dare il proprio contributo per accelerare la presa di coscienza del ruolo chiave della *cybersecurity*, fornendo uno strumento per sensibilizzare le imprese sull'importanza di adottare contromisure organizzative e tecniche per potenziare le capacità di prevenzione, monitoraggio e contrasto delle minacce. A tal fine, la campagna prevederà la realizzazione di un sito web, uno spot televisivo e alcuni strumenti di *awareness* con contenuti differenziati a vantaggio dei titolari delle PMI, dei dipendenti e dei professionisti e fornitori ICT;
- iniziative di *cybersecurity awareness* rivolte agli studenti, incluso un seminario formativo rivolto ai ragazzi delle scuole secondarie di secondo grado, organizzato dal MIM[19];
- l'avvio delle attività preliminari per la progettazione di una *e-Academy*, denominata ASCII (*A SCuola di sIcurezza cIbernetica*), che diventerà una componente del sito web istituzionale dell'Agenzia, destinata a veicolare a tutti i cittadini italiani temi e

[17] L'iniziativa, infatti, si affianca a quella che ha portato alla pubblicazione – insieme a Confindustria e Generali – del *Cyber Index PMI* (trattata nel prosieguo), rivolta anch'essa alle piccole e medie imprese.

[18] Si rimanda, a tale riguardo, alla Direttiva NIS 2 e all'ampliamento del novero dei settori coinvolti dalle prescrizioni di cybersicurezza (vds. capitolo 4).

[19] Nell'ambito dei lavori dell'edizione 2023 della fiera *"Job&Orienta"*, dedicata all'orientamento, la scuola, la formazione e il lavoro, che si è tenuta dal 22 al 25 novembre 2023.

contenuti di cybersicurezza. In particolare, è stata effettuata un'analisi di iniziative analoghe condotte a livello europeo da agenzie omologhe e sono in fase di valutazione alcune soluzioni realizzative per la piattaforma informatica a supporto del progetto.

Inoltre, nell'ambito dell'Investimento 1.5 "*Cybersecurity*" del PNRR, l'Agenzia ha promosso interventi di potenziamento e miglioramento delle capacità *cyber* della Pubblica Amministrazione (già citati nel capitolo 3). In particolare, l'Agenzia ha erogato un totale di 30 sessioni formative che hanno coinvolto circa 2.200 tra dirigenti, responsabili e funzionari delle PA coinvolte, registrando un elevato tasso di adesione e interazione. Le sessioni hanno avuto l'obiettivo di sensibilizzare il personale dipendente delle Pubbliche Amministrazioni in merito al panorama delle minacce *cyber* e alle contromisure da adottare.

In aggiunta, l'Agenzia ha attivato una progettualità mirata alla creazione di materiale formativo di consapevolezza *cyber*, fruibile in autonomia dai dipendenti delle Pubbliche Amministrazioni sulla piattaforma informatica denominata *Syllabus* del Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri. I contenuti hanno l'obiettivo di diffondere i concetti chiave afferenti alla cybersicurezza, nonché accrescere la consapevolezza sulle diverse minacce *cyber* che si possono incontrare nell'utilizzo dei sistemi informatici.

L'azione istituzionale volta al miglioramento della consapevolezza si è rafforzata nel 2023 anche attraverso la costruzione di una rete di collaborazioni che vede coinvolte le Pubbliche Amministrazioni centrali e locali, gli Organi costituzionali, le università e i centri di ricerca, le associazioni di categoria e il settore privato in tutte le sue molteplici forme, dalle grandi imprese, alle PMI fino alle *startup*. Con la sottoscrizione di 13 nuovi accordi (Figura 31), l'Agenzia ha potuto lanciare, su diversi fronti, attività di cooperazione e partenariati strategici per lo scambio di informazioni e la condivisione delle *best practice*, aggiungendo importanti tasselli nel potenziamento della sicurezza informatica del Paese. Tra questi assumono un rilievo particolare i Protocolli d'intesa con la Camera dei deputati e con il Senato della Repubblica volti a rafforzare la collaborazione tecnica tra le istituzioni.

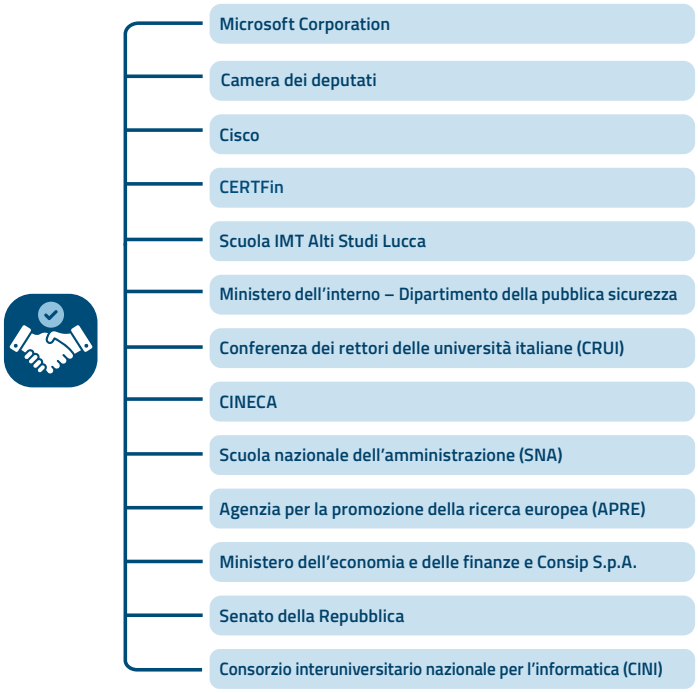


Figura 31 – Collaborazioni avviate nel 2023

Gli accordi, tra le altre cose, rafforzano la capacità dell'ACN di diffondere tra utenti e imprese la consapevolezza dei rischi *cyber*. A tale proposito, si segnala il patrocinio offerto dall'Agenzia alla campagna informativa "Cybersicuri - impresa possibile", in collaborazione con CERTFin, Banca d'Italia, ABI e numerosi altri attori del settore finanziario per sensibilizzare le imprese sull'importanza di investire in cybersicurezza e nell'informazione dei propri dipendenti. D'altro canto, in attuazione del Protocollo d'intesa sottoscritto nel 2022 con Confindustria e Generali Italia S.p.A., è stato presentato il *Cyber Index PMI*, che ha l'obiettivo di diffondere la conoscenza dei temi di cybersicurezza presso le piccole e medie imprese e di promuovere comportamenti e strumenti per il contrasto degli attacchi *cyber*. Il *Cyber Index PMI* è il primo rapporto che misura lo stato di consapevolezza e capacità di gestione in materia di rischi *cyber* delle PMI italiane.

L'Agenzia, inoltre, ha preso parte – contribuendo in taluni casi anche all'organizzazione – a più di 200 iniziative, patrocinandone 11 particolarmente rilevanti per i temi della cybersicurezza. Ampio spazio è stato dedicato alla promozione delle iniziative collegate all'attuazione della Strategia nazionale di cybersicurezza 2022-2026, tra cui la pubblicazione dell'Agenda di Ricerca e Innovazione e l'avvio del *Cyber Innovation Network*. Analogamente, l'ACN ha lavorato per promuovere le opportunità legate al PNRR tra le amministrazioni, anche locali, in stretto raccordo con il DTD, mediante un'attività di comunicazione indirizzata sia agli interlocutori istituzionali che ai destinatari degli interventi.

Nel 2023 l'Agenzia ha rafforzato la proiezione esterna partecipando, con propri rappresentanti, a oltre un centinaio di eventi e manifestazioni istituzionali, con l'obiettivo di garantire una corretta informazione sull'attività svolta nei propri ambiti di competenza. In particolare, l'ACN ha voluto rendere sistematica la partecipazione a manifestazioni rilevanti per il settore della cybersicurezza e del mondo istituzionale, a testimonianza di quanto la cybersicurezza sia condizione imprescindibile per sostenere lo sforzo di trasformazione digitale dell'Italia. Tra gli esempi più significativi, si segnala il contributo dato a maggio a ItaSec 2023 e, a ottobre, a *Cybertech Europe 2023*, importanti conferenze sulla sicurezza informatica. Da ricordare anche la partecipazione alla 40ª Assemblea nazionale dei Comuni italiani, dove l'Agenzia ha avuto modo di confermare il proprio ruolo al fianco dei Comuni per tutelarne la sicurezza informatica.

