RELAZIONE ANNUALE AL PARLAMENTO

2024

RELAZIONE ANNUALE AL PARLAMENTO 2024

SOMMARIO

SOMMARIO

PREFAZIONE

La Relazione al Parlamento sull'attività svolta dall'ACN nel 2024 è occasione per cogliere la complessità delle attività che vedono l'Agenzia quotidianamente impegnata a protezione della cybersicurezza della Nazione.

Benché, infatti, l'attenzione nel dibattito pubblico sulla cybersecurity si focalizzi per lo più sui numerosi attacchi informatici, gran parte dei quali privi di conseguenze, dalla lettura della Relazione emerge come la sicurezza cibernetica costituisca in realtà una sfida più ampia, il cui successo – mai definitivo – è legato a molteplici fattori, e ad azioni che agiscono su più livelli: il rafforzamento delle infrastrutture digitali pubbliche e private critiche; la sensibilizzazione e la formazione per irrobustire il "fattore umano", primo ineludibile presidio di sicurezza delle reti e dei sistemi informatici; il miglioramento della capacità di risposta agli attacchi cyber. Senza dimenticare, a monte, il potenziamento della capacità di generare innovazione tecnologica, attraverso investimenti in ricerca e sviluppo, nonché con collaborazioni con università, enti di ricerca e imprese.

Il Governo ha accompagnato gli sforzi compiuti dall'Agenzia nel 2024 in ciascuno dei piani in cui si articola la minaccia cyber.

Lo ha fatto anzitutto adeguando il quadro normativo: la legge n. 90/2024 – di iniziativa dell'Esecutivo, ma approvata dal Parlamento pressoché all'unanimità, grazie al positivo confronto con le forze di opposizione – ha introdotto innovazioni importanti, come il rafforzamento dei requisiti di cybersicurezza del procurement pubblico, una maggiore fluidità nei rapporti tra ACN, Polizia giudiziaria e Autorità giudiziaria in presenza di incidenti informatici, l'estensione dei principali obblighi di cybersecurity a realtà amministrative mai considerate prima dalla normativa di settore, come Regioni, Città metropolitane, Comuni e Aziende sanitarie locali. Il decreto legislativo n. 138/2024 ha poi recepito la Direttiva (UE) 2022/2555 (c.d. Direttiva NIS2), che ha radicalmente innovato lo spazio digitale europeo.

Molto è stato fatto per rafforzare la vicinanza dell'ACN ai vari soggetti del sistema digitale italiano, pubblico e privato, tramite la sottoscrizione di protocolli di collaborazione e con iniziative divulgative e di sensibilizzazione sul territorio nazionale, nei confronti di Regioni, Amministrazioni locali, Aziende sanitarie locali, piccole e medie imprese. L'accordo stipulato a dicembre col Ministero dell'istruzione e del merito permette di realizzare progetti analoghi nelle scuole.

Il Governo ha supportato le iniziative dell'ACN per stimolare investimenti sul fronte della cybersicurezza e dell'innovazione tecnologica, a partire dal settore dell'intelligenza artificiale. L'Europa e l'Italia si stanno spendendo per affermare, a livello globale, una visione dell'IA etica, antropocentrica, rispettosa dei diritti fondamentali; questo impegno rischia di rivelarsi velleitario, se non è supportato dalla capacità tecnologica di contribuire in modo efficace allo sviluppo di questo nuovo prodotto dell'ingegno umano. Emblematico dello sforzo profuso in tal senso è l'investimento da 400 milioni di euro (cofinanziati dal Governo italiano e dalla Commissione europea) per installare, nell'ambito del progetto "IT4LIA AI Factory", un supercalcolatore ottimizzato per l'IA nel Tecnopolo di Bologna.

Sfide globali richiedono risposte globali: per questo il Governo si è adoperato per consolidare la cybersicurezza sul piano internazionale. A cominciare dal G7, nella cui cornice l'Italia, Presidente di turno, ha promosso la costituzione di un nuovo Gruppo di lavoro dedicato alla sicurezza cibernetica, riscontrando ampio favore dei nostri partner; lo attesta l'inserimento di uno specifico paragrafo dedicato alla cybersecurity nella Dichiarazione finale del Vertice G7 dei Capi di Stato e di Governo. È un importante passo in avanti nella direzione di una maggiore cooperazione tra le democrazie occidentali.

Nonostante le crescenti difficoltà del contesto di riferimento – sempre più turbolento, con la dimensione cyber che rappresenta uno dei principali canali di sfogo delle tensioni globali – va riconosciuto all'ACN di aver svolto un lavoro tanto delicato quanto intenso: esso sta già proseguendo con determinazione nel 2025, per rafforzare la resilienza cibernetica del sistema-Italia.

Alfredo Mantovano

INTRODUZIONE

In uno scenario caratterizzato da un contesto geopolitico in rapido cambiamento e da un utilizzo sempre più intenso e massivo delle nuove tecnologie, il 2024 si conferma come un anno di sfide in cui gli attori malevoli hanno continuato a utilizzare – sarebbe meglio dire a sfruttare – il dominio cyber per perseguire i propri obiettivi. In tale contesto, l'Agenzia per la cybersicurezza nazionale ha proseguito il suo lavoro su più fronti per rafforzare la resilienza sistemica del Paese, in termini sia di accrescimento della capacità di protezione della superficie digitale, che di promozione dello sviluppo tecnologico.

Non si è trattato di un'azione volta solo a confrontarsi con gli effetti di una crescente minaccia, bensì di un impegno più articolato e vasto, in cui si compendiano gli elementi che in diverso modo concorrono a garantire la resilienza dell'ecosistema digitale nazionale.

In questo complesso compito, l'ACN ha agito all'interno di un'architettura istituzionale ormai solida, composta da più attori con distinte competenze e funzioni. Un'architettura che vede l'ACN in una posizione centrale per le funzioni di coordinamento e di raccordo che le vengono assegnate, e, soprattutto, per il ruolo di indirizzo e monitoraggio nell'attuazione della Strategia nazionale e del suo Piano di implementazione.

L'impegno profuso dall'Agenzia, di cui dà atto la Relazione, le ha consentito di dialogare e collaborare con le Istituzioni, le Pubbliche Amministrazioni – centrali e locali – con il mondo dell'Accademia e le Imprese. In una parola, di rivolgersi all'intera Comunità nazionale.

Solo con il contributo di tutti si può fronteggiare, infatti, una minaccia così penetrante, divenuta sempre più sofisticata e in grado di coinvolgere porzioni crescenti della popolazione, a partire dai più indifesi e dai più esposti.

La maturazione, nelle varie componenti sociali, di una più forte coscienza del rischio digitale è una condizione ineludibile per dare fondamenta più robuste alla resilienza del Paese. Come lo è, altresì, curare la crescita delle competenze digitali.

Consapevolezza e formazione, del resto, rientrano pienamente nel concetto di cultura cibernetica perché entrambe considerano il fattore umano come un terreno di impegno, sia pure dedicandovi strumenti e modalità di intervento diversi.

Operare perché la sicurezza informatica venga irrobustita e preservata in favore di ciascun cittadino è anche una grande questione di democrazia digitale e di protezione effettiva della libertà e della dignità della persona.

La dimensione globale della minaccia – in cui tanto gli attacchi quanto le soluzioni non conoscono confini – esige una risposta altrettanto globale, concertata e condivisa a livello internazionale.

In occasione della Presidenza italiana del G7, il nostro Paese ha potuto affermare, anche in ambito cyber, la sua importante statura internazionale. Su iniziativa dell'ACN, è stato costituito, per la prima volta, un Gruppo di lavoro G7 sulla cybersicurezza, venendo così a creare uno spazio di cooperazione continuativa tra le agenzie e i centri cyber dei Paesi like-minded, unico nel suo genere.

Lo scopo di promuovere una così inedita strategia di governance globale ha messo radici. L'esercizio, infatti, proseguirà anche nel corso della Presidenza canadese, e potrà offrire ulteriori spunti per una comune riflessione su temi cruciali per la cybersicurezza. Temi che, mai come ora, sembrano richiedere la più stretta solidarietà tra le grandi democrazie occidentali.

Il 2024 si è caratterizzato, inoltre, per un'articolata revisione del quadro normativo in materia di cybersicurezza, sia a livello nazionale che in ambito di Unione europea. Passaggi significativi e importanti sono stati, in tal senso, l'introduzione della legge 90 e il recepimento nazionale della Direttiva NIS2.

L'impegno dell'Agenzia, anche a quest'ultimo riguardo, è stato massimo, esprimendosi sia nella dimensione organizzativa – soprattutto con la realizzazione di una piattaforma informatica per la registrazione delle entità NIS, pubbliche e private – sia nella dimensione divulgativa, con iniziative di diffusione della conoscenza dei contenuti e degli effetti che sono attesi dall'impatto della nuova direttiva europea, sia, infine, nella dimensione coordinamentale, con l'attivazione del Tavolo NIS, cui partecipano le 9 Autorità di settore e i rappresentanti delle Regioni.

Una complessa attività di regia, quest'ultima, che si prefigge, ancora una volta, di contribuire al rafforzamento della resilienza sistemica nazionale.

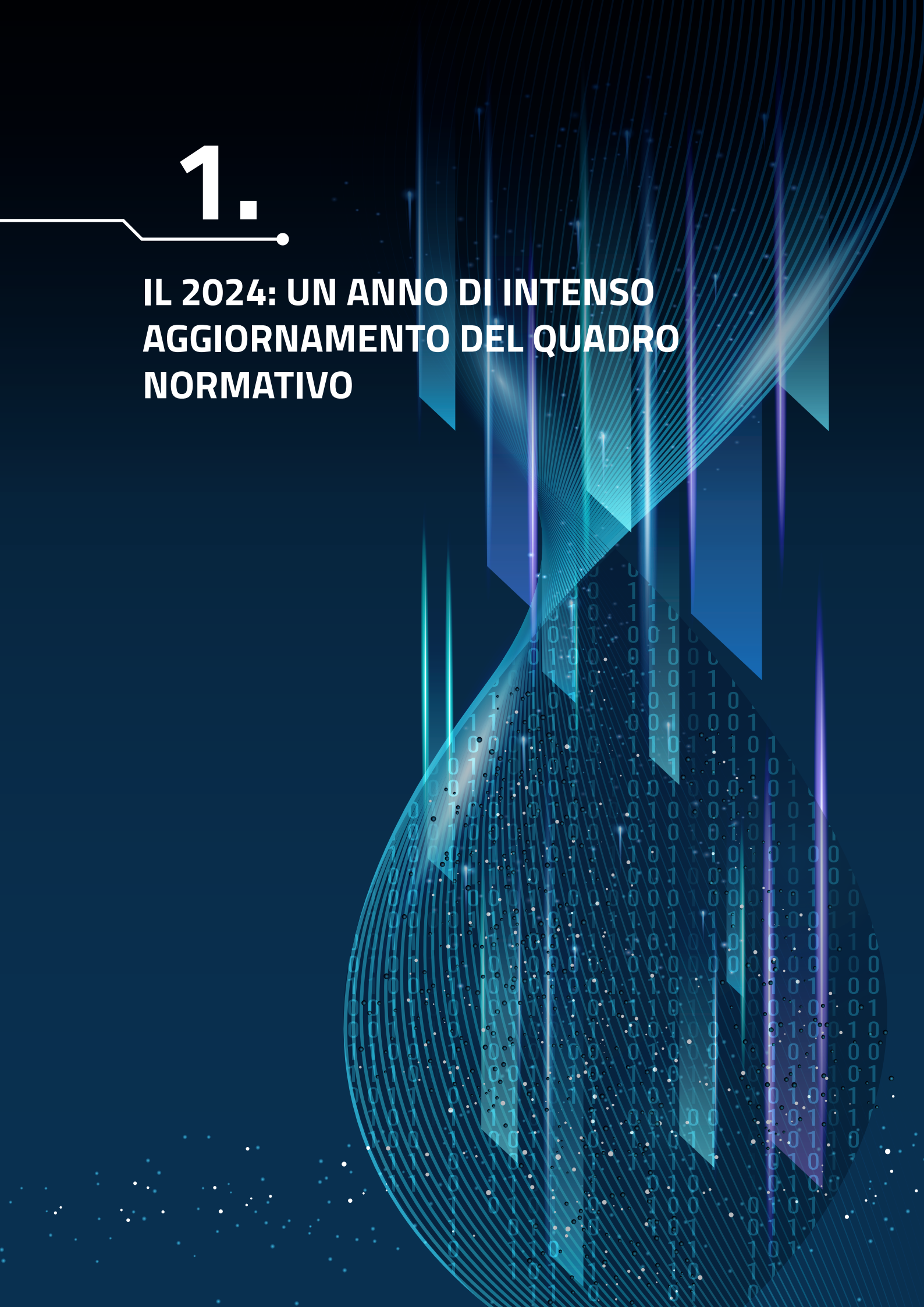
È così che l'Agenzia sta accompagnando il Paese nell'innalzamento della propria postura di cybersicurezza, mettendo a frutto le risorse del bilancio interno e i finanziamenti del PNRR.

Rivolgo, in conclusione, un doveroso e sentito ringraziamento al personale tutto dell'Agenzia per l'intensità e la qualità del lavoro svolto, e all'Autorità delegata per la sicurezza della Repubblica, per l'indirizzo, il sostegno e l'incoraggiamento costantemente assicurati.

Bruno Frattasi

1.

IL 2024: UN ANNO DI INTENSO AGGIORNAMENTO DEL QUADRO NORMATIVO



Nel 2024 l'Agenzia per la cybersicurezza nazionale è stata impegnata a garantire che il quadro normativo in materia di sicurezza cibernetica risultasse costantemente aggiornato e coerente. Infatti, in un contesto caratterizzato da un'evoluzione tecnologica rapida e continua, è essenziale la parallela evoluzione delle norme relative alla cybersicurezza, sia per far fronte alla costante crescita delle minacce informatiche che possono costituire un pregiudizio per la sicurezza nazionale e mettere a rischio gli interessi del Paese e quelli dei cittadini, sia perché le nuove tecnologie – se gestite in sicurezza – costituiscono un importante strumento di sviluppo e innovazione.

Il 2024 è stato un anno particolarmente intenso in questo ambito, dal momento che ha visto l'introduzione di numerosi provvedimenti, alcuni dei quali più puntuali e altri di più ampio respiro, sia sul piano prettamente nazionale che di adeguamento alle evoluzioni normative dell'UE. Tra gli interventi più rilevanti, si segnala l'introduzione della legge n. 90/2024 che, tra le altre cose, contiene prescrizioni volte a rafforzare la protezione dai rischi informatici delle Pubbliche Amministrazioni (PA). Ciò ha permesso, inoltre, di anticipare l'entrata in vigore di alcuni obblighi prescritti, a livello europeo, dalla Direttiva NIS2, il cui recepimento nell'ordinamento italiano è avvenuto con il D.Lgs. n. 138/2024 e che prevede un significativo ampliamento delle misure a protezione della superficie digitale dell'Unione. Un ulteriore provvedimento da segnalare è il c.d. Regolamento *cloud* con il quale si è inteso accompagnare le PA nel percorso verso una digitalizzazione sicura.

Attraverso tali provvedimenti, e altri che saranno citati nel prosieguo, sono state introdotte procedure standardizzate, obblighi puntuali e un maggiore coordinamento tra le istituzioni pubbliche e i soggetti privati, ottimizzando e semplificando la gestione della sicurezza informatica mediante strumenti adeguati che consentiranno di operare in un mondo digitale sempre più complesso e articolato.

1.1 LA LEGGE N. 90/2024: PER UN RAFFORZAMENTO DELLA RESILIENZA CYBER SU TUTTO IL TERRITORIO NAZIONALE

Con la legge n. 90/2024, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", sono stati perseguiti vari obiettivi. Da un lato, rafforzare il quadro di sicurezza cibernetica prevedendo obblighi di notifica e misure preventive per garantire la protezione dei soggetti interessati e anticipare gli attacchi cibernetici. Dall'altro, stabilire procedure di coordinamento tra gli attori coinvolti garantendo un bilanciamento tra le esigenze di resilienza, quelle investigative e quelle di *intelligence*. A ciò si aggiunge un generale aggiornamento del quadro penalistico in materia cyber.