Anche a livello internazionale l'Agenzia ha partecipato a eventi e conferenze per rafforzare la propria proiezione a sostegno degli obiettivi di consolidamento della resilienza e della sicurezza *cyber*, contribuendo ad ampliare la rete di rapporti con le comunità *multi-stakeholder* in tema di *governance* globale della cybersicurezza. Ad esempio, l'Agenzia ha partecipato al *Bled Strategic Forum* (Slovenia), al *Global Cybersecurity Forum* di Riad (Arabia Saudita), al *Tallinn Digital Summit* (Estonia), alla *Prague Cyber Security Conference* (Repubblica Ceca), alla *Cyber Week* a Tel Aviv (Israele) e al *Cyber Security Directors' Meeting* in occasione della Conferenza sulla sicurezza di Monaco (Germania).

L'Agenzia ha inoltre assicurato la partecipazione a seminari e tavole rotonde organizzate da centri di ricerca, gruppi di esperti internazionali sulla cybersicurezza e università, come ad esempio l'*Annual Meeting on Cybersecurity 2023* del *World Economic Forum*, il seminario internazionale sull'IA e la cybersicurezza ospitato dall'Università di Siena, così come la *Cyber Intelligence Europe Conference and Exhibition* di Berna.


6.
ATTUAZIONE DELLA STRATEGIA
NAZIONALE DI CYBERSICUREZZA
2022-2026

In un contesto dinamico e di rapida evoluzione tecnologica, l'Agenzia ha svolto nel 2023 un ruolo centrale di indirizzo, coordinamento e monitoraggio dell'attuazione del Piano di implementazione della Strategia nazionale di cybersicurezza 2022-2026. L'azione mirata, svolta tramite il sostegno alle amministrazioni responsabili nella definizione e pianificazione di specifici interventi di attuazione delle misure della Strategia, contribuisce a uno sforzo multilivello. Sforzo che mira in particolare ad affrontare con successo le sfide relative al rafforzamento della resilienza nella transizione digitale del sistema Paese, all'anticipazione dell'evoluzione della minaccia *cyber*, alla gestione di possibili scenari di crisi cibernetiche, al conseguimento dell'autonomia strategica nella dimensione cibernetica e al contrasto della disinformazione online.

Nel corso del 2023 l'Agenzia ha seguito lo sviluppo degli interventi necessari a raggiungere gli obiettivi definiti dalla Strategia, grazie a fondi appositamente messi a disposizione, e ha monitorato puntualmente l'avanzamento dei relativi progetti.

6.1 RISORSE ASSEGNATE E MISURE PRIORITARIE

Nell'ottica di favorire l'attuazione del Piano di implementazione, è stato anche previsto un adeguato programma di leve finanziarie. Oltre ai fondi già a disposizione delle amministrazioni con competenza in materia di cybersicurezza, la legge di bilancio per il 2023 (legge n. 197/2022) ha istituito il **Fondo per l'attuazione della Strategia nazionale di cybersicurezza**, destinato a finanziare gli investimenti mirati al conseguimento dell'autonomia tecnologica in ambito digitale, nonché all'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali, e il **Fondo per la gestione della cybersicurezza**, volto ad assicurare copertura economica alle attività di gestione operativa (Figura 32). Tali risorse sono dedicate a finanziare specifiche progettualità utili al raggiungimento degli obiettivi della Strategia per il periodo 2022-2026.

Figura 32 – Fondi istituiti con legge di bilancio 2023

A tal fine, è stata condotta una rilevazione degli interventi e di eventuali fabbisogni finanziari delle amministrazioni individuate come responsabili nel Piano di implementazione della Strategia, e degli altri soggetti interessati, beneficiari delle specifiche misure.

Tale rilevazione ha riguardato le 30 misure, classificate come prioritarie, da avviare nel 2023 (misure *"quick win"*), sulla base di quanto riportato nel Manuale operativo (il documento che consente di verificare il grado di attuazione delle misure contenute nel Piano di implementazione), al fine di consentire alle citate amministrazioni una graduale attuazione della Strategia stessa. L'Agenzia ha coinvolto nella rilevazione 12 amministrazioni con le quali ha svolto diversi incontri per la definizione e la pianificazione di 166 interventi afferenti alle citate 30 misure e che contribuiscono al raggiungimento dei diversi obiettivi della Strategia. La rilevazione sarà estesa a tutte le misure della Strategia a partire dal 2024, comprensiva di eventuali aggiornamenti per le misure avviate nel 2023.

La rilevazione degli interventi (ripartiti come in Figura 33) ha coinvolto attivamente le amministrazioni interessate, consentendo il censimento, per ciascuna misura, degli interventi già in corso e di quelli pianificati, nonché del relativo cronoprogramma, delle eventuali dispo-

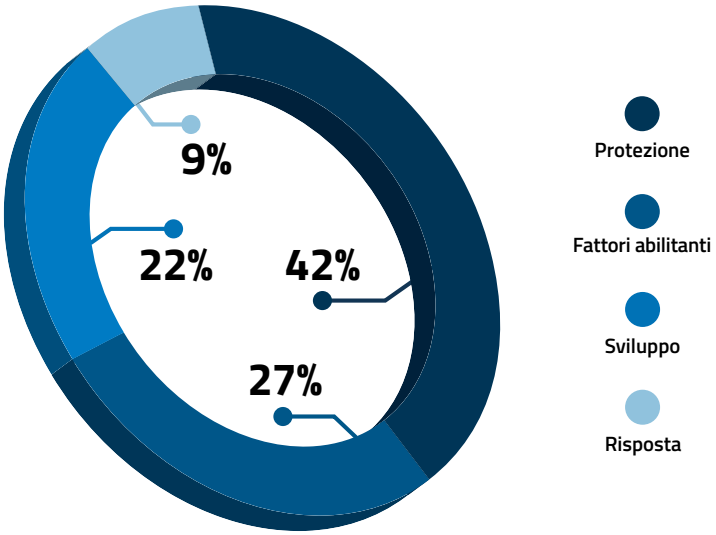


Figura 33 – Ripartizione degli interventi avviati nel 2023 sugli obiettivi della Strategia

nibilità economiche esistenti e dell'ulteriore fabbisogno finanziario necessario per la loro esecuzione.

Infatti, oltre ai succitati fondi appositamente istituiti, gli interventi possono essere finanziati anche attraverso fondi PNRR, nonché fondi propri delle Amministrazioni o con una combinazione di tali risorse.

Gli interventi proposti sono stati analizzati considerandone la rilevanza, la complessità e la coerenza rispetto alle misure di riferimento e al relativo impatto sulla cybersicurezza nazionale. Sulla base di tali analisi, su proposta dell'ACN e d'intesa con il Ministero dell'economia e delle finanze, è stato adottato il DPCM del 9 agosto 2023 per una prima assegnazione delle risorse a valere sui citati fondi nel corso del triennio 2023-2025. Sono stati così assegnati un totale di 66,7 milioni di euro a valere sui fondi per l'attuazione e per la gestione della Strategia, per sostenere 39 interventi condotti da 10 Amministrazioni (Figura 34).