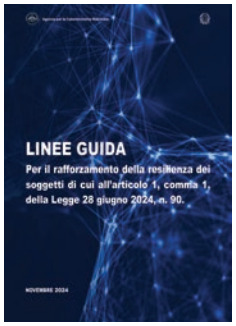
La legge introduce specifici obblighi di notifica degli incidenti cyber al CSIRT Italia (*Computer Security Incident Response Team*, la struttura tecnico-operativa dell'Agenzia) e prevede il rafforzamento delle misure di sicurezza per determinate categorie di soggetti, tra cui le Pubbliche Amministrazioni centrali, le Regioni e le Province autonome di Trento e di Bolzano, i Comuni con più di 100.000 abitanti, le società di trasporto pubblico con bacini di utenza equivalenti e le Aziende sanitarie locali. Tra tali soggetti sono comprese, altresì, le rispettive società *in house* che forniscono servizi informatici, i servizi di trasporto indicati dalla norma, ovvero servizi di raccolta, smaltimento o trattamento di acque reflue o di gestione dei rifiuti.

L'allargamento dei soggetti cui si applica l'obbligo di notifica mira a rafforzare la prevenzione e la gestione degli incidenti, riducendo i tempi di risposta e limitandone l'impatto. Sempre a tal fine, la legge prevede, inoltre, che l'ACN possa inviare segnalazioni relative a specifiche vulnerabilità alle Amministrazioni, agli enti pubblici e agli altri soggetti, fornitori di servizi pubblici, che risultano esservi potenzialmente esposti. Si è introdotta, così, una modalità di puntuale interlocuzione tra l'ACN e l'entità esposta alla potenziale minaccia, prima del tutto assente nel sistema; modalità che rappresenta una forma non alternativa bensì ulteriore rispetto agli *alert* generali che, invece, si indirizzano verso una più estesa platea soggettiva. I destinatari di tali segnalazioni devono provvedere tempestivamente all'adozione degli interventi risolutivi dandone comunicazione all'Agenzia. L'ACN nella seconda metà del 2024 ha provveduto a inviare 6 segnalazioni circa specifiche vulnerabilità ai soggetti che sono risultati potenzialmente esposti, nonché a indicare gli interventi risolutivi da adottare.

Altro punto rilevante riguarda il rafforzamento della resilienza delle PA, attraverso l'istituzione di una struttura interna alle Amministrazioni dedicata alla sicurezza cibernetica, presso la quale individuare la figura del referente per la cybersicurezza a cui è affidato il compito di garantire che i diversi processi operativi siano in linea e si conformino alle indicazioni dell'ACN, incluse quelle previste da specifiche Linee guida (vedasi box).

Linee guida ACN

Il ricorso a Linee guida, quale strumento di soft law, è stato scelto dall'ACN in diverse occasioni per garantire la conformità alle normative e il miglioramento della sicurezza complessiva di Amministrazioni e operatori interessati.



Al fine di accompagnare i soggetti nella concreta attuazione delle misure volte al rafforzamento della loro resilienza, previste dalla legge n. 90/2024, l'ACN ha adottato specifiche Linee guida. Queste sono articolate in due parti. La prima individua 26 misure di sicurezza indicando i requisiti minimi da soddisfare per l'implementazione minima attesa, una descrizione di dettaglio della misura e i contenuti dell'impianto documentale che i soggetti devono produrre. La seconda supporta e indirizza questi ultimi nell'attuazione delle misure stesse, descrivendo le modalità di implementazione raccomandate.

L'Agenzia ha impiegato lo strumento delle Linee guida anche per meglio specificare le modalità di protezione delle banche dati critiche rispetto al rischio di utilizzo improprio. Il documento si inserisce nella più ampia azione dell'ACN volta a rafforzare la resilienza dello spazio digitale italiano attraverso misure tecniche, organizzative e procedurali indirizzate, in primo luogo, ai soggetti pubblici e privati inclusi nel Perimetro di sicurezza nazionale cibernetica (PSNC). Le Linee guida indicano una serie di possibili azioni di contrasto alla minaccia – interna ed esterna – di utilizzo improprio delle banche dati, in particolare in termini di misure di sicurezza, raccomandazioni e buone pratiche.

La legge n. 90/2024 è intervenuta anche nell'ambito della disciplina del *procurement* pubblico, poiché l'approvvigionamento di beni e servizi informatici è fondamentale, data la sua rilevanza ai fini della resilienza cyber. In particolare, tale intervento, in continuità con le disposizioni contenute nel Codice dei contratti pubblici (D.Lgs. n. 36/2023), prevede l'individuazione degli elementi

essenziali di cybersicurezza che le PA, i gestori di servizi pubblici, le società a controllo pubblico, nonché i soggetti privati inseriti nel Perimetro devono tenere in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici. Il coinvolgimento diretto dell'Agenzia nell'individuazione degli elementi essenziali di cybersicurezza garantisce che le misure adottate siano conformi agli standard internazionali e alle migliori pratiche in materia.

Nella medesima prospettiva, è prevista l'introduzione, per la tutela della sicurezza nazionale, di criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di determinati Paesi. Questi includono gli Stati membri dell'Unione europea, quelli aderenti all'Alleanza atlantica (*North Atlantic Treaty Organization*-NATO), nonché Paesi terzi individuati con apposito DPCM tra quelli che sono parte di accordi di collaborazione con l'UE o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

La legge n. 90/2024 valorizza anche l'utilizzo della crittografia quale strumento di protezione cibernetica e istituisce il Centro nazionale di crittografia presso l'Agenzia (vedasi box). Al riguardo, la legge dispone che l'ACN provveda allo sviluppo e alla diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, nonché alla valutazione della sicurezza dei sistemi crittografici. Inoltre, demanda all'Agenzia l'attivazione delle procedure per promuovere la collaborazione con centri universitari e di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali, nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni.

Centro nazionale di crittografia

La legge n. 90/2024 ha istituito il Centro nazionale di crittografia, col compito di svolgere le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato. L'ACN ha avviato specifiche iniziative per istituire il Centro, il cui funzionamento sarà disciplinato con un provvedimento del Direttore generale.

Ciò rappresenta un ulteriore passo per diffondere il corretto utilizzo della crittografia come strumento di cybersicurezza, ambito nel quale l'Agenzia è attivamente impegnata fin dalle origini e al quale ha dedicato una serie di pubblicazioni, le "Linee guida 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 (vedasi Capitolo 4).

La legge disciplina, inoltre, i rapporti tra l'Agenzia, il Procuratore nazionale antimafia e antiterrorismo, la Polizia giudiziaria e il Pubblico ministero, introducendo un sistema di reciproca informazione volto a contemperare le esigenze dell'accertamento giudiziario con quelle, altrettanto importanti, di resilienza operativa dei sistemi e dei servizi impattati, per una loro più immediata ripresa funzionale. Al riguardo, il legislatore ha normato una prassi collaborativa già in essere tra i soggetti citati che si è dimostrata vincente anche rispetto a specifici casi giudiziari.

Si prevede, in particolare, che l'ACN informi senza ritardo il Procuratore nazionale antimafia e antiterrorismo nei casi in cui ha notizia di un attacco ai sistemi informatici o telematici di cui all'art. 371-*bis*, co. 4-*bis*, del Codice di procedura penale e, in ogni caso, quando risultino interessati soggetti inclusi nel PSNC, operatori di servizi essenziali e fornitori di servizi digitali (soggetti

NIS), imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico (soggetti TELCO). Corrispondentemente, il Pubblico ministero – quando acquisisce la notizia dei citati gravi delitti informatici – deve darne tempestiva informazione all'Agenzia, assicurando anche il raccordo informativo con l'organo centrale del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione. Il Pubblico ministero, in ogni caso, ricevuta la notizia di reato e assunta la direzione delle indagini, è chiamato a impartire le disposizioni necessarie ad assicurare che gli accertamenti urgenti si svolgano tenendo conto delle attività di ripristino svolte dall'Agenzia e può eventualmente disporre il differimento di una o più attività per evitare un grave pregiudizio per il corso delle indagini. Viene, infine, introdotta la possibilità per l'ACN di partecipare agli accertamenti tecnici irripetibili per i delitti richiamati.

Per garantire il miglior allineamento informativo tra l'Agenzia, la Direzione nazionale antimafia e antiterrorismo e la Polizia di Stato, è stato siglato un protocollo finalizzato proprio a strutturare il flusso delle informazioni, necessario per consentire a ognuna delle parti di esercitare le funzioni attribuite dalla legge.

Sempre nell'ottica di un bilanciamento delle diverse esigenze che possono entrare in gioco in caso di eventi o incidenti cyber, la legge n. 90/2024 disciplina anche il coordinamento operativo tra l'ACN e gli Organismi di informazione per la sicurezza della Repubblica. Viene introdotta, infatti, una specifica procedura che consente alle Agenzie di informazione per la sicurezza (AISE e AISI) di richiedere, in caso di eventi o incidenti informatici, il differimento di attività di resilienza per il perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza della Repubblica. Tale richiesta avviene attraverso il Dipartimento delle informazioni per la sicurezza (DIS) e deve essere valutata dal Presidente del Consiglio dei ministri, sentiti i Direttori generali del DIS e dell'ACN.

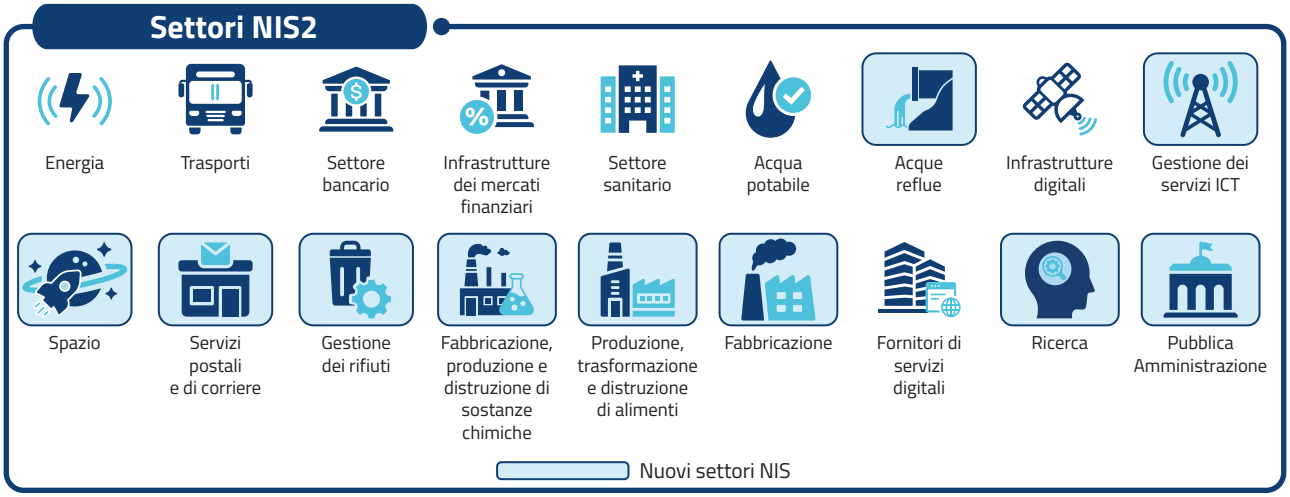
1.2 LA DISCIPLINA NIS2: UNO SGUARDO A TUTTO TONDO PER INNALZARE LE PROTEZIONI CYBER DEL PAESE

Con riferimento all'attività legislativa di derivazione europea, il 2024 è stato caratterizzato dalla scadenza del 17 ottobre per il recepimento nazionale della Direttiva NIS2 (Direttiva (UE) 2022/2555), volta a garantire un livello comune elevato di cybersicurezza nell'UE. La direttiva, nel rinnovare e rafforzare l'impianto delineato dalla precedente direttiva in materia di *Network and Information Security* (NIS), intende contribuire a un migliore funzionamento del mercato unico attraverso un generale innalzamento della sicurezza e resilienza cyber dell'Unione nel suo complesso e dei suoi Stati membri.

La Direttiva NIS2 prevede in particolare:

- l'ampliamento dell'ambito di applicazione a 18 settori, inclusa una porzione rilevante della Pubblica Amministrazione;
- l'individuazione dei soggetti prevalentemente con un approccio dal basso (c.d. *bottom-up*) che include, in linea generale, tutte le medie e grandi imprese riconducibili alle tipologie di soggetto individuate dalla direttiva nei citati settori;
- una revisione dei requisiti minimi di sicurezza e delle procedure di notifica degli incidenti;

- una particolare attenzione ai rischi della *supply chain* e alla *compliance* della catena degli approvvigionamenti;
- l'estensione dei poteri di supervisione, specie con l'introduzione di poteri di esecuzione e con l'allineamento dell'ammontare delle sanzioni a quanto previsto dal Regolamento GDPR;
- l'istituzione formale della rete europea di organizzazioni di collegamento per le crisi informatiche (*Cyber Crisis Liaison Organisation Network*-EU-CyCLONe);
- l'armonizzazione normativa tra Stati UE e tra normative settoriali, come quella sulla resilienza operativa digitale per il settore finanziario e quella sulla resilienza delle entità critiche;
- nuovi strumenti quali un quadro nazionale ed europeo di gestione delle crisi di sicurezza informatica su vasta scala, la divulgazione coordinata delle vulnerabilità (*Coordinated Vulnerability Disclosure*-CVD) e la mutua assistenza tra le Autorità nazionali competenti NIS degli Stati membri.



1.2.1 Il recepimento della Direttiva NIS2

Con l'entrata in vigore, il 16 ottobre 2024, del D.Lgs. n. 138/2024 (c.d. decreto NIS2), l'Italia è stata tra i primi Stati membri a completare l'iter legislativo di recepimento nei tempi previsti dall'UE, all'esito di un percorso concertato e condiviso con gli attori pubblici coinvolti nell'attuazione e con i soggetti privati impattati dalla nuova disciplina.

Il decreto NIS2 introduce rilevanti specificità nazionali rispetto al testo della direttiva, nell'ottica di promuoverne un'applicazione sostanziale ed efficace anche attraverso la conferma dell'ACN quale motore principale per l'attuazione della nuova disciplina NIS attraverso lo svolgimento delle funzioni di Autorità nazionale competente e Punto di contatto NIS, nonché di CSIRT nazionale. A tali ruoli si aggiunge quello di Autorità di gestione delle crisi informatiche su vasta scala, per la parte relativa alla resilienza nazionale e con funzioni di coordinatore, attese le attribuzioni del Ministero della difesa in qualità di Autorità di gestione delle crisi informatiche su vasta scala per gli aspetti che concernono la difesa dello Stato. Questa centralizzazione – coerente con l'indirizzo impresso dal D.L.

n. 82/2021 di riorganizzazione dell'architettura nazionale cyber e istitutivo dell'Agenzia – consente un'azione unitaria nel contesto NIS a livello nazionale ed europeo. Vengono, altresì, valorizzate le specificità settoriali e locali con l'individuazione di 9 Autorità di settore NIS, che siedono, unitamente a rappresentanti designati dalla Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano, al Tavolo per l'attuazione della disciplina NIS (c.d. Tavolo NIS, di cui si tratterà più approfonditamente nel Capitolo 3) istituito presso l'Agenzia.

Con riferimento all'ambito di applicazione, di particolare importanza è l'inclusione della PA. Novità introdotta dalla NIS2 e recepita a livello nazionale – già con l'impianto "anticipatorio" della legge n. 90/2024 – riconducendo nel contesto NIS tutta la Pubblica Amministrazione centrale, nonché le Regioni e le Province autonome, le Città metropolitane, i Comuni con popolazione superiore ai 100.000 abitanti, i Comuni capoluogo di Regione e le Aziende sanitarie locali. Questa prima elencazione potrà essere ulteriormente estesa sulla base di un criterio di gradualità, dell'evoluzione del livello di esposizione al rischio, della probabilità che si verifichino incidenti e della loro gravità, compreso il loro eventuale impatto sociale ed economico. Sono state introdotte ulteriori tipologie di soggetti, attesa la riscontrata rilevanza della sicurezza informatica del trasporto pubblico locale, della ricerca, della cultura e del settore pubblico in generale.

Inoltre, considerando la rilevanza della gestione del rischio della catena di approvvigionamento, il recepimento nazionale introduce la facoltà per le Autorità di settore di individuare ulteriori soggetti NIS tenuto conto della loro criticità quale elemento sistemico della *supply chain* di uno o più soggetti ricompresi nella disciplina. Infine, è stata prevista una clausola di salvaguardia per mitigare l'applicazione della nuova disciplina a realtà imprenditoriali laddove questa possa risultare sproporzionata.