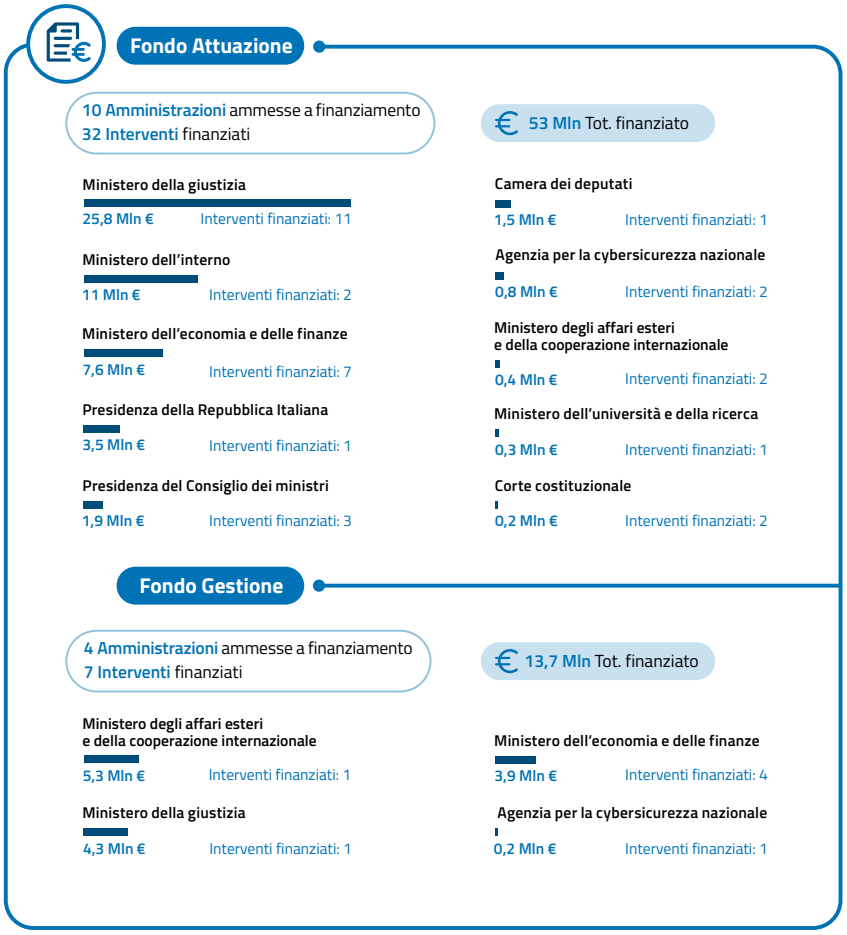


Figura 34 – Interventi a valere sul fondo "Attuazione" e sul fondo "Gestione"

6.2 COORDINAMENTO, INDIRIZZO E MONITORAGGIO DELLA STRATEGIA

Data la complessità dei compiti da realizzare nell'ambito della Strategia e considerata la partecipazione di numerosi soggetti al Piano di implementazione, l'Agenzia ha sviluppato un modello di coordinamento, indirizzo e monitoraggio specifico per consentire di

seguire lo stato di avanzamento degli interventi pianificati. Tale modello è essenziale per garantire il regolare andamento delle attività e assicurarne il buon esito, nel rispetto delle tempistiche concordate.

Infatti, così come previsto dal Piano di implementazione, nonché nel citato DPCM del 9 agosto 2023, le amministrazioni responsabili sono tenute a comunicare all'Agenzia gli esiti delle azioni condotte nell'ambito delle misure di pertinenza. Tali informazioni, che confluiscono al 31 dicembre dell'anno di riferimento in un documento riepilogativo, sono necessarie all'Agenzia per riferire sullo stato di attuazione della Strategia al Comitato interministeriale per la cybersicurezza, il quale esercita l'alta sorveglianza sull'attuazione della stessa. Inoltre, il monitoraggio ha lo scopo di prevenire e gestire potenziali criticità nel raggiungimento degli obiettivi della Strategia.

Il monitoraggio si è articolato su tre livelli principali (Figura 35).

Figura 35 – I tre livelli di monitoraggio

Al fine di rendere operativo il modello di indirizzo, coordinamento e monitoraggio sono state definite e condivise con le amministrazioni interessate le Linee Guida, con lo scopo di dettagliare e rendere note le modalità di monitoraggio delle attività svolte e di rendicontazione dei risultati raggiunti.

Tale modello è stato messo alla prova una prima volta nel secondo quadrimestre del 2023, consentendo un monitoraggio iniziale delle attività realizzate. In ragione

dell'assegnazione delle risorse avvenuta nell'ultimo quadrimestre dell'anno, la rilevazione ha potuto riguardare principalmente due livelli: il monitoraggio progettuale e quello dei risultati, per gli interventi non finanziati con i fondi per l'attuazione e per la gestione della Strategia. Tale attività ha coinvolto, oltre all'ACN, altre 7 amministrazioni, per un totale di 141 interventi sottoposti a monitoraggio e 21 misure impattate (Figura 36).

Figura 36 – Focus monitoraggio II quadrimestre 2023

La successiva fase di monitoraggio, avviata a fine 2023, ha consentito di raccogliere informazioni riguardanti l'intera annualità e ha incluso anche il monitoraggio finanziario degli interventi relativi all'attuazione delle 30 misure *quick win*.

La rilevazione degli interventi e le attività di monitoraggio hanno consentito di fornire una panoramica complessiva delle azioni necessarie per il raggiungimento dei diversi obiettivi della Strategia (Figura 37).

Con riguardo alla **protezione degli *asset* strategici nazionali**, sono stati avviati, anche completando gli interventi già avviati e finanziati con risorse dell'Investimento 1.5 "*Cybersecurity*" del PNRR:

- 19 interventi sullo **scrutinio tecnologico** riferiti: alla **Misura #1**, rivolta al potenziamento del sistema di scrutinio tecnologico nazionale per garantire la sicurezza della *supply chain* e alla promozione di schemi di certificazione europea di *cybersecurity*;

Obiettivi	Aree tematiche	Interventi avviati
Protezione	Scrutinio tecnologico	19
	Conoscenza approfondita del quadro della minaccia cibernetica	27
	Potenziamento capacità *cyber* della Pubblica Amministrazione	6
	Sviluppo di capacità di protezione per le infrastrutture nazionali	12
	Promozione dell'uso della crittografia	4
	Definizione e implementazione di un piano di contrasto alla disinformazione online	2
Risposta	Servizi *cyber* nazionali	12
	Contrasto al *cybercrime*	3
Sviluppo	Impulso all'innovazione tecnologica e alla digitalizzazione	37
Fattori abilitanti	Formazione	4
	Promozione della cultura della sicurezza cibernetica	12
	Cooperazione	27
	Metriche e *Key Performance Indicators*	1
Totale complessivo		**166**

Figura 37 – Misure *quick win.* Panoramica del numero di interventi avviati nel 2023

alla **Misura #2**, orientata a sviluppare le capacità dei CV del Ministero dell'interno e del Ministero della difesa accreditati dall'ACN. Gli interventi avviati riguardano il potenziamento delle capacità del CVCN dell'ACN, con la progettazione del laboratorio di analisi hardware e software e la predisposizione del piano di acquisti delle licenze software e della strumentazione di laboratorio, nonché con l'avvio di specifica attività formativa anche per i CV dei Ministeri dell'interno e della difesa. Sono state altresì avviate le attività per l'attivazione di un'articolazione deputata allo svolgimento delle attività di verifica tecnico-documentale e ispezione presso l'Agenzia, per la verifica del rispetto degli obblighi discendenti dalle normative *cyber* vigenti, come previsto dalla **Misura #3;**

- 27 interventi sulla **conoscenza approfondita del quadro della minaccia cibernetica**, di cui 18 riferiti alla **Misura #12** volta al rafforzamento delle capacità di *situational awareness* e 9 alla **Misura #13** per la realizzazione di un servizio di monitoraggio del rischio *cyber* nazionale finalizzato a informare i processi decisionali. Gli interventi avviati riguardano il potenziamento e il rafforzamento degli strumenti tecnici e delle capacità specialistiche e operative delle amministrazioni e di un sistema integrato di gestione del rischio *cyber* per la valutazione di vulnerabilità, minacce e rischi. In particolare, sono stati definiti i requisiti funzionali dei sistemi di monitoraggio e analisi di software malevoli e del piano di raccolta di dati da sorgenti esterne, anche ai fini del loro arricchimento e integrazione, nonché potenziate le attività di rilevazione e disseminazione di eventi di sicurezza e di *early warning*, grazie anche al progetto HyperSOC, che consente di valorizzare i vettori di rischio;
- 6 interventi sul **potenziamento di capacità *cyber* della Pubblica Amministrazione**, riferiti alla **Misura #15**, volta a qualificare i servizi *cloud* per la Pubblica Amministrazione, in linea con la Strategia *Cloud* Italia[20], per garantire elevati standard di sicurezza per i servizi e i dati della PA. Gli interventi avviati riguardano la definizione della progettualità per la nuova piattaforma di *Cloud Marketplace*, attraverso la quale le Pubbliche Amministrazioni potranno continuare a consultare e analizzare i servizi e le infrastrutture *cloud* qualificati;
- 12 interventi sullo **sviluppo di capacità di protezione per le infrastrutture nazionali**, riferiti alla **Misura #19**, volta all'implementazione del monitoraggio della vulnerabilità e delle configurazioni erronee dei servizi digitali esposti su Internet di interesse della PA, attraverso attività di *early warning*, e alla **Misura #20**, finalizzata alla promozione delle *best practice* nella gestione dei domini di posta elettronica della PA. Le attività condotte hanno riguardato il potenziamento della condivisione di bollettini, *alert* e pubblicazioni di interesse dei membri della *constituency* del CSIRT Italia, nonché la definizione dei requisiti funzionali dei sistemi di monitoraggio delle configurazioni dei domini di posta elettronica, così da prevenire eventuali campagne di *phishing* e abusi. Inoltre, la condivisione di informazioni tra l'Agenzia e la Polizia postale e delle comunicazioni consentirà di accrescere il numero dei domini di posta elettronica della PA che usufruiscono di servizi di monitoraggio e protezione contro le campagne di *phishing* e, contestualmente, di incrementare i domini disattivati, collegati a campagne di *phishing* o a operazioni di *brand abuse*;
- 4 interventi sulla **promozione dell'uso della crittografia**, riferiti alla **Misura #22**, dedicata a promuovere l'adozione della crittografia in conformità ai principi di sicurezza e di tutela della vita privata. Gli interventi avviati favoriscono l'impiego della