È stato, altresì, attribuito all'ACN l'esercizio di poteri di esecuzione, come l'imposizione, tra l'altro, di audit di terze parti, nonché la possibilità di applicare strumenti deflattivi del contenzioso per rafforzare l'attività di accompagnamento dei soggetti NIS in una fase antecedente al concretizzarsi di eventuali violazioni. Queste attività, finalizzate a mitigare l'insorgenza di comportamenti incoerenti all'impianto regolatorio, assumono particolare rilevanza tenuto conto del severo regime sanzionatorio definito dalla Direttiva NIS2, che arriva a punire le violazioni più gravi fino a un massimo del 2% del fatturato (nei casi di mancata osservanza degli obblighi in materia di organi di amministrazione e direttivi, delle misure di sicurezza e di notifica di incidente, nonché di inottemperanza alle disposizioni adottate dall'Autorità nazionale competente NIS).

Framework nazionale per la cyber security e la data protection

Il Decreto NIS2 demanda a ulteriori successivi strumenti la definizione di specifici obblighi, ad esempio in materia di misure di sicurezza. A tale riguardo, l'Agenzia è attiva per delineare le citate misure. In particolare, è stata avviata una collaborazione con il centro di ricerca di Cyber Intelligence and Information Security della Sapienza Università di Roma al fine di promuovere l'aggiornamento del "Framework nazionale per la cyber security e la data protection" (FNCS), recependo anche le modifiche introdotte dalla revisione del framework statunitense (sviluppato dal National Institute of Standards and Technology-NIST) da cui deriva quello nazionale. Di fatto, anche nell'attuazione della NIS2 – in continuità con quanto fatto per la disciplina NIS1, PSNC e Regolamento cloud – l'FNCS potrà essere impiegato quale indice per le misure di sicurezza di carattere organizzativo, procedurale e tecnico che i soggetti NIS dovranno implementare.

Per meglio coordinarne il recepimento e la successiva attuazione della direttiva, l'ACN ha avviato, fin da subito, un proficuo confronto con le Amministrazioni competenti per i diversi settori di applicazione. Ha, dunque, riunito in un tavolo tecnico (che ha nei fatti anticipato il Tavolo NIS) inizialmente i rappresentanti dei 5 Ministeri già individuati quali Autorità di settore dalla precedente disciplina (dell'economia e delle finanze, delle imprese e del *made in Italy*, dell'ambiente e della sicurezza energetica, delle infrastrutture e dei trasporti e della salute), allargandolo poi progressivamente alla Presidenza del Consiglio dei ministri e ad altri 3 Ministeri (dell'agricoltura e della sovranità alimentare, dell'università e della ricerca e della cultura), coinvolti in ragione della loro competenza sui nuovi settori inclusi nella NIS2.

Nell'ottica di addivenire a un recepimento quanto più inclusivo delle diverse istanze, sono stati ingaggiati ulteriori soggetti istituzionali coinvolti nell'attuazione della nuova disciplina NIS, tra cui l'Autorità di regolazione per energia reti e ambiente (ARERA), l'Agenzia italiana del farmaco (AIFA) e la Conferenza dei Rettori delle università italiane (CRUI), oltre che le associazioni datoriali di settore e, in particolare, Confindustria.

Tale scelta è risultata di particolare efficacia non solo per assicurare un raccordo già dalle prime fasi del recepimento, ma anche per intercettare tempestivamente le tematiche di coordinamento tra la nuova disciplina NIS e quelle del *Digital Operational Resilience Act* (DORA, Regolamento (UE) 2022/2554) per il settore finanziario, e della *Critical Entities Resilience Directive* (CER, Direttiva (UE) 2022/2557), relativa alla protezione fisica delle infrastrutture critiche degli Stati membri.

Attuazione coordinata tra disciplina NIS2 e altre

Coerentemente con il ruolo di Autorità nazionale per la cybersicurezza che l'ACN riveste nell'architettura nazionale, le sono state attribuite ulteriori funzioni da diverse normative europee, primo fra tutte dalla Direttiva NIS2.

Il recepimento della Direttiva CER prevede una governance articolata, nel cui ambito l'Agenzia è designata quale Autorità di settore competente per il settore delle infrastrutture digitali in collaborazione con il Ministero delle imprese e del made in Italy, anche per le attività di valutazione del rischio e di individuazione dei soggetti critici, promuovendo un'attuazione coerente con la disciplina NIS.

L'ACN è stata designata quale Autorità competente anche per l'esecuzione dei compiti individuati dal Codice di rete relativo a disposizioni settoriali per gli aspetti di sicurezza informatica dei flussi transfrontalieri di energia elettrica (Network Code on Cybersecurity-NCCS), istituito a livello UE nel 2024.

Anche in ambito UE l'Agenzia ha continuato a svolgere un ruolo attivo nei negoziati degli atti di esecuzione della Commissione europea volti a stabilire i requisiti tecnici e metodologici in relazione alle misure di sicurezza e in materia di notifiche di incidenti significativi per specifiche tipologie di soggetti. Ha, inoltre, promosso e supportato iniziative per concertare soluzioni a possibili interpretazioni eccessivamente estensive dell'ambito di applicazione della direttiva e per assicurare la tenuta dell'impianto orizzontale stabilito dalla nuova disciplina, quale principale strumento legislativo al quale ancorare eventuali ulteriori attività normative di carattere settoriale nel dominio della sicurezza cibernetica.

1.2.2 L'attuazione della nuova disciplina NIS

La pluralità e l'eterogeneità dei soggetti NIS ha determinato l'esigenza di individuare modalità di definizione degli obblighi per assicurare un'adozione nella sostanza, oltre che nella forma della nuova disciplina, nonché l'applicabilità in contesti estremamente differenziati in termini di risorse

disponibili, maturità e consapevolezza cyber iniziale oltre che di effettiva esposizione al rischio. A tale riguardo, il decreto NIS2 introduce il principio di gradualità che complementa il principio di proporzionalità declinato nella direttiva stessa. In particolare, si prevede, in un primo momento, che i soggetti NIS adottino dei requisiti di sicurezza informatica "di base". Successivamente, tramite un'analisi del rischio, facilitata e concertata a livello settoriale, potranno essere declinati obblighi man mano crescenti, al fine di definire un percorso condiviso di progressivo rafforzamento della postura dei soggetti, sia privati che pubblici.

L'attuazione della nuova disciplina NIS si articola su tre fasi sulla base dei termini previsti per l'attività regolamentare e per l'adozione degli obblighi in capo ai soggetti (Figura 1).

Figura 1 – Fasi di attuazione della disciplina NIS2

Nella prima fase – che si caratterizza per il maggior sforzo in termini di regolamentazione – l'ACN ha, tra l'altro, disciplinato termini e modalità per la registrazione dei soggetti NIS. A tal fine, è stata creata un'apposita piattaforma, accessibile nel portale servizi dell'Agenzia, per agevolare l'assolvimento dell'obbligo di registrazione.

Con l'entrata in vigore del decreto NIS2, le Autorità di settore hanno dato formale avvio ai tavoli settoriali, convocando oltre 20 riunioni nei quali l'Agenzia e i Ministeri hanno potuto incontrare ampie rappresentanze dei soggetti NIS per avviare un confronto a partire dai primi passi attuativi, con particolare riferimento proprio alla registrazione. Rilevante sarà il ruolo di tali tavoli anche rispetto alla definizione degli obblighi di carattere tecnico.

L'Agenzia ha, inoltre, intensificato le iniziative divulgative e di sensibilizzazione, partecipando a oltre 50 seminari, corsi e *webinar*, tra cui l'evento di portata nazionale organizzato insieme a Sapienza Università di Roma il 27 novembre 2024 (vedasi Capitolo 3), oltre che incontrando numerose associazioni settoriali e diversi portatori d'interesse.

Infine, un'intensa attività di comunicazione ha caratterizzato la prima fase dell'attuazione della NIS2, tramite l'aggiornamento del sito web dell'ACN, arricchito da una sezione dedicata alla disciplina NIS2 contenente un catalogo di risposte a domande frequenti, la periodica diffusione di notizie e la produzione di video illustrativi (vedasi Capitolo 9).

1.3 ENTRATA IN VIGORE DEL NUOVO REGOLAMENTO *CLOUD*: IL RUOLO DELL'ACN PER UNA DIGITALIZZAZIONE SICURA DELLA PA

Tra le tecnologie che hanno un forte impatto sui processi di digitalizzazione e innovazione, il *cloud* ha certamente un ruolo di primo piano, non solo perché permette di ottenere un alto livello di sca-

labilità e flessibilità dei servizi IT, incrementando i livelli di sicurezza e riducendo i costi, ma anche perché costituisce un fattore abilitante per importanti tecnologie emergenti, tra cui le applicazioni di intelligenza artificiale (IA) e le reti di comunicazione di nuova generazione.

Al riguardo, in linea con l'obiettivo strategico di digitalizzazione della PA secondo il paradigma "*cloud first*" e grazie anche all'accelerazione resa possibile dai finanziamenti del Piano nazionale di ripresa e resilienza (PNRR), nel 2024 è stato impresso un notevole impulso alla migrazione dei dati e dei servizi pubblici verso soluzioni *cloud*. Ciò implica che gli stessi siano gestiti attraverso le infrastrutture di operatori terzi (cosiddetti *Cloud Service Provider*) o tramite quelle messe a disposizione dalle PA, secondo un quadro regolatorio che assicuri livelli omogenei di resilienza.

In tale ambito, il 2024 ha rappresentato un punto di svolta con l'adozione del nuovo Regolamento unico per le infrastrutture digitali e i servizi *cloud* per la PA (Decreto n. 21007 del 27 giugno 2024), adottato dall'ACN d'intesa con il Dipartimento per la trasformazione digitale (DTD) della Presidenza del Consiglio dei ministri, dopo aver acquisito il parere del Garante per la protezione dei dati personali (GPDP) e concluso la procedura di *standstill* prevista dalla normativa europea. Il Regolamento aggiorna e razionalizza in un unico quadro normativo le disposizioni previste per le infrastrutture digitali e i servizi *cloud*, al fine di incentivare il settore pubblico verso le tecnologie *cloud* secondo i migliori standard di sicurezza, resilienza, *performance* e scalabilità, nonché affidabilità, capacità elaborativa e risparmio energetico.

Come illustrato nella Figura 2, il Regolamento è frutto di un percorso di evoluzione del preesistente impianto normativo, a seguito del trasferimento delle funzioni in tema di qualifica dei servizi *cloud* per la PA dall'Agenzia per l'Italia Digitale (AgID) all'ACN.

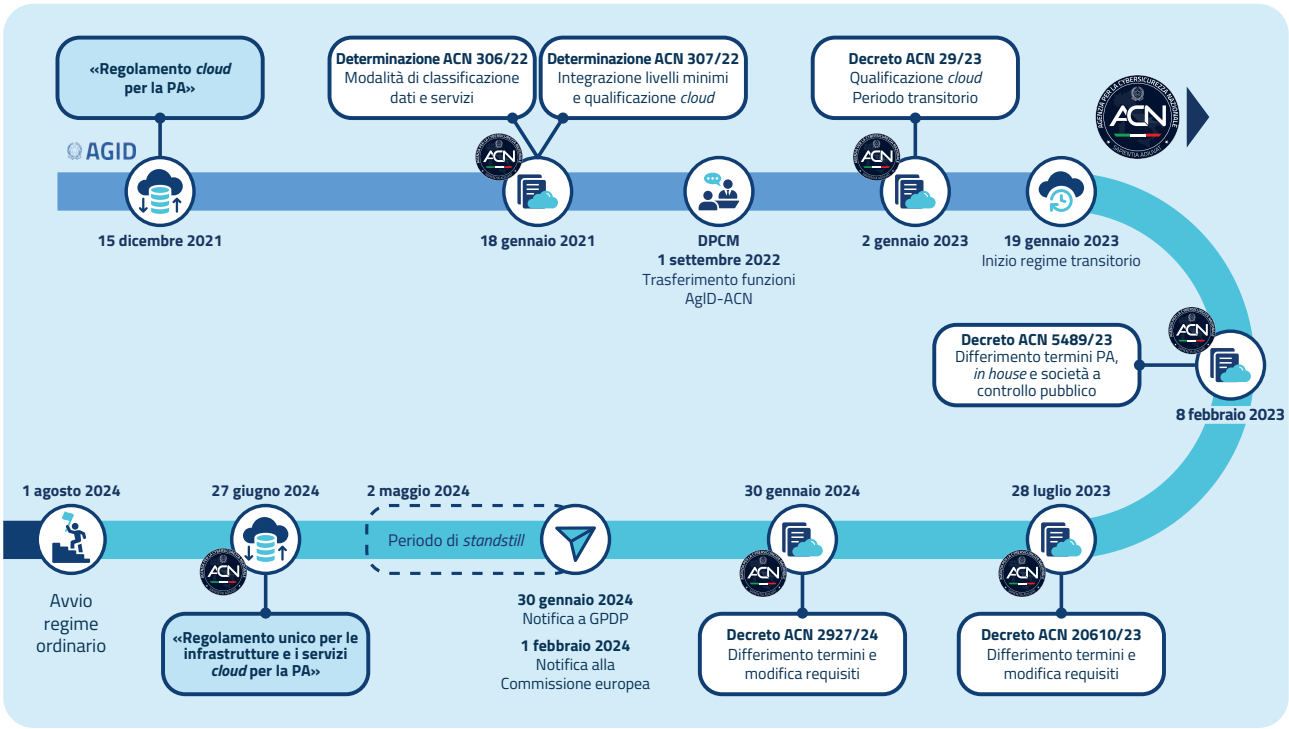


Figura 2 – Principali sviluppi sul *cloud* per la PA

Nel 2024 si è, inoltre, concluso il regime transitorio per la qualificazione dei servizi *cloud*, istituito al fine di garantire la continuità dei servizi degli operatori privati già in uso da parte delle PA e la necessaria gradualità nel passaggio al nuovo regime. In tale periodo, è stato anche definito il regime per le Amministrazioni che gestiscono *on premises* le proprie infrastrutture, che affidano dati e servizi a società *in house*, o che li affidano a società a controllo pubblico per espressa previsione normativa.

Il nuovo Regolamento è entrato in vigore il 1° agosto 2024, il giorno successivo alla conclusione del regime transitorio. Il nuovo quadro prevede:

- la conversione in forma ordinaria e permanente degli istituti di natura transitoria e temporanea previsti per la classificazione, per la qualifica e per l'adeguamento;
- la revisione del processo di adeguamento e qualifica, con livelli di sicurezza crescenti rispetto al livello di classificazione dei dati e dei sevizi digitali trattati;
- la definizione del processo di monitoraggio ex-post, necessario per la verifica del mantenimento dei requisiti nell'arco del periodo di qualifica e adeguamento (fino a 36 mesi) e del processo di revoca previsto nel caso di inadempienze, secondo un approccio graduale;
- l'armonizzazione e la revisione delle caratteristiche dei servizi *cloud* utilizzati dalla PA e dei livelli minimi previsti per le infrastrutture digitali alla base della loro erogazione, prevedendo un'applicazione differita al 1° febbraio 2025 nel caso di interventi che richiedono tempi di implementazione.

Ai sensi del Regolamento cloud tutte le Pubbliche Amministrazioni sono tenute a classificare i propri dati e servizi digitali in strategici, critici e ordinari.

Attraverso il processo di adeguamento e qualificazione, l'ACN valuta la conformità di infrastrutture digitali e servizi cloud offerti da operatori privati, dei quali le PA si possono avvalere. Qualora queste volessero, invece, utilizzare le proprie infrastrutture e servizi cloud, sono tenute all'adeguamento.

Qualificazione e adeguamento sono volti a garantire il rispetto delle caratteristiche dei servizi cloud e dei livelli minimi delle infrastrutture digitali, a beneficio delle PA e dei cittadini.

In ragione dell'impatto connesso all'applicazione del nuovo Regolamento, la sua pubblicazione è stata supportata da un importante sforzo di condivisione e comunicazione, consentendo di divul-

gare le principali novità e contribuire a indirizzare gli sforzi di adeguamento da parte delle Amministrazioni e dei fornitori coinvolti.