[20] https://www.acn.gov.it/portale/strategia-cloud-italia

crittografia commerciale lungo l'intero ciclo di vita dei sistemi e servizi ICT e riguardano la predisposizione di specifiche linee guida e raccomandazioni sull'utilizzo della crittografia come strumento di cybersicurezza. Sono state, inoltre, predisposte collaborazioni con università e altri enti di ricerca per lo studio di algoritmi di cifratura, anche nell'ambito della crittografia post-quantistica, e delineati percorsi formativi in crittografia applicata alle tematiche di cybersicurezza;

- 2 interventi sulla **definizione e implementazione di un piano di contrasto alla disinformazione online**, riferiti alla **Misura #24**, finalizzata ad attuare un coordinamento nazionale, per prevenire e contrastare – anche attraverso campagne informative – la disinformazione online. Gli interventi avviati riguardano la realizzazione di studi che mirano ad approfondire il fenomeno delle *fake news* online, anche attraverso la redazione di specifiche linee guida e la realizzazione di campagne di sensibilizzazione rivolte ai cittadini.

Ai fini della **risposta alle minacce, agli incidenti e alle crisi *cyber* nazionali**, sono stati ulteriormente sviluppati i meccanismi di coordinamento interistituzionale a livello nazionale con il Nucleo per la cybersicurezza (**Misura #25**) e a livello europeo con la rete CyCLONe (**Misura #26**) ed è proseguita la partecipazione a esercitazioni per simulare e testare le capacità tecniche e operative di gestione di tali eventi (**Misure #38 e 39**). Sempre ai fini della risposta, sono stati avviati:

- 12 interventi sui **servizi *cyber* nazionali**, che hanno consentito di definire il processo operativo di raccolta, analisi, condivisione e gestione di eventi di sicurezza e fattori di rischio da veicolare all'interno dell'HyperSOC, sulla base del patrimonio informativo dell'Agenzia, così da poter individuare precocemente eventuali modelli di attacco complessi e abilitare una gestione del rischio *cyber* in chiave preventiva (**Misura #30)**. Ciò, anche grazie all'avvio di attività istruttorie per la stipula di apposite convenzioni con gli *Internet Service Provider* (**Misura #31**), alla progressiva attivazione dei servizi da parte di un ISAC, istituito presso l'Agenzia per coordinare l'analisi di informazioni operazionali e strategiche prodotte dai vari servizi *cyber* nazionali (**Misura #34**), nonché alla predisposizione di una metodologia di gestione del rischio *cyber* nazionale a beneficio delle Pubbliche Amministrazioni, dei soggetti NIS, Perimetro e Telco (**Misura #37**);
- 3 interventi avviati sul **contrasto al *cybercrime***, riferiti alle **Misure #41 e 42**, che riguardano l'acquisizione di piattaforme software investigative e il potenziamento delle attività di addestramento nell'ambito della prevenzione e del contrasto ai crimini informatici e della diffusione di contenuti di odio, violenza e discriminazione online.

In relazione, poi, allo **sviluppo consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale**, essenziale per rispondere alle diverse esigenze e

dinamiche di mercato e consentire al Paese di acquisire un vantaggio strategico sul piano globale, sono stati avviati:

- 37 interventi sull'**impulso all'innovazione tecnologica e alla digitalizzazione**, riferiti alla **Misura #55**, volta alla promozione della digitalizzazione e dell'innovazione in ambito sicurezza, anche attraverso l'utilizzo di risorse PNRR. Tra gli interventi avviati, la diffusione dello strumento di pagamento PagoPA e delle piattaforme nazionali di identità digitale (Sistema Pubblico di Identità Digitale e Carta d'Identità Elettronica).

Al fine di consentire il raggiungimento dei citati obiettivi, è essenziale sviluppare una serie di **fattori abilitanti** quali formazione, promozione della cultura della sicurezza cibernetica e cooperazione. In tale contesto sono stati avviati:

- 4 interventi sulla **formazione**, riferiti sia alla **Misura #62**, nel cui ambito è stata avviata la progettualità per sviluppare, all'interno del sito web istituzionale dell'Agenzia, una componente dedicata alla formazione e alla sensibilizzazione online dei cittadini, denominata "A SCuola di sIcurezza cIbernetica", sia alla **Misura #68**, per la quale sono stati avviati piani formativi altamente specializzati in materia di cybersicurezza, per il contrasto dei crimini informatici, anche attraverso metodologie di prevenzione, difesa cibernetica e *digital forensic*;
- 12 interventi su **promozione della cultura della sicurezza cibernetica**, riferiti alle **Misure #71 e 73**, in relazione alle quali si è registrato un incremento di iniziative e campagne di sensibilizzazione per un corretto uso degli strumenti digitali – focalizzate, oltre che sul personale delle PA interessate, anche sulle PMI – e per la protezione online dei minori;
- 27 interventi sulla **cooperazione**, riferiti alle **Misure #78 e 79** per lo sviluppo di attività di *capacity building* a favore di Paesi terzi e la stipula di accordi bilaterali e multilaterali con i Paesi di interesse strategico, facendo altresì leva su una rete che coinvolga anche operatori privati nazionali. In relazione, poi, alla **Misura #80**, si evidenzia che l'ACN partecipa attivamente al gruppo di lavoro UE HWPCI, nel quale vengono negoziati atti normativi e documenti di *policy* in materia di cybersicurezza. Ai fini di una migliore cooperazione a livello nazionale, inoltre, si sta ulteriormente strutturando la collaborazione permanente con i soggetti Perimetro attraverso specifiche interlocuzioni settoriali (**Misura #74**);
- 1 intervento su **metriche e *key performance indicators***, riferito alla **Misura #82** attuata attraverso l'elaborazione del Manuale operativo sopra richiamato.

Per accompagnare l'efficace dispiegamento di tutti gli interventi sopra descritti, si è rivelata importante l'opera di costante aggiornamento del quadro normativo e regolatorio in materia di cybersicurezza, che potesse mantenerlo al passo con i progressivi sviluppi

tecnologici e coerente con gli indirizzi europei e internazionali in materia. In questo contesto sono state anche promosse dall'ACN e adottate disposizioni volte a dare attuazione alle **Misure #6, 7 e 8** (vds. capitolo 2).

Infine, per l'attuazione delle attività e delle misure della Strategia nazionale di cybersicurezza, la legge di bilancio 2024 ha previsto che l'Agenzia per la cybersicurezza nazionale possa avvalersi del supporto dell'Istituto Poligrafico e Zecca dello Stato S.p.A.[21]

[21] Art. 1, co. 58, della legge 30 dicembre 2023, n. 213 (legge di bilancio 2024).

7.

ORGANIZZAZIONE E FUNZIONAMENTO DELL'ACN

L'Agenzia per la cybersicurezza nazionale sta rafforzando progressivamente le proprie capacità operative così da poter assolvere al proprio mandato istituzionale, nonché ai nuovi compiti assegnati dal legislatore.

Nel 2023 sono state potenziate le risorse umane e strumentali dell'Agenzia, ingaggiando competenze qualificate al fine di assicurare a tutte le sue strutture adeguate risorse per garantire l'espletamento delle proprie mansioni e un costante aggiornamento all'evolversi della sfida tecnologica.

Rilevante è stato, inoltre, lo sforzo per dotarsi di procedure che garantiscano l'efficiente impiego delle risorse assegnate, anche grazie alla puntuale osservanza delle previsioni legislative in tema di prevenzione della corruzione, di trasparenza e di trattamento dei dati personali.

L'ACN si sta impegnando per valorizzare la propria proiezione esterna e per comunicare con una platea sempre più vasta di cittadini, imprese e istituzioni, contribuendo altresì ai dibattiti sullo stato e le prospettive della cybersicurezza al fine di accrescere la consapevolezza e la diffusione della cultura della sicurezza cibernetica.

7.1 SVILUPPO DELLE PERSONE E DELL'ORGANIZZAZIONE

Nel corso del 2023, il piano di reclutamento avviato con l'inizio dell'attività dell'ACN è proseguito per sostenere il processo di strutturazione dell'Agenzia, anche al fine di raggiungere, in sede di prima applicazione, le 300 unità di dotazione organica iniziale previste dal D.L. n. 82/2021.

In particolare, il proseguimento delle procedure di reclutamento ha consentito di disporre di personale competente e qualificato, chiamato sia a sostenere il consolidamento e l'ampliamento delle funzioni istituzionali nel campo della sicurezza e della resilienza cibernetica[22], sia a occuparsi di nuovi ambiti di attività per fronteggiare le sfide emergenti.

Al riguardo, anche nel 2023 sono state attivate alcune delle principali possibilità di reclutamento previste dal decreto-legge istitutivo: 1) concorsi pubblici a tempo indeterminato; 2) inquadramenti in via straordinaria di personale messo a disposizione da PA secondo specifiche modalità; 3) assunzioni a tempo determinato (c.d. *vacancy*), mediante procedure selettive pubbliche, aperte e comparative.

Infatti, l'alimentazione della compagine dell'Agenzia è stata perseguita, in primo luogo, con le assunzioni ordinarie a tempo indeterminato, tramite **concorso pubblico**. In relazio-

[22] Che vanno, in particolare, dalla gestione, indirizzo, coordinamento e monitoraggio dei Fondi per l'attuazione della Strategia nazionale di cybersicurezza e per la gestione della cybersicurezza (legge di bilancio 2023), alla collaborazione con l'Autorità per le garanzie nelle comunicazioni in materia di requisiti tecnici e operativi della piattaforma tecnologica per il contrasto alla pirateria online (legge n. 93/2023); dalle attività dirette all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, alla collaborazione con il Procuratore nazionale antimafia e antiterrorismo in materia di contrasto alla criminalità informatica (D.L. n. 105/2023).

ne a tale modalità, a fine novembre 2023, si è conclusa la selezione pubblica, articolata in 7 distinti concorsi, per l'assunzione di **60 diplomati con profilo tecnico *cyber***, necessari per assicurare l'operatività di strutture quali il CSIRT Italia e i laboratori di scrutinio tecnologico, indispensabili, tra l'altro, per la corretta attuazione della normativa in materia di *Golden Power* e di Perimetro di sicurezza nazionale cibernetica. A seguito della suddetta procedura concorsuale, è stato possibile pianificare l'assunzione dei vincitori già nei primi mesi del 2024, lasciando, altresì, aperta la possibilità di operare mirati scorrimenti delle graduatorie.

A fine anno l'Agenzia ha, inoltre, pubblicato i bandi per l'assunzione di **11 unità** appartenenti alle categorie protette ed equiparate, in possesso di laurea triennale nelle discipline giuridico-amministrative.

In merito alla seconda modalità di reclutamento, il 31 dicembre 2023 è stato completato il processo di selezione e inquadramento nel ruolo del personale dell'Agenzia di ulteriori **48 unità messe a disposizione**, ai sensi dell'art. 17, co. 8.1, del D.L. n. 82/2021, da Pubbliche Amministrazioni e Autorità indipendenti, al fine di assicurare la prima operatività dell'Agenzia. La procedura ha consentito l'immediato rafforzamento della capacità amministrativa attraverso il reclutamento di risorse umane specializzate e con una consolidata esperienza professionale nel settore pubblico.

Quanto al terzo canale di reclutamento (***vacancy***), in seguito alle procedure selettive per l'assunzione a tempo determinato, di soggetti in possesso di alta e particolare specializzazione per lo svolgimento di attività assolutamente necessarie all'operatività dell'Agenzia, ovvero per la realizzazione di specifiche progettualità, nel 2023 hanno preso servizio **7 unità**. In particolare, sono stati assunti: 3 *Advisor* per le attività di coordinamento interistituzionale con altri organi dello Stato e/o altre amministrazioni e di sviluppo delle relazioni internazionali; 1 *Advisor* per le funzioni di *Deployable Digital Forensic and Incident Response team manager*; 1 *Senior Advisor* per le funzioni di *security auditor*; 1 *Legal Advisor* per le attività di regolamentazione in materia *cyber*; 1 *Advisor* per le attività di accreditamento e certificazione di percorsi formativi. Le 7 unità così assunte – tra le quali alcune rientranti da un periodo lavorativo svolto all'estero – provengono da vari settori professionali, sia per natura, sia per esperienza.

In aggiunta alle citate modalità, grazie a specifiche intese con altri enti e istituzioni pubbliche, sono stati disposti, nel 2023, ulteriori distacchi, comandi, fuori ruolo o altre analoghe posizioni, per 3 unità (2 dal Ministero dell'interno e 1 dalla Guardia di Finanza).

Inoltre, è stata anche attivata la possibilità di avvalersi di un contingente massimo di **50 esperti** in possesso di specifica ed elevata competenza nel campo dell'ICT, come pre-

visto dall'art. 12 del D.L. n. 82/2021. Facendo ricorso a tale bacino, nel corso del 2023 l'Agenzia, svolgendo un ruolo catalizzatore e attrattivo di qualificate risorse professionali, ha reclutato 2 elevate professionalità, entrambe provenienti dal mondo accademico, per la realizzazione di progetti in materia di processi di trasformazione tecnologica, nonché di comunicazione e disseminazione, intesa, quest'ultima, come consapevolezza del valore della sicurezza cibernetica, in un quadro di generale resilienza del Paese.

A fine 2023, la compagine dell'Agenzia, composta complessivamente da **213 unità**, riporta una situazione di estrema specializzazione (Figura 38), con una nettissima preva-

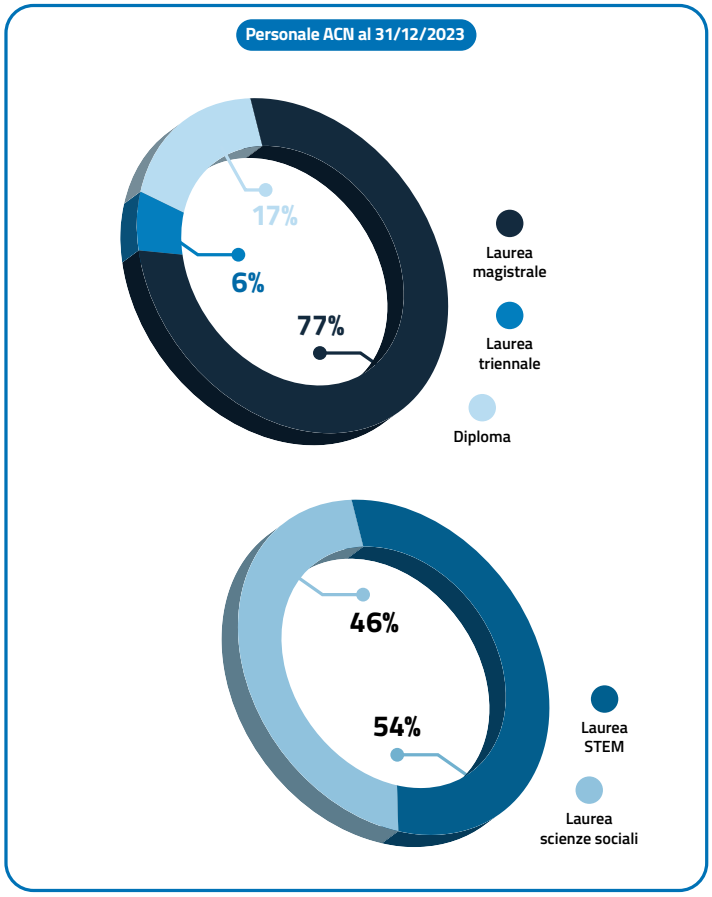


Figura 38 – Titoli di studio del personale ACN

lenza di dipendenti in possesso di laurea, anche magistrale, indispensabile per seguire ai massimi livelli i *dossier* all'attenzione dell'Agenzia. A questo si associa la presenza tanto di professionisti con competenze tecnico-scientifiche (molti sono laureati in ingegneria informatica e altre discipline STEM), quanto di quelli con un profilo attinente alle scienze sociali.