L'intero impianto del nuovo Regolamento *cloud* è stato anche presentato a livello UE, sia alla Commissione europea che a omologhe agenzie cyber. Ciò anche in ragione del suo inserimento nella bozza di schema di certificazione europeo previsto dal *Cybersecurity Act* (CSA) per armonizzare la regolazione della tecnologia *cloud* tra i Paesi membri, un processo che presenta profili di particolare delicatezza, dovendo contemperare le esigenze di un mercato caratterizzato da forti investimenti nel settore. In particolare, il Regolamento è stato riconosciuto, insieme a quelli di Francia, Germania e Paesi Bassi, tra i pochi schemi nazionali esistenti che godranno di una fase di transizione in vista dell'adozione di quello UE. Lo schema nazionale rappresenta un esempio virtuoso per bilanciare le misure di controllo rispetto alla sensibilità dei dati trattati, attraverso il processo di classificazione, evitando così di avere impatti in forma indistinta e garantendo un adeguato livello di innovazione, in un quadro di resilienza ben definito.

1.4 L'IMPULSO DELL'UNIONE EUROPEA ALLA NORMATIVA CYBER: APPROVAZIONE DEL *CYBER RESILIENCE ACT*, DEL REGOLAMENTO EIDAS2 E DELL'*AI ACT*

Un importante impulso alla regolamentazione con significativi risvolti in ambito cyber si è registrato a livello di Unione europea, con la conclusione dei negoziati su diversi importanti testi normativi:

- emendamenti al citato *Cybersecurity Act* per quanto riguarda i servizi di sicurezza gestiti;
- *Cyber Solidarity Act* (CSoA), che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevare e rispondere a minacce e incidenti informatici;
- *Cyber Resilience Act* (CRA), contenente requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali;
- Regolamento eIDAS2 (*electronic IDentification, Authentication and trust Services*), per la creazione del portafoglio europeo di identità digitale;
- Regolamento sull'intelligenza artificiale (*Artificial Intelligence Act* o *AI Act*), che stabilisce regole armonizzate sull'IA.

Cyber Solidarity Act

Il CSoA prevede, tra le altre cose, l'istituzione di:

- *una rete paneuropea di poli informatici nazionali e transfrontalieri per migliorare le capacità di rilevamento e analisi delle minacce cyber e di prevenzione degli incidenti;*
- *un meccanismo per le emergenze cyber, volto a sostenere gli Stati membri nell'affrontare gli incidenti cyber nelle fasi di preparazione, risposta, mitigazione e recovery, attraverso una riserva dell'UE per la cybersicurezza, da realizzare gradualmente, grazie alla collaborazione di determinati operatori privati.*

Il Cyber Solidarity Act integra le disposizioni della Direttiva NIS2 in materia di risposta agli incidenti e alle crisi cyber con impatto significativo o su vasta scala creando un quadro di risposta operativo a livello UE.

EUCC E ALTRI SISTEMI DI CERTIFICAZIONE

Il 31 gennaio 2024 è stato adottato EUCC, il primo sistema di certificazione europeo discendente dal *Cybersecurity Act*, in vigore dal 27 febbraio 2025. Il nuovo sistema è basato sullo standard internazionale *Common Criteria* (ISO 15408) e sostituisce gli schemi nazionali esistenti che si basano sullo stesso modello. Tra questi, anche lo schema italiano, adottato con DPCM 30 ottobre 2003, cessa di produrre effetti, ferma restando la possibilità di completare, entro il 26 febbraio 2026, i processi di certificazione in corso.

Nel 2024 l'ACN ha avviato l'adeguamento delle proprie procedure in conformità alle nuove regole armonizzate stabilite dall'EUCC, per poter operare dal 2025 nel duplice ruolo di Autorità nazionale di certificazione della cybersicurezza e Organismo di certificazione della sicurezza informatica. In tal senso, nel 2024 l'ACN ha tenuto incontri con gli altri portatori di interesse del settore, tra cui Accredia, l'ente nazionale di accreditamento, e i Laboratori di valutazione della sicurezza che, in prospettiva, potranno accreditarsi come organismi di valutazione della conformità.

Seguendo lo stesso iter del sistema EUCC, la Commissione europea adotterà sistemi europei di certificazione della cybersicurezza per ambiti specifici. Questi avranno effetto diretto sugli ordinamenti nazionali, disponendo regole armonizzate per l'emissione e la gestione dei certificati di cybersicurezza, i quali attesteranno la resistenza dei prodotti, dei servizi e dei processi ICT (*Information and Communication Technology*) agli attacchi e alle minacce informatiche. In particolare, nel 2024, sono proseguiti i lavori per l'elaborazione dei sistemi di certificazione per gli ambiti di maggiore rilevanza per promuovere la digitalizzazione in Europa vale a dire i servizi *cloud* (EUCS) e le reti 5G (EU5G).

Cyber Resilience Act

Il *CRA* (Regolamento (UE) 2024/2847), entrato in vigore il 10 dicembre 2024, mira ad armonizzare a livello UE i requisiti essenziali di cybersicurezza per i prodotti con elementi digitali immessi nel mercato unico, eliminando la preesistente frammentazione del panorama regolamentare di tipo settoriale. Allo stesso tempo, il CRA intende preservare la cybersicurezza di tali prodotti durante l'intero ciclo di vita, richiedendo ai produttori adeguate modalità di gestione delle vulnerabilità che dovessero eventualmente emergere.

Il Regolamento – che diverrà applicabile dall'11 dicembre 2027 – include tutti i "prodotti con elementi digitali connettibili", compresi i software *open source* resi disponibili sul mercato per la distribuzione o l'uso nel corso di un'attività commerciale. Un nuovo prodotto, per poter essere immesso nel mercato UE, dovrà ottenere e riportare la marcatura CE; a tal fine, il fabbricante dovrà dimostrare la conformità del prodotto a specifici requisiti di sicurezza.

Gli intensi negoziati hanno consentito al nostro Paese di conseguire alcuni importanti risultati, anche grazie ai contributi forniti dall'ACN. Tra questi rilevano, in particolare, l'allineamento ai termini previsti dalla Direttiva NIS2 per la notifica di incidenti cyber significativi e di vulnerabilità attivamente sfruttate, nonché la riduzione del numero delle categorie di prodotti con componenti digitali che rientrano nell'ambito di applicazione del Regolamento, sulla base di un approccio improntato alla gradualità, così da non gravare di oneri eccessivi specie i produttori.

In vista dell'entrata in vigore del CRA, l'Agenzia ha provveduto a coinvolgere gli operatori privati interessati in una serie di consultazioni informali con l'obiettivo di acquisire elementi utili per la redazione dei relativi atti implementativi. L'ACN ha, inoltre, designato propri esperti, nell'ambito di un dedicato gruppo di lavoro, con il compito di assistere la Commissione nella predisposizione di *policy*, atti delegati, atti di esecuzione e documenti di indirizzo, per facilitare l'attuazione del CRA, nonché agevolare la cooperazione tra Commissione, Stati membri e parti interessate.

eIDAS2

Nel corso del 2024 si sono concluse le attività normative volte alla creazione del portafoglio europeo di identità digitale (*European Digital Identity Wallet*-EUDI Wallet), uno strumento che mette l'identità digitale del cittadino sotto il suo controllo esclusivo. In particolare, il 20 maggio 2024 è entrato in vigore il Regolamento (UE) 2024/1183, noto come eIDAS2, che emenda il precedente Regolamento eIDAS (Regolamento (UE) 2014/910) e istituisce il citato EUDI Wallet. Entro la seconda metà del 2026 ciascuno Stato membro dovrà dotarsi di una soluzione EUDI Wallet nazionale, in conformità con i requisiti UE, e ogni versione del portafoglio dovrà essere interoperabile oltre che funzionare ovunque nell'Unione europea.

Durante le fasi precedenti all'entrata in vigore di eIDAS2, l'ACN ha contribuito, in coordinamento con il DTD e l'AgID, alla revisione di alcuni degli atti di esecuzione della Commissione europea in attuazione del citato Regolamento. Ha, inoltre, partecipato al gruppo di lavoro della Commissione dedicato alla certificazione di sicurezza dell'EUDI Wallet. In particolare, i principali aspetti di sicurezza riguardano la certificazione obbligatoria secondo uno schema nazionale che dovrà essere conforme ai requisiti di sicurezza europei e certificare un livello di garanzia "elevato", oltre a dimostrare la conformità della soluzione al GDPR per il trattamento dei dati personali.

Artificial Intelligence Act

In relazione all'*AI Act* (Regolamento (UE) 2024/1689), l'Agenzia ha seguito, per quel che concerne gli aspetti di cybersicurezza, i negoziati che hanno condotto alla sua entrata in vigore ad agosto. L'obiettivo dell'*AI Act* è proteggere i diritti fondamentali, la democrazia, lo Stato di diritto e la sostenibilità ambientale dai sistemi di IA, specialmente quelli ad alto rischio, favorendo allo stesso tempo l'innovazione e assicurando all'Unione un ruolo guida nel settore. Il Regolamento intende promuovere lo sviluppo e l'adozione di un'IA sicura e affidabile nell'intero mercato unico dell'UE e rappresenta un passo importante nella definizione degli standard globali per l'uso responsabile dell'IA.

L'*AI Act* si fonda sulla classificazione dei sistemi di IA a seconda del rischio che comportano per le persone e la società. Sulla base di tale approccio le regole diventa-

La definizione di intelligenza artificiale nell'AI Act

Art. 3: "sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".

no più stringenti in relazione al potenziale danno alla società, applicando misure più severe per i sistemi ad alto rischio. Vi sono, infine dei sistemi che, in ragione del livello inaccettabile di rischio, sono vietati, come ad esempio quelli per il riconoscimento delle emozioni in contesti scolastici o lavorativi, quelli volti a prevedere la probabilità che un individuo commetta un reato o quelli per il *social scoring*.

Il Regolamento prevede anche l'istituzione di un Comitato europeo per l'IA (*AI Board*), con compiti di consulenza e supporto alla Commissione europea al fine favorire l'attuazione delle sue previsioni. Per l'Italia sono stati designati quali rappresentanti il Direttore generale dell'ACN unitamente a quello d'AgID. Alla riunione inaugurale, il 20 settembre, sono state concordate, tra le altre cose, l'organizzazione delle attività del Comitato e dei suoi 12 sotto-gruppi. Di questi, 6 hanno avviato i propri lavori a fine 2024, mentre i restanti 6 diverranno operativi nel corso del 2025 (Figura 3). L'ACN assicura la partecipazione ai sotto-gruppi relativi a ecosistema dell'innovazione, *sandbox* per l'IA, proibizioni, standard e IA per scopi generali.

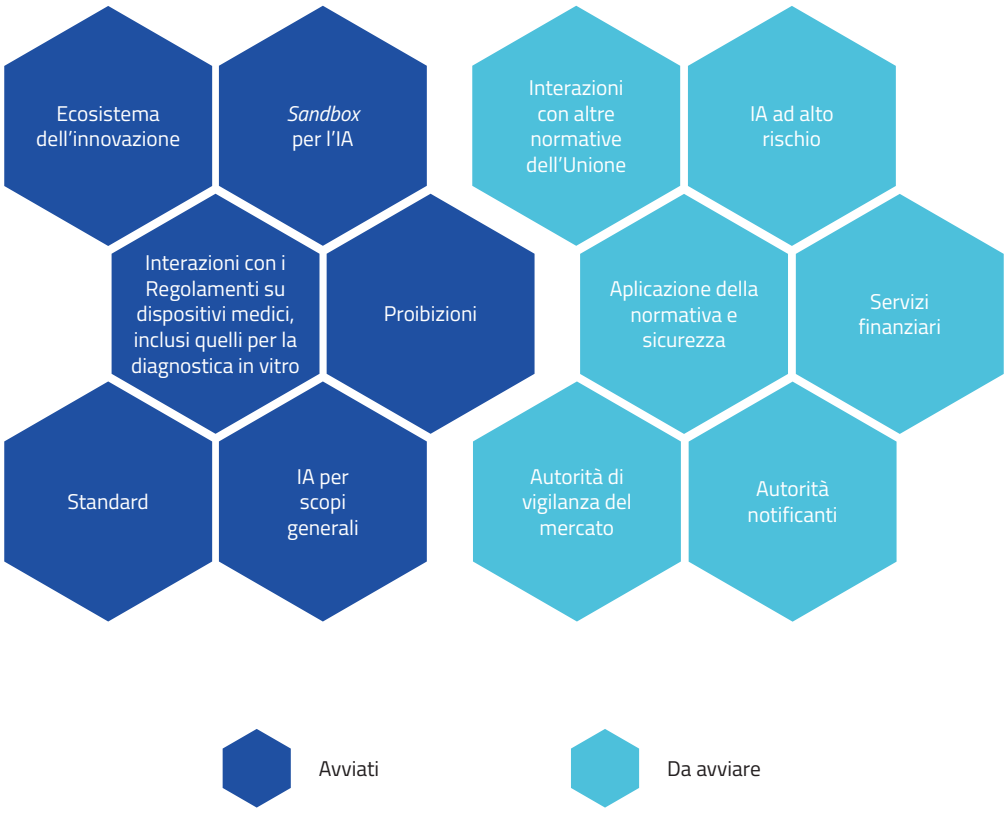


Figura 3 – I 12 sotto-gruppi dell'*AI Board*

L'Agenzia ha messo a disposizione la propria *expertise* per contribuire a definire, sia sul piano tecnico che regolamentare, come rendere pienamente operativo l'*AI Act*. A tale riguardo, ha potuto beneficiare del significativo lavoro preparatorio che era stato compiuto in diversi formati per meglio comprendere le minacce derivanti dai modelli di intelligenza artificiale e i relativi controlli di

sicurezza da adottare. Ne sono un esempio i progressi fatti a livello UE in materia di definizione di schemi di certificazione di cybersicurezza per sistemi di IA e le interlocuzioni internazionali per giungere a uno standard in materia.

Al fine di accompagnare gli Stati nell'attuazione dell'*AI Act*, si è attivato anche il mondo della ricerca, con il sostegno di consistenti finanziamenti europei tramite progetti che vedono la partecipazione di diversi attori istituzionali, inclusa l'Agenzia. Particolare rilievo ha, infatti, la cosiddetta fabbrica di IA "*IT4LIA AI-Factory*", per la creazione di un supercalcolatore ottimizzato per l'intelligenza artificiale, che verrà messo a disposizione di operatori industriali e della ricerca (vedasi Capitolo 5). A ciò si aggiunge il progetto EUSAiR, aggiudicato nel 2024, che riguarda la predisposizione, a livello nazionale, di spazi di sperimentazione normativa (c.d. *regulatory sandboxes*), creando ambienti controllati per testare i sistemi di IA prima della loro immissione nel mercato. EUSAiR, che sarà avviato nel 2025 e disporrà di un budget di circa 2 milioni di euro, finanziato interamente dalla Commissione europea, include primari partner ed enti affiliati di tutta Europa, tra università, centri per il supercalcolo, PMI e organizzazioni specializzate in IA e in comunicazione. Il progetto permetterà di sviluppare i richiamati strumenti previsti dall'*AI Act*, nonché di promuovere sinergie con l'EuroHPC (Impresa comune europea per il calcolo ad alte prestazioni) e iniziative analoghe per test ed esperimenti nel campo dell'IA.

Anche sul piano nazionale il 2024 ha registrato importanti passi avanti sulla regolazione dell'IA, con la presentazione da parte del Governo del Disegno di legge sull'intelligenza artificiale. In linea di continuità con l'approccio europeo, anche la proposta al vaglio del Parlamento intende prevedere norme di principio e disposizioni di settore per promuovere l'utilizzo dell'IA e fornire soluzioni per la gestione dei rischi connessi. Il testo proposto individua l'AgID e l'ACN come Autorità nazionali per l'intelligenza artificiale, affidando all'ACN compiti di vigilanza a tutela della cybersicurezza, nonché di promozione e sviluppo dell'IA sempre relativamente ai profili di sicurezza cibernetica.

2.

LA MINACCIA CYBER IN EVOLUZIONE: PREVENZIONE E GESTIONE DI EVENTI E INCIDENTI CIBERNETICI

L'Agenzia per la cybersicurezza nazionale ha fatto fronte, nel 2024, a una minaccia cyber che continua ad aumentare sia dal punto di vista quantitativo che qualitativo, con possibili conseguenze importanti per le vittime e per il sistema Paese nel suo complesso. Anche quest'anno l'Italia ha continuato a essere oggetto di un'intensa attività DDoS (*Distributed Denial of Service*), ma anche di attacchi di tipo *ransomware* e di attività malevole ad opera di *Advanced Persistent Threat* (APT). Complessivamente, la minaccia ha interessato una vasta gamma di soggetti pubblici e privati operanti in numerosi settori, anche critici.