A supporto delle attività necessarie per gestire l'acquisizione delle ulteriori risorse umane, sono state realizzate delle piattaforme informatiche *ad hoc.* In particolare, una piattaforma specifica consente l'acquisizione delle candidature per le posizioni con contratto a tempo determinato e per il contingente di esperti, permettendo una gestione più fluida e organizzata del processo di reclutamento, nonché favorendo l'identificazione e l'ingaggio di professionisti con specifica ed elevata competenza oltre che significativa esperienza nel settore.

È stata, inoltre, realizzata una piattaforma per l'***Onboarding*** che centralizza e semplifica la gestione delle informazioni dei dipendenti e gestisce in modo efficace tutti gli obblighi contrattuali del lavoratore. La piattaforma *Onboarding* è stata anche integrata con il sistema di *Asset management* dell'ACN. Ciò ha consentito al lavoratore, al momento dell'assunzione, il conferimento automatico dei profili di accesso ai sistemi, agevolando, da un lato, l'abilitazione dei nuovi dipendenti ai flussi di lavoro dell'Agenzia e migliorando, dall'altro, l'efficienza operativa nell'assegnazione ai dipendenti degli *asset* informatici utilizzati come strumento di lavoro.

Più in generale, all'interno della strategia di sviluppo dell'organizzazione, è stato realizzato il Sistema di Gestione integrato (ISO 27001/9001) per la corretta gestione dei sistemi informatici e delle informazioni, utile ai fini di garantire l'esecuzione dei processi e delle operazioni in modo sicuro e conforme alle *best practice* nazionali e internazionali.

Sul fronte della formazione, alla luce delle positive sinergie sviluppate con la Banca d'Italia, sono state avviate le attività volte a rinnovare l'accordo del 4 marzo 2022 che la lega all'Agenzia per proseguire le iniziative di sviluppo del capitale umano delle rispettive compagini di personale, nonché lo scambio di esperienze professionali. Nel medesimo ambito è stato stipulato un accordo con la Scuola nazionale dell'amministrazione.

Nel corso del 2023, la progressiva acquisizione di un adeguato numero di risorse volto a un efficace esercizio delle competenze dell'ACN ha consentito di attivare e rendere operativo, dapprima, il **Servizio Autorità e sanzioni** per lo svolgimento della funzione di regolamentazione attribuita all'Agenzia, e, in un secondo momento, il **Servizio Strategie e cooperazione** per assicurare la realizzazione della Strategia nazionale di cybersicurezza,

nonché la definizione di una *policy* unitaria e coerente nella materia della cybersicurezza in ambito nazionale e internazionale.

Infine, le attività dell'Agenzia hanno potuto beneficiare – in termini di tracciamento delle informazioni, ottimizzazione dei processi interni, sicurezza e protezione dei documenti – dello sviluppo e del perfezionamento di un complesso sistema per la gestione documentale e protocollo informatico, che ha permesso di gestire oltre 100.000 documenti. Ciò si è rivelato particolarmente importante in occasione degli *audit* che hanno interessato le articolazioni tecniche dell'Agenzia (*Voluntary Periodic Assessment* per OCSI e l'*audit* per l'accreditamento al FIRST per CSIRT Italia).

7.2 PIANIFICAZIONE STRATEGICA, PROGRAMMAZIONE E *PROCUREMENT POLICIES*

L'Agenzia è dotata di autonomia contabile e finanziaria e annovera tra le proprie entrate, oltre al finanziamento ordinario, quelle ulteriori elencate nel decreto-legge istitutivo[23]. Il sistema contabile dell'Agenzia si ispira ai principi civilistici ed è basato su quello della competenza economica che, attraverso la rilevazione dei costi e dei ricavi, consente di orientare la gestione a criteri di efficacia ed efficienza.

In questa ottica, il bilancio d'esercizio 2022 (consuntivo), adottato il 28 aprile 2023 con delibera del Direttore generale, e approvato con DPCM del 6 luglio 2023, previo parere del Comitato interministeriale per la cybersicurezza, ha registrato un utile d'esercizio di 21.706.431 euro, destinato alla costituzione di una riserva di patrimonio netto per la copertura di future spese di investimento funzionali al potenziamento dell'efficacia dell'Agenzia.

Per quanto attiene agli adempimenti di natura previsionale, nel corso del 2023 sono stati predisposti i provvedimenti di assestamento del bilancio 2023 (revisione del *budget* economico), adottato il 1° agosto 2023, e di adozione del bilancio preventivo 2024 (*budget* economico), approvato il 31 ottobre 2023.

In relazione alle dimensioni economiche e finanziarie che connotano i bilanci dell'Agenzia, l'art. 18, co. 1, del D.L. n. 82/2021 e le autorizzazioni di spesa intervenute successiva-

[23] In particolare: i corrispettivi per i servizi prestati a soggetti pubblici o privati; i proventi derivanti dallo sfruttamento della proprietà industriale, dei prodotti dell'ingegno e delle invenzioni dell'Agenzia; altri proventi patrimoniali e di gestione; contributi dell'Unione europea o di organismi internazionali, anche a seguito della partecipazione a specifici bandi, progetti e programmi di collaborazione; i proventi delle sanzioni irrogate dall'Agenzia ai sensi di quanto previsto dal decreto legislativo NIS, dal decreto-legge Perimetro e dal decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative; ogni altra eventuale entrata.

mente, hanno delineato una progressiva crescita delle risorse finanziarie, in parallelo con la crescita strutturale dell'ACN e dei compiti ad essa affidati. Lo stanziamento annuale per l'Agenzia, previsto a legislazione vigente, è riportato in Figura 39.

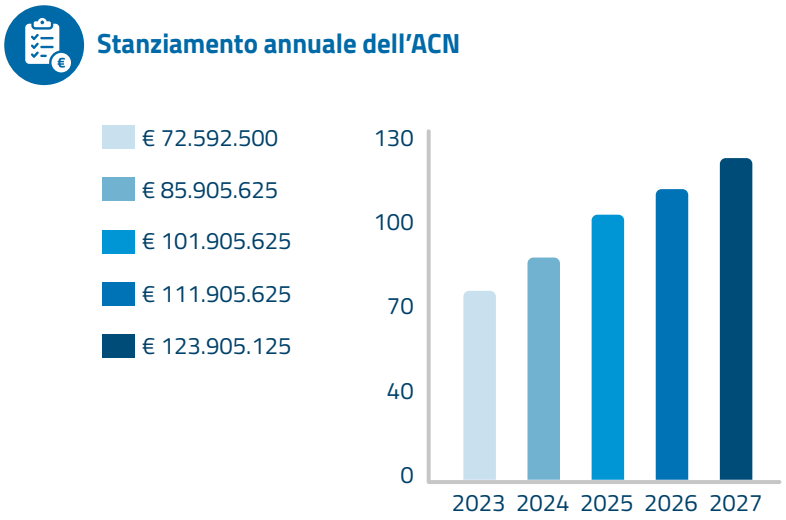


Figura 39 – Risorse finanziarie assegnate all'Agenzia

Inoltre, fino all'anno 2026 l'Agenzia potrà far ricorso ai finanziamenti del PNRR in qualità di Soggetto attuatore dell'Investimento 1.5 "*Cybersecurity*", del valore complessivo di 623 milioni di euro, come approfondito nel capitolo 3.

Infine, per soddisfare le esigenze di tutela cibernetica delle amministrazioni pubbliche (come previsto dal Piano di implementazione della Strategia), si potrà far ricorso anche alle disponibilità dei citati Fondo per l'attuazione della Strategia nazionale di cybersicurezza e Fondo per la gestione della cybersicurezza, istituiti nello stato di previsione del Ministero dell'economia e delle finanze con legge n. 197/2022 (vds. capitolo 6).

Una parte delle risorse finanziarie destinate al funzionamento dell'Agenzia è stata dedicata al raggiungimento dell'obiettivo, considerato primario, della crescita di competenze e specifiche professionalità mediante il reclutamento di personale con elevate compe-

tenze nel settore della *cybersecurity*, ma anche, per altro verso, all'acquisizione di immobilizzazioni immateriali e materiali connotate dal forte contenuto di innovazione.