L'Agenzia può contare su un'ampia visibilità sull'effettiva minaccia cibernetica ai danni dell'Italia grazie alla propria articolazione tecnico-operativa, il CSIRT Italia, che è *hub* nazionale delle notifiche obbligatorie e volontarie di incidenti cibernetici previste dalla normativa cyber vigente. Le attività preventive e reattive portate avanti dall'ACN hanno permesso di limitare e mitigare gli effetti di eventi e incidenti cyber, mentre l'allertamento fornito nei confronti di soggetti potenzialmente vulnerabili ha contribuito ad arginare il rischio.

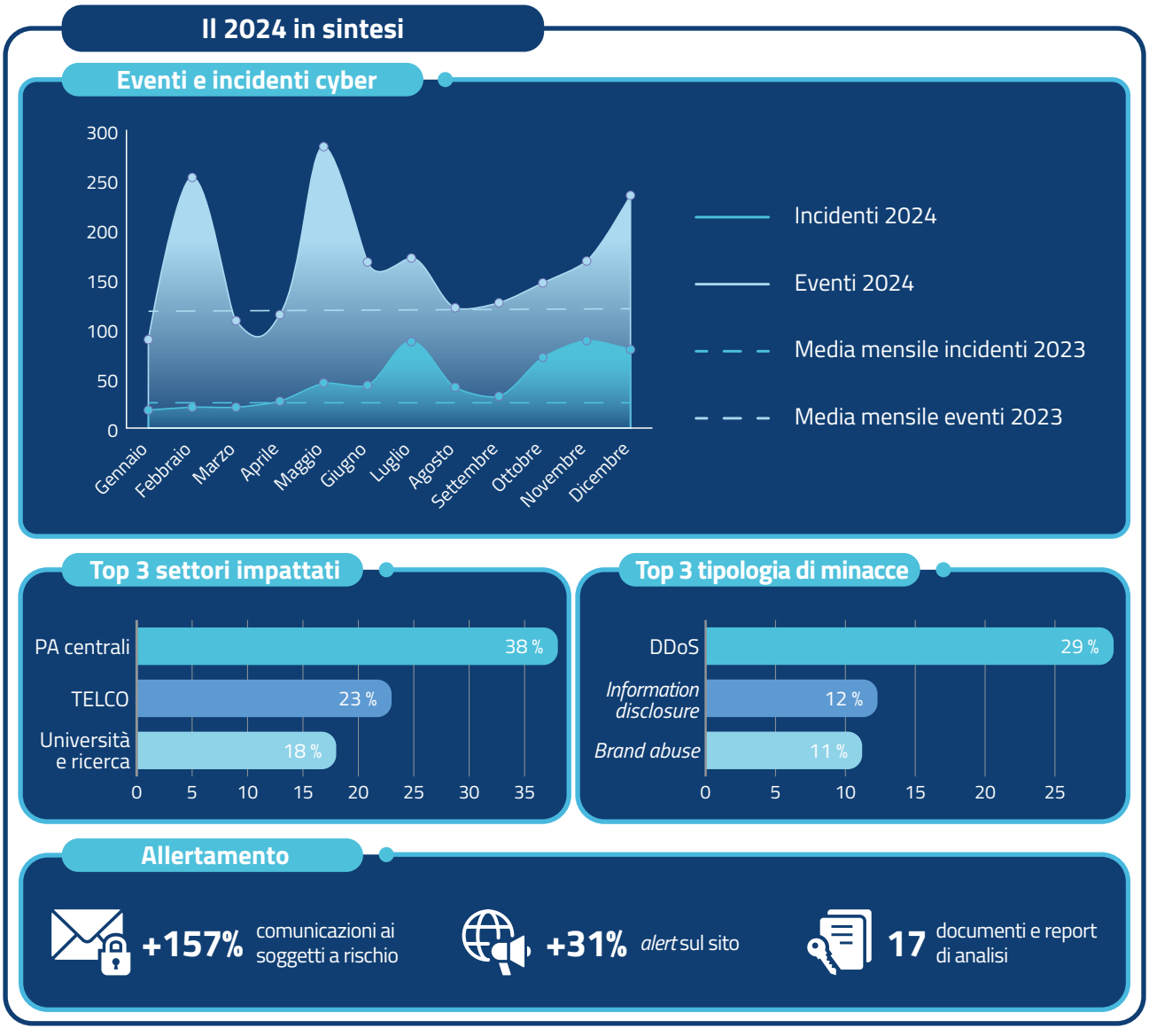


Figura 1 – Il 2024 in sintesi

2.1 I NUMERI DEL CSIRT ITALIA

Tutte le attività operative dell'Agenzia hanno subito nel 2024 un notevole incremento rispetto all'anno precedente, indice di un generale aumento della minaccia cyber, rilevato anche a livello europeo e globale. Come dimostrano i numeri delle principali attività svolte dal CSIRT Italia (riassunti nel box), l'Agenzia è stata particolarmente impegnata sia nella fase preventiva di monitoraggio, analisi delle minacce e allertamento dei soggetti esposti ai rischi, sia nella fase reattiva di risposta agli incidenti (Figura 2).

Attività e numeri del CSIRT Italia 2024

Gestione eventi

- **1.979 eventi cyber** gestiti (165 al mese)
- **573 incidenti** con impatto confermato (48 al mese)
- **2.734 vittime,** di cui univoche 1.260
- **40 interventi** a supporto delle vittime

Allertamento

- **53.470 comunicazioni** inviate ai soggetti (4.456 al mese)
- **587 *alert* e bollettini** pubblicati sul **portale pubblico**
- **64 *alert* e bollettini** pubblicati sul **portale servizi**
- **629 stime di impatto** di nuove vulnerabilità
- **6 segnalazioni** puntuali di vulnerabilità **ex legge n. 90/2024**
- **+125.000 indicatori di compromissione** condivisi

Monitoraggio sistemi italiani

- **11.290 dispositivi e servizi** a rischio segnalati ai soggetti
- **722 tentativi di *phishing* segnalati** alle vittime

Monitoraggio attori cyber

- **91 attori *ransomware*** monitorati
- **77 attori hacktivisti** monitorati

Analisi minacce

- **41** campagne **APT**
- **180 malware** analizzati
- **30 report specialistici**

Documenti e report di analisi

- **12 *Operational Summary*** sullo stato della minaccia in Italia
- **1 report di analisi** sullo stato della minaccia cibernetica nel settore sanitario
- **1 report di analisi** sullo stato della minaccia *ransomware*
- **1** documento operativo per la **notifica degli incidenti**
- **1** documento operativo sulla **tassonomia** cyber
- **1** documento operativo **sulla *constituency* del CSIRT Italia**

Gestione eventi	2023	2024	variazione %
Notifiche	349	**450**	**+28,9%**
Comunicazioni ricevute	5.444	**9.827**	**+80,5%**
Case	2.684	**2.963**	**+10,4%**
Eventi cyber	1.411	**1.979**	**+40,3%**
Incidenti	303	**573**	**+89,1%**
Vittime univoche	566	**1.260**	**+122,6%**

Allertamento	2023	2024	variazione %
Comunicazioni inviate	20.825	**53.470**	**+156,8%**
Alert e bollettini portale pubblico	447	**587**	**+31,3%**
Richieste di informazioni	205	**310**	**+51,2%**

FIgura 2 – Dati 2023 e 2024 a confronto

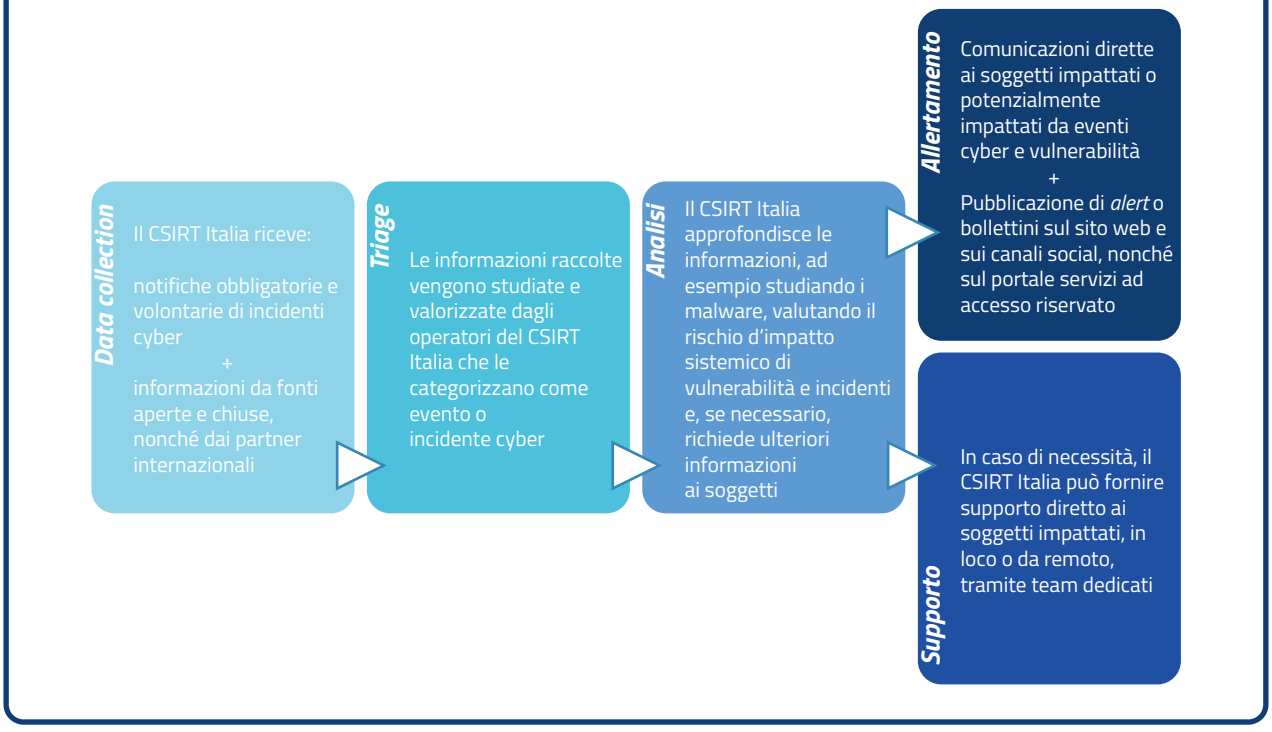
In generale, il 2024 è stato caratterizzato da un aumento in termini quantitativi degli indicatori presi a riferimento per fotografare lo stato di esposizione del Paese alle minacce cibernetiche. Tra questi emerge un sensibile incremento delle notifiche indirizzate all'Agenzia, dovuto in parte alla legge n. 90/2024, entrata in vigore a luglio, che ha imposto obblighi di notifica d'incidente per ulteriori soggetti, ampliando in sostanza il novero di soggetti vigilati dall'Agenzia.

È stato registrato, inoltre, un notevole incremento sia degli eventi cyber (+40% rispetto al 2023), sia degli incidenti (quasi raddoppiati), un incremento dovuto principalmente all'intensificarsi delle campagne di attacchi DDoS condotte nei confronti di soggetti nazionali, ma anche all'aumento degli eventi di tipo *information disclosure*, ovvero l'esposizione non autorizzata di informazioni sensibili precedentemente esfiltrate a seguito di attività malevole, e al crescente numero di campagne di *spearphishing* rilevate.

Nel 2024, le vittime di eventi cibernetici individuate dal CSIRT Italia sono state 2.734. Tenuto conto della reiterazione degli attacchi nei confronti di alcune di esse, le "vittime univoche" corrispondono 1.260 soggetti. Tale dato segna un incremento rispetto all'anno precedente, con un numero di vittime univoche più che raddoppiato.

Di particolare rilevanza è anche l'attività messa in campo dall'ACN per prevenire l'insorgere o l'allargarsi di incidenti cyber tramite un'opera di diffusione della conoscenza in merito a eventi e vulnerabilità. Ha segnato, infatti, un netto aumento l'allertamento svolto dall'Agenzia, sia tramite comunicazioni dirette (oltre 53.000), inviate per segnalare potenziali compromissioni o fattori di rischio ai soggetti monitorati, che mediante i canali di diffusione pubblica (portale pubblico e portale servizi).

La metodologia del CSIRT Italia



DEFINIZIONI

Notifica: comunicazione prevista per legge per i soggetti appartenenti al Perimetro di sicurezza nazionale cibernetica, per gli operatori di servizi essenziali e fornitori di servizi digitali (Direttiva NIS), per gli operatori del settore delle telecomunicazioni (Decreto del Ministro dello sviluppo economico del 12 dicembre 2018, c.d. Decreto TELCO) e per i soggetti inclusi nelle previsioni della legge n. 90/2024.

Comunicazione ricevuta: e-mail ricevuta dal CSIRT Italia relativa a informazioni contenenti profili di natura cyber anche generiche, sottoposte a valutazione preliminare per determinare l'apertura o meno di un case.

***Asset* a rischio:** dispositivi o servizi esposti su Internet rilevati dalle attività di monitoraggio proattivo e per i quali vengono inviate specifiche comunicazioni.

***Triage*:** fase in cui gli operatori analizzano le segnalazioni, le comunicazioni ricevute e ogni possibile evento cyber di cui il CSIRT Italia viene 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.

***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.

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.

Impatto: perturbazione causata da un evento cyber.

Incidente cyber: un evento cyber con impatto confermato dalla vittima o dal CSIRT Italia.

Indicatore di compromissione: marcatore digitale che indica la possibile presenza di un'attività malevola o un'intrusione nel sistema informatico. Gli indicatori di compromissione (*Indicators of Compromise*-IOC) sono prove che gli analisti di sicurezza informatica utilizzano per identificare, rilevare e rispondere a una compromissione.

Richieste di informazioni: richieste effettuate 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).

Comunicazione inviata: *alert*, anche massivi, inviati a Pubbliche Amministrazioni e soggetti privati potenzialmente interessati da eventi cyber.

***Constituency*:** insieme dei soggetti ai quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli eventi e incidenti cyber.

Portale servizi: 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.

Guida alla notifica degli incidenti al CSIRT Italia

Nel 2024 è stata pubblicata la "Guida alla notifica degli incidenti al CSIRT Italia". La corretta adozione della procedura di notifica degli incidenti cibernetici costituisce, infatti, un elemento cruciale per garantire sicurezza e resilienza delle reti, dei sistemi informativi e dei servizi informatici.

La prontezza e la precisione delle informazioni fornite durante il processo di notifica rivestono un ruolo fondamentale per consentire al CSIRT Italia di acquisire rapidamente una conoscenza completa ed esaustiva dell'incidente ai fini dell'attività di allertamento e per fornire ai soggetti impattati il supporto necessario per il ripristino dei servizi stessi.

La Guida rappresenta un compendio delle istruzioni per i diversi soggetti, pubblici e privati, tenuti per legge alla notifica degli incidenti: soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica, quelli operanti in ambito NIS e TELCO, nonché quelli previsti dalla legge n. 90/2024.

La Guida si rivolge anche ai soggetti pubblici e privati che, pur non essendo obbligati alla notifica, intendono segnalare volontariamente l'incidente al CSIRT Italia, contribuendo così a una migliore condivisione della conoscenza del livello e dell'intensità della minaccia, per rafforzare la resilienza dell'ecosistema digitale italiano.

La tassonomia cyber dell'ACN

Dal 1° gennaio 2024 l'Agenzia ha definito una propria tassonomia cyber al fine di agevolare lo scambio di informazioni a livello nazionale attraverso l'adozione di un lessico comune. Ciò rappresenta una base metodologica uniforme, utile sia per la condivisione di informazioni riguardo agli eventi cyber, sia per la notifica degli incidenti al CSIRT Italia, nonché per potenziare le attività di reportistica e rendicontazione.

La tassonomia consente di identificare, definire e caratterizzare gli eventi cyber tramite un'unica metodologia rilevante a livello nazionale, fornendo un documento che si armonizzi con le tassonomie internazionali in materia di cybersicurezza e che sia al contempo adeguato al contesto normativo di riferimento.