A quest'ultimo riguardo, assumono particolare rilevanza i costi di ricerca e sviluppo, finanziati con fondi PNRR, attraverso i quali l'Agenzia intende dare attuazione a numerose misure della Strategia nazionale di cybersicurezza, ad esempio interventi volti alla realizzazione, allo sviluppo o all'evoluzione di applicazioni software, nonché allo sviluppo di attività specialistiche di natura intellettuale, di studio, progettazione, analisi d'impatto, finalizzate alla realizzazione di nuovi strumenti software. Tali prodotti rappresentano elementi patrimoniali destinati a essere utilizzati durevolmente, ossia a far parte per un periodo di tempo prolungato della struttura tecnico-organizzativa e strategica dell'organizzazione.

L'Agenzia ha strutturato, nel corso dell'anno, processi atti a definire la razionalizzazione degli acquisti, in linea con la pianificazione e la programmazione nel rispetto degli obiettivi di bilancio, della normativa di settore e delle *milestone* e *target* previsti dal PNRR, migliorando e dando uniformità alla gestione degli acquisti predisposti secondo la programmazione biennale (2023-2024). È stata, inoltre, adottata una disciplina interna per le procedure di spesa volta a stabilire un quadro di regole comuni, in aderenza all'efficienza e alla piena tracciabilità dei flussi informativi legati alla spesa.

Al tempo stesso, l'ACN è stata chiamata a misurarsi con la disciplina degli appalti PNRR, dalla quale è emersa la necessità di contemperare gli interessi della sicurezza nazionale nello spazio cibernetico, cui l'Agenzia è preposta, con il nuovo assetto normativo in materia di contratti pubblici. In particolare, l'entrata in vigore del nuovo Codice dei contratti pubblici (D.Lgs. n. 36/2023) ha richiesto di operare un opportuno coordinamento con la normativa derogatoria dell'Agenzia in materia (DPCM 1° settembre 2022, n. 166), che ha poi consentito all'Agenzia di poter avviare, secondo quest'ultima disciplina, una procedura negoziata per l'acquisto di strumentazioni informatiche di carattere specialistico per assicurare lo svolgimento di attività di particolare rilievo operativo ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

L'Agenzia, in attuazione del c.d. "principio del risultato", di cui al Codice dei contratti pubblici, e in un'ottica di snellimento e semplificazione dell'azione amministrativa, il 4 luglio 2023 si è qualificata quale stazione appaltante per l'affidamento di servizi e forniture fino a 750.000 euro e per l'affidamento di lavori fino a 1.000.000 euro.

7.3 PREVENZIONE DELLA CORRUZIONE, TRASPARENZA E PROTEZIONE DEI DATI

Trasparenza, correttezza, tempestività e protezione dei dati sono alcuni dei valori ai quali l'Agenzia ha da subito improntato la sua azione. In linea con questi valori, nell'ambito del

processo di strutturazione interna, si è adoperata per rendere le proprie procedure coerenti con l'obiettivo di conformarsi velocemente alle generali regole applicabili agli enti pubblici in materia di prevenzione della corruzione, di trasparenza dell'attività amministrativa e di protezione dei dati, compatibilmente con le funzioni in materia di sicurezza nazionale.

In tale ottica, il Direttore generale dell'ACN ha definito gli "Obiettivi strategici dell'Agenzia in materia di prevenzione della corruzione e trasparenza" e ha adottato il Piano triennale di prevenzione della corruzione e della trasparenza 2023-2025.

Nel medesimo contesto, l'Agenzia ha provveduto ad:

- attivare la sezione "Amministrazione trasparente" sul sito web istituzionale;
- allineare la propria procedura di segnalazione degli illeciti (c.d. *whistleblowing*) alle prescrizioni del D.Lgs. n. 24/2023 e secondo le indicazioni fornite dalle Linee guida dell'Autorità nazionale anticorruzione. A tal fine, è stata è stata predisposta una piattaforma informatica di *Whistleblowing*;
- adottare il proprio Codice etico.

In materia di protezione dei dati, ai fini della corretta implementazione del concetto di *accountability* – pilastro centrale del Regolamento (UE) 2016/679 (GDPR) – e pertanto dell'assegnazione, a ogni trattamento svolto dall'Agenzia, delle corrette misure di sicurezza tecniche e organizzative, sono state analizzate le molteplici attività istituzionali. In tale contesto, le stesse sono state confrontate con i parametri desumibili dalle più aggiornate linee guida fornite da ENISA, dal *National Institute of Standards and Technology* statunitense e dai controlli contemplati dalle norme ISO via via applicabili, onde attribuire a ciascuna attività un coefficiente di rischio e l'individuazione delle misure necessarie a contenerlo. Le misure di sicurezza già in essere sono state confrontate con quelle suggerite dall'esito dell'indagine di cui sopra, ai fini del loro adeguamento e realizzazione.

Relativamente alle attività di trattamento che risultavano meritevoli di ulteriori approfondimenti, alla luce delle linee guida predisposte dall'*European Data Protection Board,* sono state svolte le corrispondenti analisi di impatto *privacy*, come previsto dall'art. 35 del GDPR.

È stato poi predisposto il manuale relativo alla *data protection* per i dipendenti dell'Agenzia, dedicato alla formazione e alla consultazione periodica.

Infine, l'informativa *privacy* dell'Agenzia, elemento centrale per concretizzare il requisito della trasparenza, è stata aggiornata e contestualizzata in relazione alle varie attività svolte, adottando al contempo un innovativo modello di infografica sviluppato dall'Università di Maastricht, tra i vincitori del *contest* "Informative chiare" lanciato dal Garante per la protezione dei dati personali nel 2021.

Nel medesimo contesto, anche in aderenza al protocollo sottoscritto nel 2022, la collaborazione con il Garante è stata particolarmente proficua, anche in ragione dei diversi punti di contatto tra sicurezza cibernetica e tutela dei dati personali.

7.4 COMUNICAZIONE

Nel corso del 2023 l'Agenzia ha posto particolare attenzione sul rafforzamento della sua proiezione esterna, attività indispensabile per far conoscere e comprendere il suo ruolo e per migliorare l'interazione con le diverse comunità di riferimento, dai soggetti inclusi nella *constituency* alla cittadinanza nel suo complesso, fino agli interlocutori stranieri.

Al riguardo, in collaborazione con le strutture del CSIRT Italia, sono state promosse attività di comunicazione istituzionale in occasione di eventi e incidenti *cyber* rilevanti, al fine di fornire un'informazione chiara e accurata verso i media e il pubblico, oltre che per supportare le amministrazioni, vittime di incidenti informatici, nel gestire la comunicazione stessa.

La costruzione e il rafforzamento dell'identità dell'Agenzia sono state consolidate anche tramite un'informazione costante e trasparente, attraverso i media e i canali di comunicazione istituzionali, delle iniziative e dei progetti strategici. In tal senso vanno le iniziative volte a valorizzare le attività progettuali e le opportunità per imprese e centri di ricerca, nonché a favorire la diffusione della cultura *cyber* nella società italiana, per sensibilizzare e promuovere le competenze dei cittadini e accrescere la consapevolezza sui rischi derivanti dall'uso delle tecnologie informatiche.

Nell'anno di riferimento sono state avviate numerose iniziative di promozione e divulgazione della visione strategica dell'Agenzia e delle attività tecnico-progettuali, realizzando oltre 50 interviste a dirigenti ACN e pubblicando 21 comunicati stampa.

Sul fronte della comunicazione digitale, nel mese di giugno è stato pubblicato il nuovo sito web istituzionale, innovato nella forma, nei contenuti e nel *design*, con l'obiettivo di informare con chiarezza i cittadini, le amministrazioni e le imprese sulle iniziative, le norme e le opportunità della cybersicurezza. Il nuovo sito contiene notizie e informazioni sull'attività istituzionale dell'ACN, con circa 200 notizie pubblicate nel corso dell'anno, approfondimenti sulle progettualità strategiche, anche attraverso la rete dei portali pubblici (di CSIRT Italia e del CVCN), rispetto ai quali il sito web istituzionale funge da porta di accesso.

A soli sei mesi dalla sua pubblicazione, il sito web ha registrato un totale di circa 174.000 visite, durante le quali sono state effettuate diverse azioni, tra cui la visualizzazione delle pagine, il *download* di documenti (per un totale di circa 70.000) e la ricerca interna dei contenuti di approfondimento. Le "visualizzazioni pagina" si attestano intorno alle 525.000, di cui circa 350.000 rappresentano visualizzazioni uniche.