2.2 ANALISI DEGLI EVENTI

Durante il corso del 2024 il CSIRT Italia ha trattato un totale di 1.979 eventi cyber, con una media di circa 165 al mese e con un picco massimo di 283 a maggio. Sul totale degli eventi, 573 sono stati classificati come incidenti, con una media di circa 48 al mese (Figura 3). Rileva segnalare non solo che gli eventi sono aumentati del 40% e gli incidenti quasi del 90% rispetto al 2023, ma che la proporzione di eventi confermati come incidenti è passata da circa 1/5 a quasi 1/3. Tali incrementi, oltre che al già richiamato aumento delle notifiche obbligatorie, sono riconducibili a una serie di fattori, tra cui l'allargamento esponenziale della superficie digitale che, con il crescere della digitalizzazione di processi e servizi e dell'impiego di dispositivi connessi, include una quantità sempre maggiore di *asset*. A ciò si aggiunge spesso l'obsolescenza dei sistemi, nonché la mancanza di personale sufficientemente formato in particolare per la gestione della cybersicurezza.

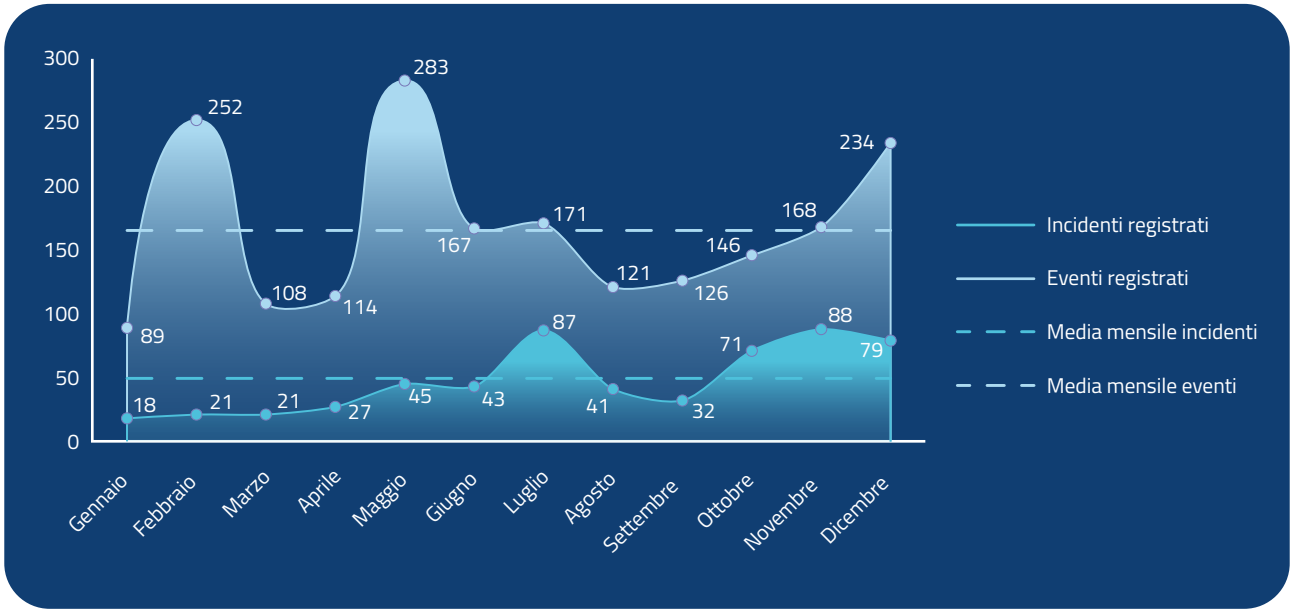
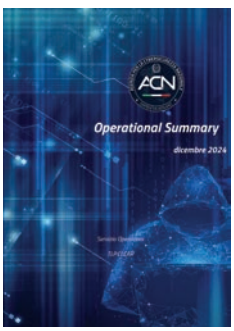


Figura 3 – Distribuzione temporale degli eventi e incidenti cyber nel 2024

I picchi di febbraio, maggio e dicembre sono stati determinati da tre campagne di attacchi DDoS rivendicate da un noto gruppo hacktivista filorusso – NoName057(16) – che, dal 2022, conduce attacchi contro numerosi Paesi occidentali, nel contesto del conflitto russo-ucraino. Un attacco di tipo *supply chain* registrato a luglio 2024 ha, invece, causato un notevole incremento nel numero di eventi registrati nel mese, in quanto la compromissione di un fornitore IT ha avuto effetti su numerosi altri soggetti a cui questo erogava servizi.

La crescente esposizione delle infrastrutture digitali a minacce cyber rende necessaria un'analisi strutturata degli impatti, distinguendo tra sistemi, account e applicazioni, che sono soggetti a compromissione, e dati, per i quali la valutazione si concentra su riservatezza, integrità e disponibilità. Tale categorizzazione consente di comprendere più distintamente la perturbazione causata da un evento cyber, nonché di adottare misure di mitigazione mirate, rafforzando la postura di sicurezza dei soggetti interessati e migliorando la capacità di risposta agli attacchi.

Operational Summary



A partire da maggio 2023, l'ACN ha avviato la redazione dell'Operational Summary, un documento mensile che riporta i numeri relativi alle principali fenomenologie cyber gestite e censite dal CSIRT Italia. Le informazioni di carattere operativo, provenienti dalle attività condotte dall'ACN, forniscono dati e indicatori sull'analisi e l'andamento della minaccia cyber, con focus sui principali settori impattati e le tipologie di minacce più frequenti.

Il documento è redatto in tre versioni: una a uso interno ACN, una a diffusione limitata, trasmessa alla constituency del CSIRT Italia e, a partire da maggio 2024, una versione pubblica scaricabile dal sito web dell'ACN. Il documento è tradotto anche in inglese per la condivisione con i partner internazionali.

FOCUS SUGLI IMPATTI

I **sistemi** rappresentano l'insieme di risorse informatiche interconnesse (hardware, software e reti), attraverso cui vengono elaborate, archiviate e trasmesse informazioni. La loro compromissione può inficiare la continuità operativa e la sicurezza delle informazioni trattate.

Gli **account** regolano l'accesso alle risorse mediante meccanismi di autenticazione e autorizzazione, definendo i privilegi degli utenti nei sistemi informatici. Un account compromesso può consentire accessi non autorizzati e agevolare movimenti laterali all'interno della rete.

Le **applicazioni** sono programmi software progettati per eseguire funzioni specifiche. La loro compromissione può consentire agli attaccanti di eseguire codice malevolo, manipolare i dati o ottenere accesso privilegiato ai sistemi sottostanti.

I **dati** rappresentano informazioni codificate in formato digitale, che possono essere generate, raccolte, elaborate, archiviate o trasmesse. A differenza degli altri elementi, non si parla di compromissione diretta, ma di impatti sulla riservatezza, integrità e disponibilità, con conseguenze potenzialmente critiche sulla protezione delle informazioni e sulla continuità operativa.

In quest'ottica, gli impatti derivanti da eventi cyber (Figura 4), hanno riguardato prevalentemente la riservatezza e integrità dei dati (35%). Si tratta di esfiltrazioni di informazioni, diffusione indebita di dati, accessi non autorizzati e modifica di parametri e altre informazioni tecniche, attività queste condotte dagli attaccanti per garantirsi persistenza nei sistemi attaccati oppure per riuscire a compromettere ulteriori sistemi. In altri casi (26%), sono state rilevate operazioni volte a

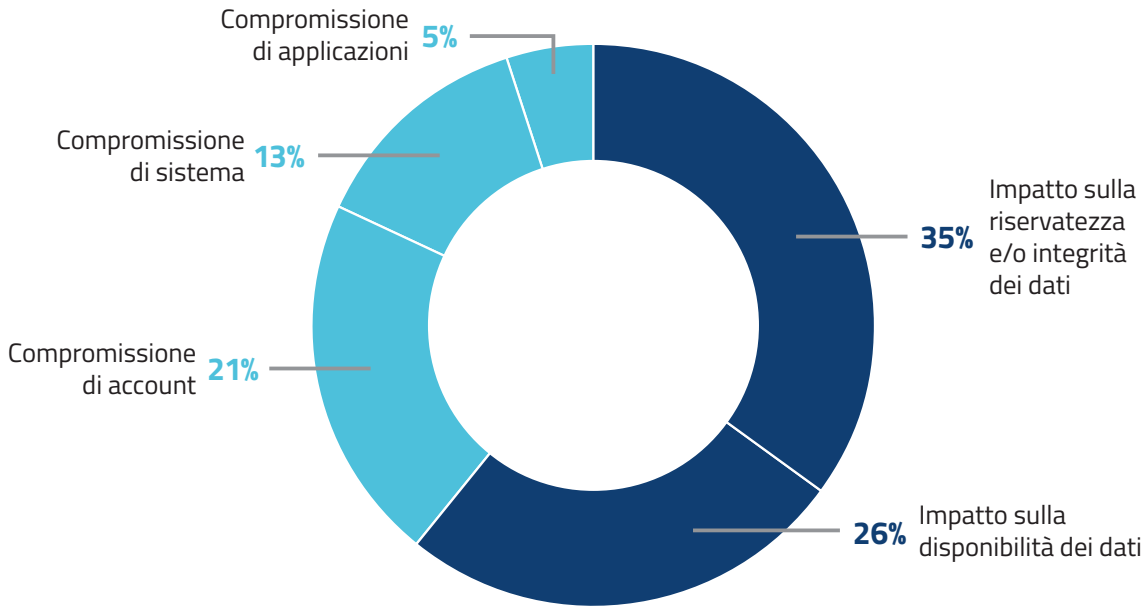


Figura 4 – Impatti rilevati negli eventi cyber

rendere i dati non disponibili, come la cifratura che caratterizza gli attacchi *ransomware*, la cancellazione indebita delle informazioni oppure, come negli attacchi DDoS, il blocco dell'accesso a siti web e altre risorse esposte su Internet (su entrambi si rimanda alle apposite sezioni). Gli altri impatti hanno riguardato la compromissione di sistemi, account o applicazioni.

Affinché un attore ostile possa compromettere sistemi, account o applicazioni è necessario che riesca a ottenere l'accesso all'interno di una rete o di un sistema informatico. Per raggiungere tale obiettivo vengono sfruttati specifici vettori di attacco che consentono all'attaccante di eludere le misure di sicurezza ed esercitare un controllo non autorizzato sulla rete o sul sistema informatico. Tali vettori possono essere impiegati non solo per ottenere un accesso iniziale, ma anche per consolidare la presenza all'interno dell'ambiente compromesso o per evitare il rilevamento.

PRINCIPALI VETTORI DI ATTACCO

I vettori di attacco rappresentano le modalità mediante le quali una minaccia si concretizza attraverso lo sfruttamento o l'utilizzo indebito di uno degli elementi di seguito descritti.

E-mail: impiego di comunicazioni fraudolente per indurre l'utente a divulgare credenziali, eseguire codice malevolo o fornire informazioni sensibili.

Sfruttamento di vulnerabilità: esecuzione di codice arbitrario attraverso falle di sicurezza presenti in sistemi operativi, applicazioni o dispositivi di rete, con l'obiettivo di ottenere privilegi elevati, eseguire operazioni non autorizzate o interrompere la disponibilità dei servizi.

Account validi: sfruttamento di credenziali compromesse, ottenute tramite esfiltrazione di dati, attacchi di forza bruta o *phishing*, per accedere ai sistemi con identità legittime, riducendo le probabilità di rilevamento e favorendo il movimento laterale.

Supply chain: attacco ai fornitori di software, hardware o servizi IT per introdurre elementi malevoli prima della distribuzione o durante gli aggiornamenti, in modo da compromettere le infrastrutture digitali su vasta scala.

Servizi remoti esposti: sfruttamento di configurazioni non sicure o mancata protezione di protocolli di accesso remoto, che consentono agli attaccanti di ottenere un accesso diretto ai sistemi informatici.

Social media: diffusione di contenuti ingannevoli per raccogliere informazioni sensibili o agevolare ulteriori fasi dell'attacco informatico, come la profilazione di specifici bersagli per operazioni mirate.

Tra questi, i principali sono stati (Figura 5) la posta elettronica, sfruttata per condurre attacchi di *phishing* e per carpire credenziali valide, seguita dallo sfruttamento di vulnerabilità, derivanti dal mancato aggiornamento dei sistemi, e dall'utilizzo indebito di account validi, in quanto presumibilmente compromessi in precedenza. La preponderanza dell'impiego dell'e-mail quale vettore per l'inizio della maggior parte degli attacchi richiama l'importanza cruciale che riveste il fattore umano quale argine determinante contro le minacce cyber.

L'analisi di tali vettori di attacco riveste un ruolo fondamentale nella comprensione delle dinamiche di compromissione, rappresentando un elemento essenziale per la definizione di misure di prevenzione e mitigazione volte a ridurre l'esposizione ai rischi, prevenire accessi non autorizzati e contenere l'impatto di eventuali intrusioni.

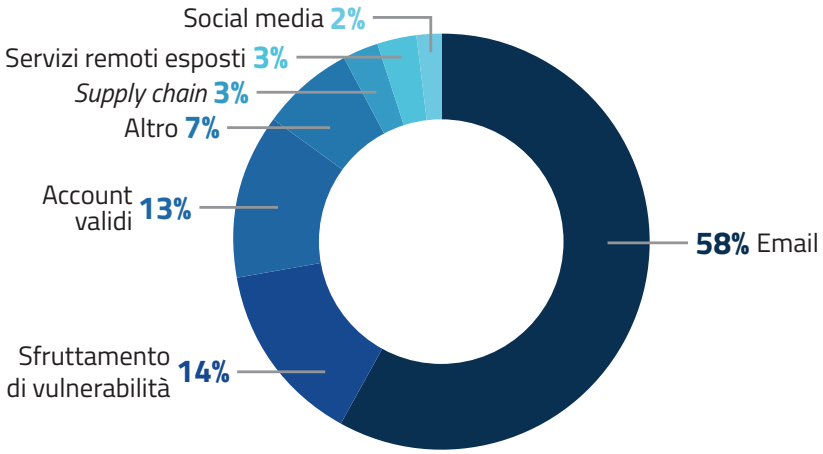


Figura 5 – Distribuzione dei principali vettori di attacco

Dall'analisi e successiva classificazione dei 1.979 eventi cyber è stato possibile individuare le tipologie di minacce riportate in Figura 6. Dal punto di vista numerico, emerge il DDoS quale minaccia preponderante, seguita dall'*information disclosure* e dal *brand abuse* (l'utilizzo di loghi e immagini istituzionali, solitamente ai fini di *phishing*). Occorre segnalare anche la rilevanza del *ransomware* che, pur rappresentando solo la sesta minaccia in termini numerici (198 eventi), ha impatti estremamente rilevanti, in quanto quasi nella totalità dei casi provoca l'indisponibilità prolungata dei dati con conseguenze importanti sull'operatività dell'Amministrazione o impresa colpita. Un'altra minaccia di particolare rilevanza, benché numericamente esigua, è costituita dagli APT, sia a causa della complessità degli strumenti impiegati che della strategicità dei soggetti *target*. Si noti che ogni evento può essere associato a una o più tipologie di minacce: 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*.