SITO WEB ACN

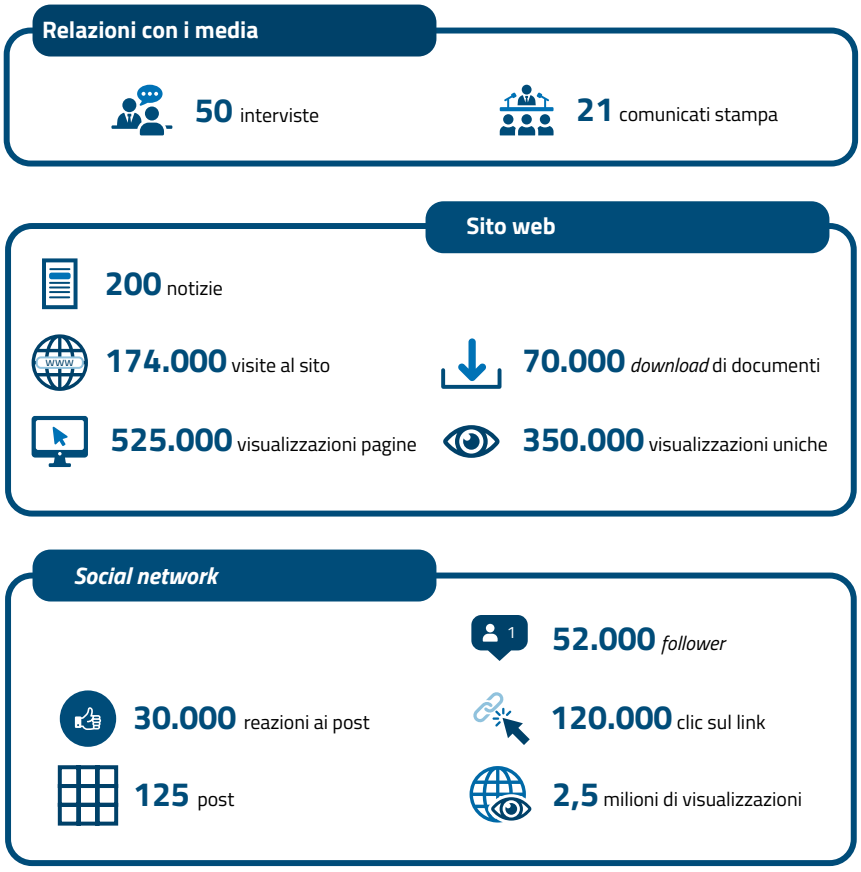
Il nuovo sito web è stato progettato secondo le linee guida del Codice dell'amministrazione digitale per il *design* dei siti Internet e i servizi digitali della PA e la normativa sull'accessibilità dei siti web e delle applicazioni mobili, in conformità con la Direttiva (UE) 2016/2102. Il sito web fornisce contenuti accessibili a tutti grazie a un'esperienza di navigazione ottimale anche per chi fa uso di tecnologie assistive o particolari configurazioni di sistema.

www.acn.gov.it

Per quanto riguarda i *social network*, è proseguita la crescita della pagina *LinkedIn*, privilegiando una narrazione volta a promuovere la conoscenza del ruolo e delle competenze dell'Agenzia, mentre a ottobre è stato aperto il canale istituzionale su *YouTube*. Le attività di comunicazione su *LinkedIn* hanno portato a un netto aumento di *follower* dell'ACN rispetto al 2022, raggiungendo oltre 52.000 contatti. La produzione di contenuti ha generato, con 125 post, oltre 2,5 milioni di visualizzazioni, oltre 30.000 reazioni, mentre sono stati registrati 120.000 clic sui link dei contenuti diffusi da ACN.

La diffusione di specifiche campagne informative è uno degli strumenti attraverso cui l'Agenzia mira ad aumentare il livello di consapevolezza del rischio *cyber*. Come già ricordato (vds. capitolo 5), in concomitanza con il mese europeo della cybersicurezza,

l'Agenzia ha promosso alcune campagne informative, in collaborazione con ABI, CERTFin e Banca d'Italia, e con ENISA. Quest'ultima campagna, in particolare, è stata diffusa sul sito web dell'Agenzia, sul profilo *LinkedIn* e sul canale *YouTube*, totalizzando, sui canali *social*, circa 108.000 visualizzazioni e 10.000 interazioni. I clic sui contenuti diffusi sono stati 8.340 mentre le reazioni circa 1.400. Il mese di campagna ha visto una copertura di circa 76.000 utenti.



8.

LISTA DEGLI ACRONIMI

A

AgID: Agenzia per l'Italia digitale

AISE: Agenzia informazioni e sicurezza esterna

AISI: Agenzia informazioni e sicurezza interna

ANCS: Agence Nationale de la Cybersécurité

APRE: Agenzia per la promozione della ricerca europea

APT: *Advanced Persistent Threat*

ASCII: A SCuola di sIcurezza cIbernetica

C

CBM: *Confidence-Building Measure*

CCRA: *Common Criteria Recognition Arrangement*

CERT: *Computer Emergency Response Team*

CIC: Comitato interministeriale per la cybersicurezza

CIN: *Cyber Innovation Network*

CINI: Consorzio interuniversitario nazionale per l'informatica

CISA: *Cybersecurity and Infrastructure Security Agency*

COPASIR: Comitato parlamentare per la sicurezza della Repubblica

CRA: *Cyber Resilience Act*

CRI: *Counter Ransomware Initiative*

CRUI: Conferenza dei rettori delle università italiane

CSA: *Cybersecurity Act*

CSIRT: *Computer Security Incident Response Team*

CSoA: *Cyber Solidarity Act*

CTS: Comitato tecnico-scientifico

CV: Centro di valutazione

CVCN: Centro di valutazione e certificazione nazionale

CVD: *Coordinated Vulnerability Disclosure* – Divulgazione coordinata delle vulnerabilità

D

DDFIR: *Deployable Digital Forensic Incident Response*

DDoS: *Distributed Denial of Service*

DEP: *Digital Europe Programme*

DIS: Dipartimento delle informazioni per la sicurezza

DTD: Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri

E

ECCC: *European Cybersecurity Competence Centre* – Centro europeo di competenze in cybersicurezza

ECCG: *European Cybersecurity Certification Group*

ECSF: *European Cybersecurity Skills Framework*

ENISA: *European Union Agency for Cybersecurity* – Agenzia dell'Unione europea per la cibersicurezza

EU-CyCLONe: *European Cyber Crisis Liaison Organisation Network*

EUCC: *European Common Criteria*

EUCS: *European Cybersecurity Certification Scheme for Cloud Services*

F

FIRST: *Forum of Incident Response and Security Teams*

G

GFCE: *Global Forum on Cyber Expertise*

GPDP: Garante per la protezione dei dati personali

H

HPC: *High Performance Computing*

HWPCI: *Horizontal Working Party on Cyber Issues*

I

IA: Intelligenza Artificiale

ICT: *Information and Communication Technologies* – Tecnologie dell'informazione e della comunicazione

ISAC: *Information Sharing and Analysis Centre*

ITS: Istituti tecnologici superiori

L

LAP: Laboratori accreditati di prova

LVS: Laboratori di valutazione della sicurezza

M

MAC: *Message Authentication Code* – Codice di autenticazione del messaggio

MAECI: Ministero degli affari esteri e della cooperazione internazionale

MEF: Ministero dell'economia e finanze

MIM: Ministero dell'istruzione e del merito

MIMIT: Ministero delle imprese e del *made in Italy*

ML: *Machine learning*

MUR: Ministero dell'università e della ricerca

N

NCC: *National Coordination Centre* – Centro nazionale di coordinamento

NCCA: *National Cybersecurity Certification Authority*

NCS: Nucleo per la cybersicurezza

NIS: *Network and Information Systems*

NISCG: *NIS Cooperation Group* – Gruppo di cooperazione NIS

NISP: Nucleo interministeriale situazione e pianificazione

NLO: *National Liaison Officer*

O

OCSI: Organismo di certificazione della sicurezza informatica

P

PA: Pubblica Amministrazione

PMI: Piccole e medie imprese

PNRR: Piano nazionale di ripresa e resilienza

PPP: *Partnership* pubblico-privato

PSNC: Perimetro di sicurezza nazionale cibernetica

S

SNA: Scuola nazionale dell'amministrazione

SOC: *Security Operation Centre*

SOG-IS: S*eniors Officials Group Information Systems Security*

T

TTO: *Technology Transfer Offices*

PAGINA BIANCA

192180104640