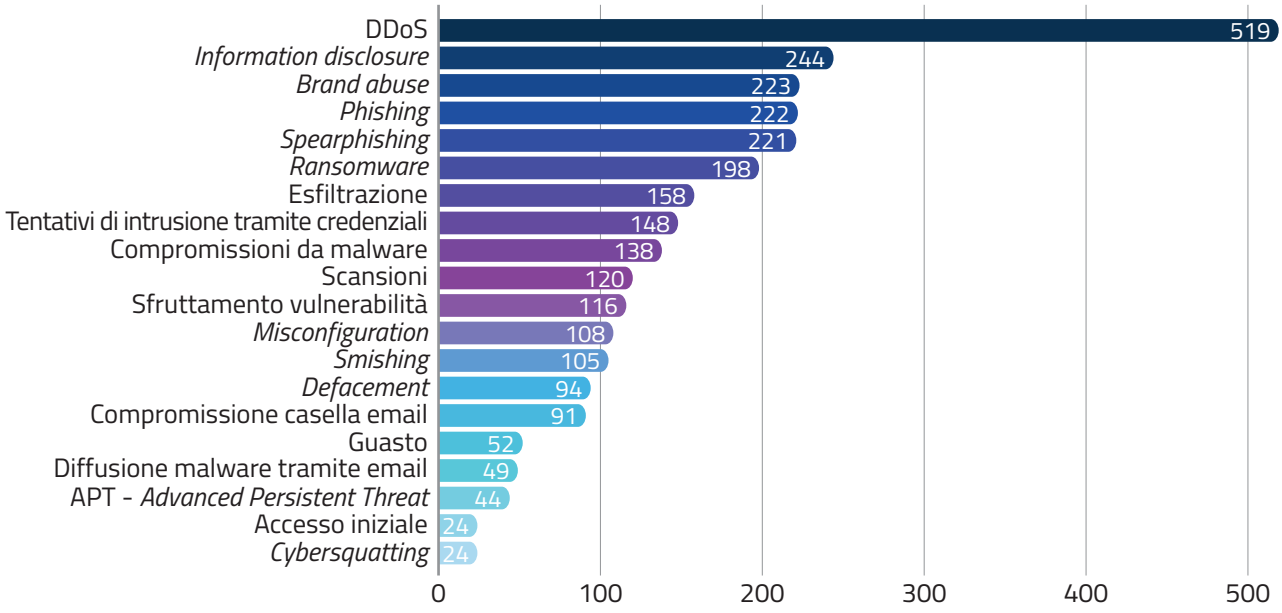


Figura 6 – Minacce rilevate negli eventi cyber trattati nel 2024 (top 20)

Le vittime accertate nel 2024 sono state quasi 2.800 ma, considerando che in alcuni casi uno stesso soggetto ha subito più di un evento, il totale di vittime univoche si ferma a 1.260. Queste sono situate prevalentemente nel Nord Italia, in particolare Milano e Torino, e nell'area di Roma (Figura 7), confermando una concentrazione delle attività ostili in contesti caratterizzati da un'elevata densità di insediamenti industriali, di infrastrutture critiche e di sedi di rilevanza istituzionale.

Per quanto attiene ai settori di attività delle vittime, prevale la Pubblica Amministrazione, sia a livello locale che centrale, seguita dal settore delle telecomunicazioni (Figura 8). Al fine di una corretta lettura del dato, è importante sottolineare che ciascun evento può interessare una o più vittime, ognuna operante in uno o più settori di attività. Occorre precisare, inoltre, che la visibilità più ampia di cui l'ACN gode riguarda la Pubblica Amministrazione e i settori critici individuati dalla normativa vigente, per la ragione che su di essi principalmente ricadono gli obblighi di notifica.

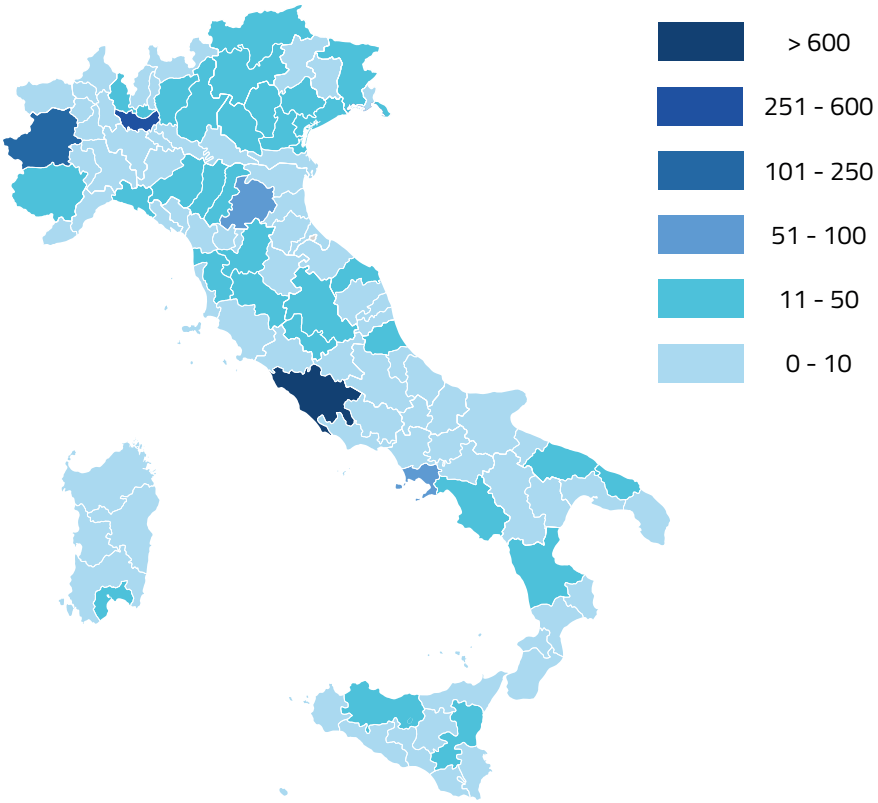


Figura 7 – Distribuzione geografica delle vittime degli eventi cyber trattati nel 2024

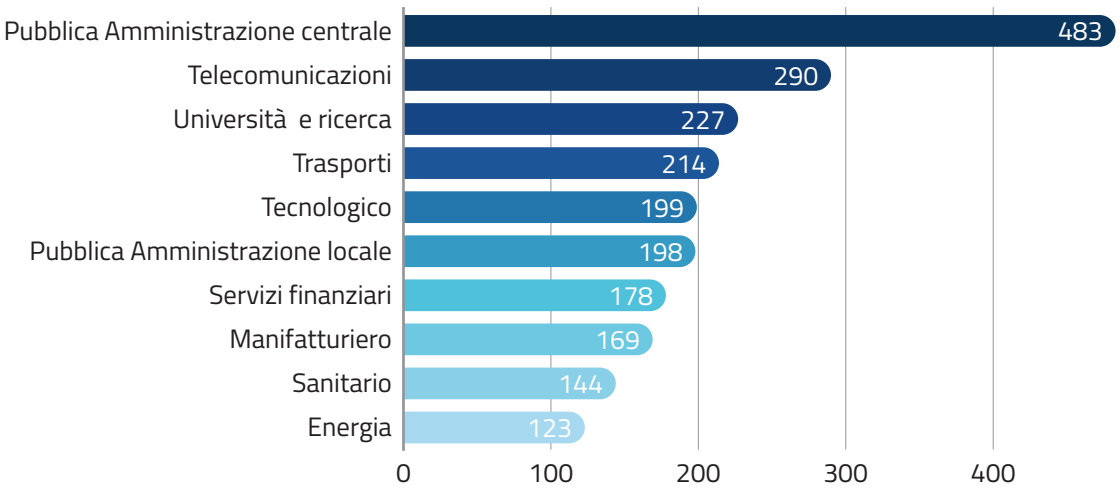


Figura 8 – Vittime di eventi cyber trattati nel 2024 per settore *target* (top 10)

La Figura 9 rappresenta la distribuzione delle vittime di incidente in base a tre livelli di criticità, mostrando come il numero più elevato di vittime si registri nelle fasce di criticità massima anche in ragione, come si è precisato, degli obblighi normativi di notifica. In particolare, le vittime a criticità massima (325) rientrando nei parametri di notifica obbligataria prevista dal Perimetro di sicurezza nazionale cibernetica, dalla Direttiva NIS, dal Decreto TELCO e dalla legge n. 90/2024, sono oggetto di una più ampia azione di monitoraggio sia proattiva, volta a prevenire e mitigare ulteriori impatti, sia reattiva, finalizzata alla gestione degli incidenti già avvenuti.

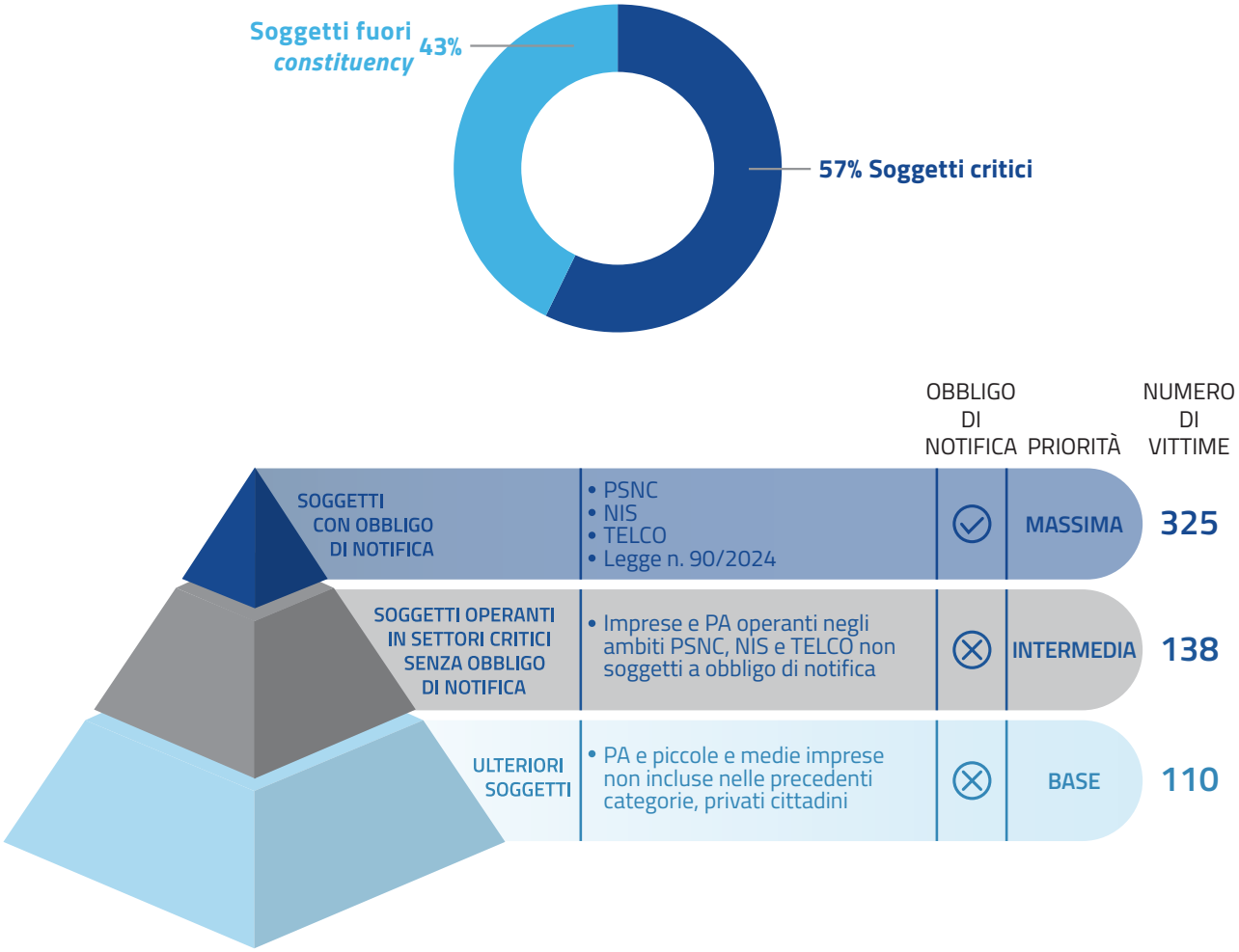


Figura 9 – Distribuzione delle vittime di incidenti in base alla loro criticità

2.3 FOCUS SULLE PRINCIPALI MINACCE: DDOS, *RANSOMWARE* E APT

2.3.1 DDoS: l'hacktivismo contro soggetti italiani

Anche nel 2024 l'hacktivismo ha continuato a rappresentare una componente significativa delle attività cyber rilevate in Italia, in crescita del 63% rispetto all'anno passato. Tale fenomeno è quasi sempre direttamente riconducibile a gruppi non statuali ma allineati a specifici interessi geopolitici, particolarmente nel quadro del conflitto in Ucraina. I gruppi filorussi, infatti, sono i più attivi contro i soggetti italiani (circa 500 attacchi) e, tra questi, quello che ha colpito più di frequente è NoName057(16).

In termini generali, gli hacktivisti hanno condotto attacchi DDoS contro istituzioni pubbliche e settori strategici, rivendicando le proprie azioni con post sui social media. Tali azioni, di carattere prettamente dimostrativo, generano disservizi temporanei per le risorse attaccate che non sono protette tramite appositi sistemi di difesa automatici. In assenza di questi, l'intervento manuale sulle configurazioni dei sistemi da parte degli operatori è comunque sufficiente per neutralizzarne gli impatti, che quindi sono generalmente piuttosto limitati. Tuttavia, il breve tempo che intercorre tra l'avvio dell'attacco e l'adozione di contromisure consente agli attaccanti di rivendicare il disservizio, millantando impatti molto significativi.

Durante l'anno sono state registrate tre campagne di attacchi DDoS, nei mesi di febbraio, maggio e dicembre (Figura 10), tutte rivendicate da collettivi hacktivisti di impronta filorussa. Dei 519 attacchi DDoS rilevati, solo il 15% ha prodotto disservizi misurabili di carattere temporaneo (tipicamente circa un'ora di irraggiungibilità della risorsa attaccata), mentre nei restanti casi non sono stati rilevati impatti.

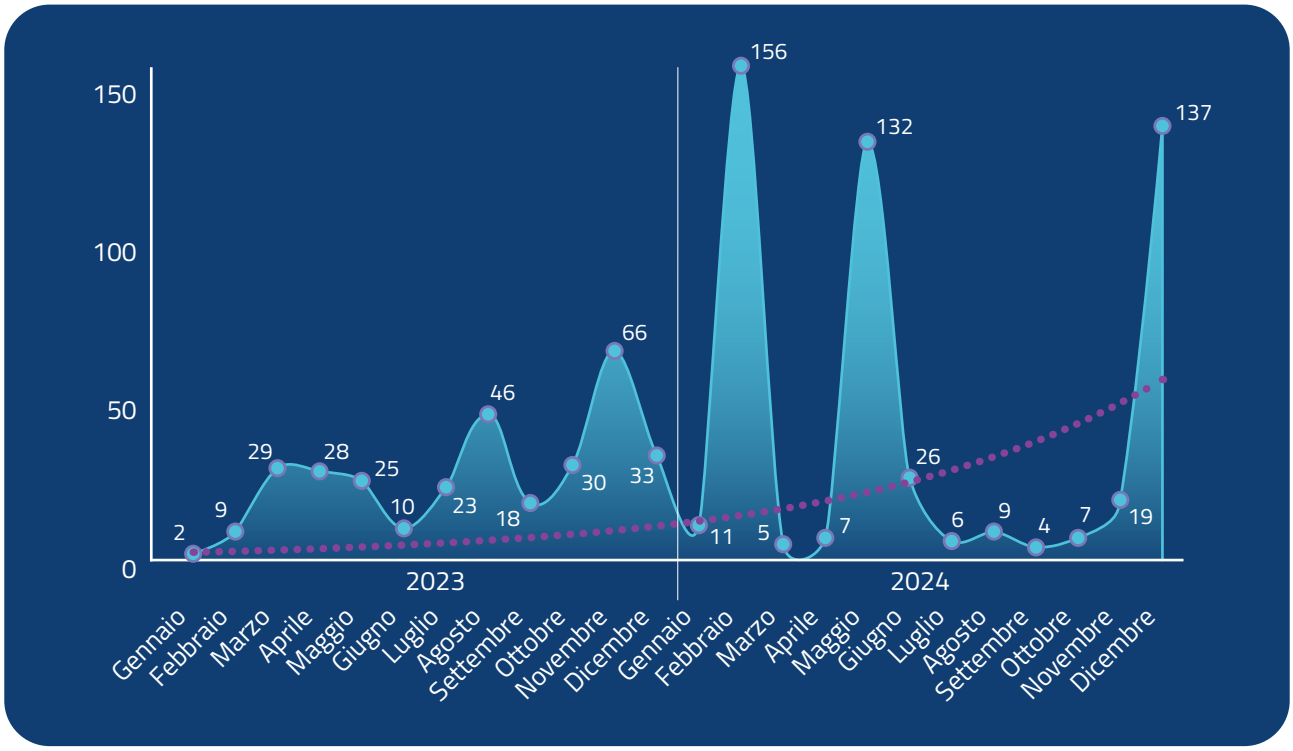


Figura 10 – Numero di eventi DDoS censiti dall'Agenzia a partire da gennaio 2023

Tra le vittime di DDoS si rileva una prevalenza di obiettivi pubblici (Figura 11). I settori più colpiti (Figura 12) sono risultati quello dei trasporti (tipicamente siti web di compagnie di trasporto locale), le Pubbliche Amministrazioni centrali e i servizi finanziari.

Per quanto attiene ai siti web attaccati, si è registrato un aumento dell'attività verso servizi secondari o periferici non critici, e pertanto

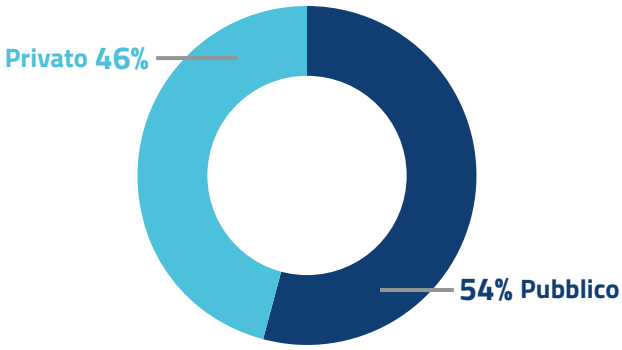


Figura 11 – Eventi DDoS per tipologia di vittima

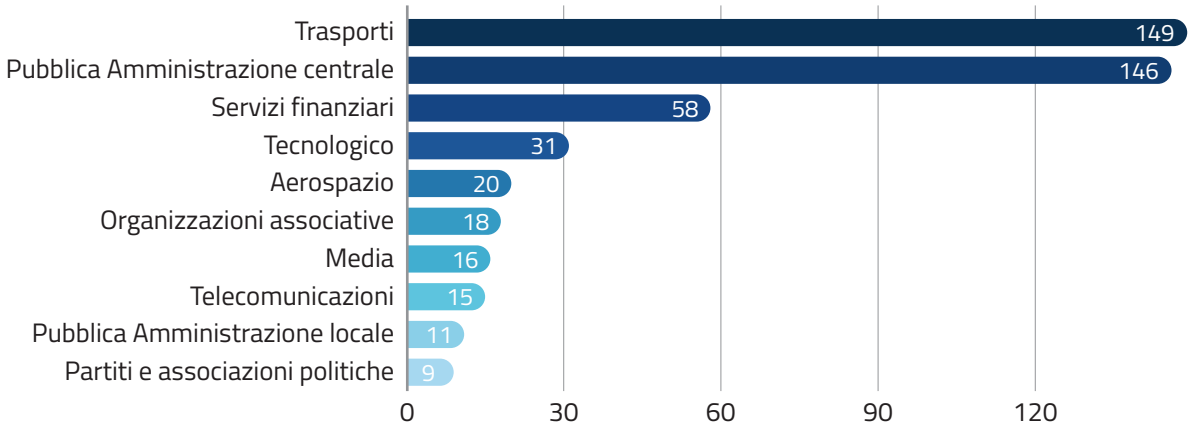


Figura 12 – Numero di eventi DDoS per settore di attività economica della vittima (top 10)

spesso privi di protezione anti-DDoS, piuttosto che verso i servizi principali. Questo ha permesso agli attaccanti di rivendicare comunque disservizi, alimentando la narrativa attivista pur in assenza di impatti significativi. In tutte le circostanze, il CSIRT Italia ha effettuato campagne di allertamento ai soggetti obiettivo dei DDoS, indicando loro contromisure di mitigazione e pubblicando sul portale pubblico dei bollettini dedicati.

Dall'analisi delle rivendicazioni degli attacchi DDoS nel mondo, effettuata monitorando i canali utilizzati a tale scopo dagli hacktivisti, emerge che l'Italia si colloca al nono posto a livello globale e al quarto tra i Paesi dell'UE (Figura 13).

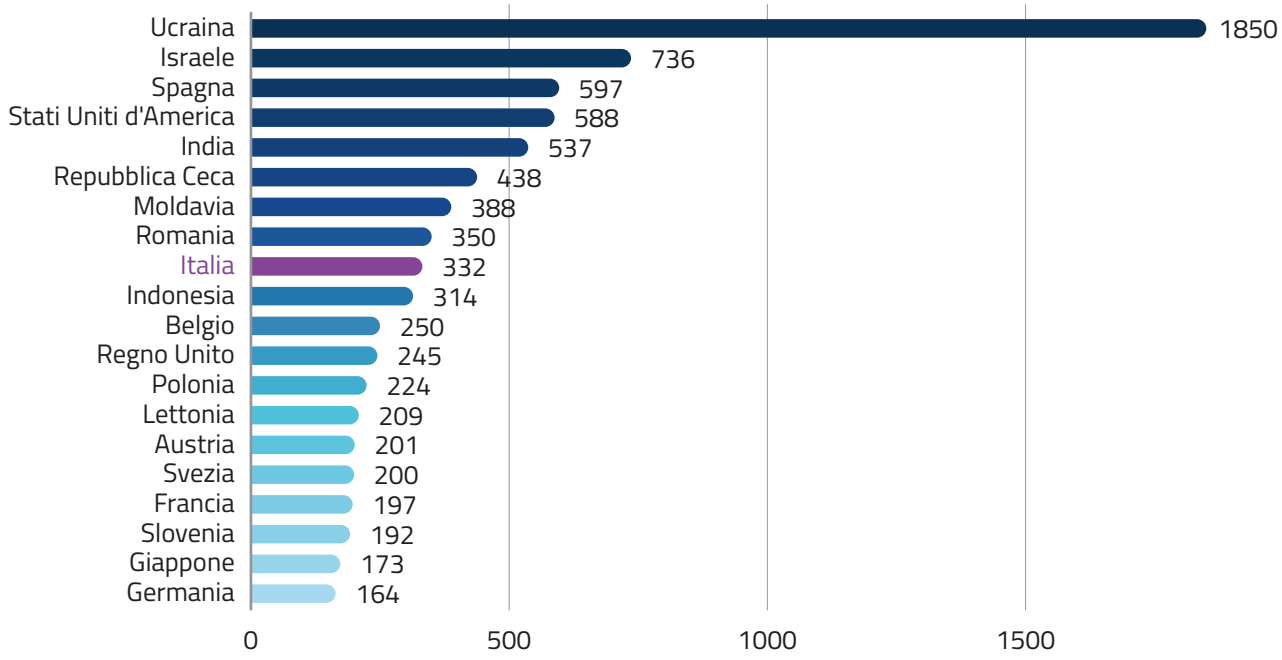


Figura 13 – Numero di rivendicazioni di DDoS per Paese (top 20)

2.3.2 *Ransomware*: la minaccia che colpisce sempre più le PMI

In linea di continuità con quanto osservato durante il 2023, il *ransomware* si è confermato una delle minacce cibernetiche più impattanti con 198 eventi rilevati (Figura 14), un incremento del 20% rispetto all'anno precedente. Le vittime accertate sono state complessivamente 192, mentre in 6 occasioni non è stato possibile risalire al soggetto interessato.

È bene evidenziare, tuttavia, che il dato osservato rappresenta solo una frazione del numero complessivo di eventi *ransomware* effettivamente avvenuti, in quanto questi spesso non emergono pubblicamente e non vengono denunciati alle autorità. Ciò deriva, da un lato, dalla tendenza da parte di molte vittime a non segnalare gli incidenti e, dall'altro, dalla scelta di alcuni attori criminali di non rivendicare sui propri siti le operazioni ai fini della richiesta di riscatto, fattori che contribuiscono a ridurre la visibilità sul fenomeno.

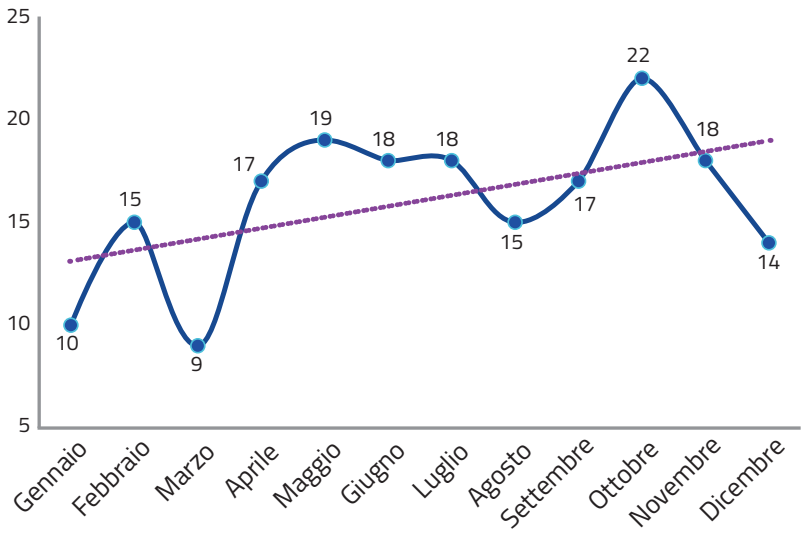


Figura 14 – Vittime di eventi *ransomware* gestiti dall'Agenzia nel 2024

Gli attacchi *ransomware* hanno colpito prevalentemente il settore privato e, in particolare, le piccole e medie imprese (PMI), interessate dal 75% degli eventi ai danni dei privati (Figura 15).

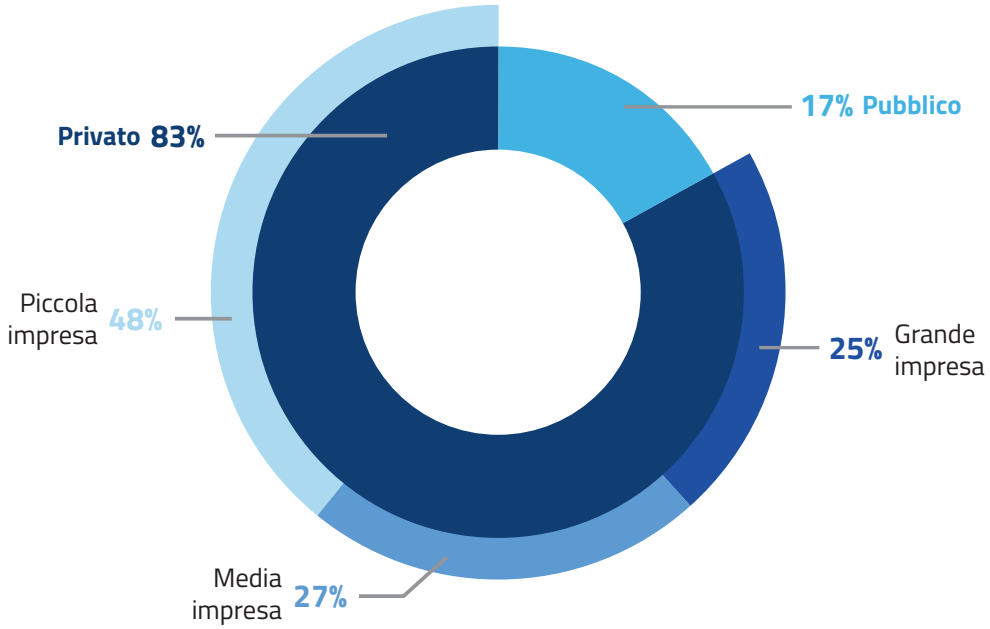


Figura 15 – Vittime di eventi *ransomware* per tipologia e dimensione aziendale

L'analisi delle vittime di *ransomware* mostra che nella grande maggioranza dei casi (95%) sono stati interessati soggetti a minor criticità, mentre solo il 5% degli eventi ha avuto come obiettivo soggetti classificati come a criticità massima, ovvero destinatari di obblighi di legge quali la notifica degli incidenti. Ciò a conferma sia di una concentrazione della minaccia *ransomware* verso obiettivi meno strutturati e dotati di limitate capacità di cybersicurezza – e presumibilmente più proni al pagamento del riscatto – sia dell'efficacia degli interventi normativi in materia (Figura 16).

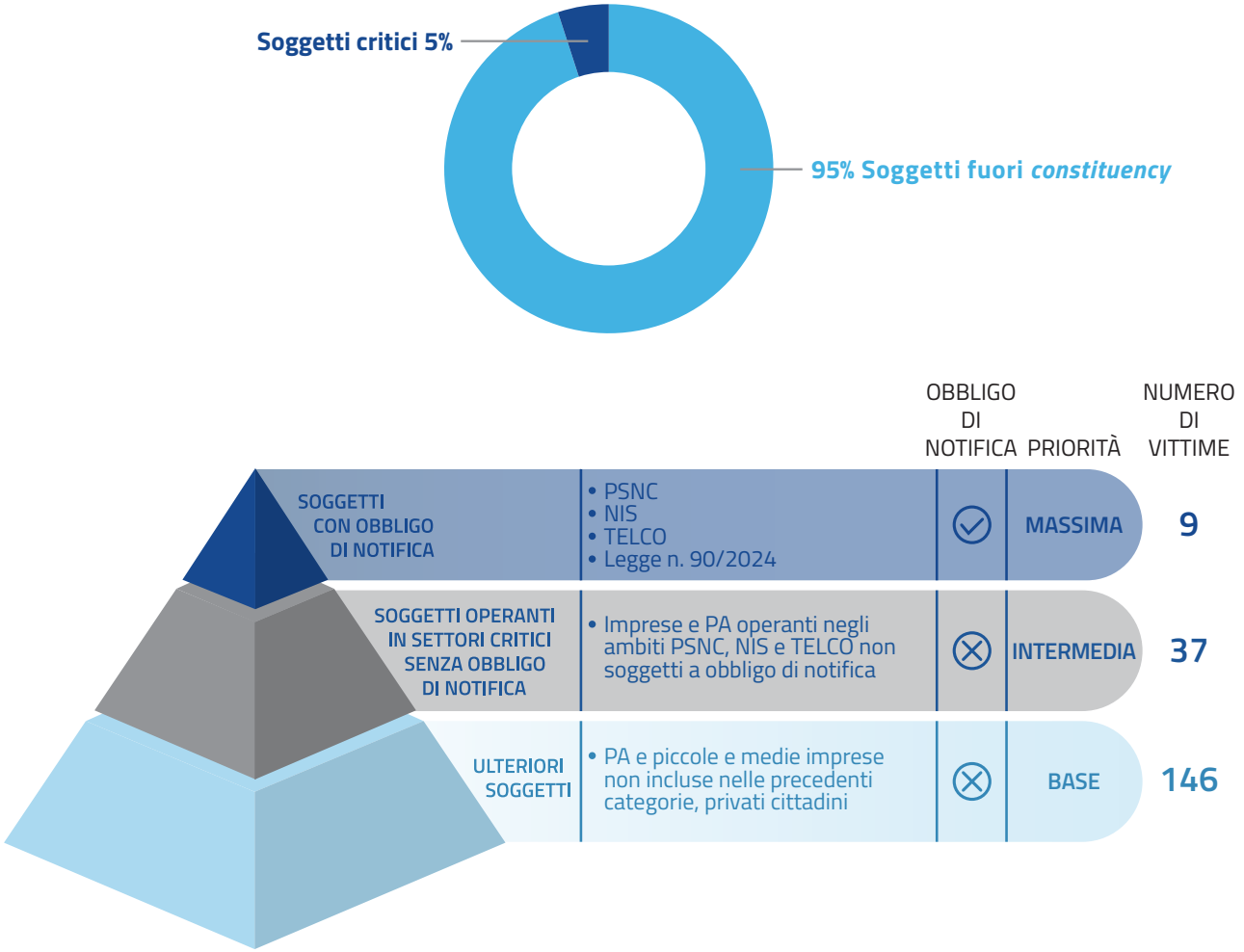


Figura 16 – Distribuzione delle vittime di *ransomware* in base alla loro criticità

Tra i settori economici (Figura 17), il manifatturiero continua a essere il più colpito, riflettendo la vulnerabilità intrinseca di un comparto caratterizzato da una forte presenza di piccole e medie imprese, spesso prive di competenze specialistiche e di strutture interne dedicate e, quindi, non sufficientemente attrezzate per proteggere adeguatamente i propri sistemi. Particolare attenzione merita, inoltre, il settore sanitario che, pur non risultando il più colpito in termini di numero di eventi, si distingue per la gravità degli impatti, sia sull'operatività che sulla riservatezza dei dati, particolarmente alla luce della sensibilità dei dati esfiltrati. Sul piano geografico, le aree metropolitane di Roma e Milano rimangono le più colpite.

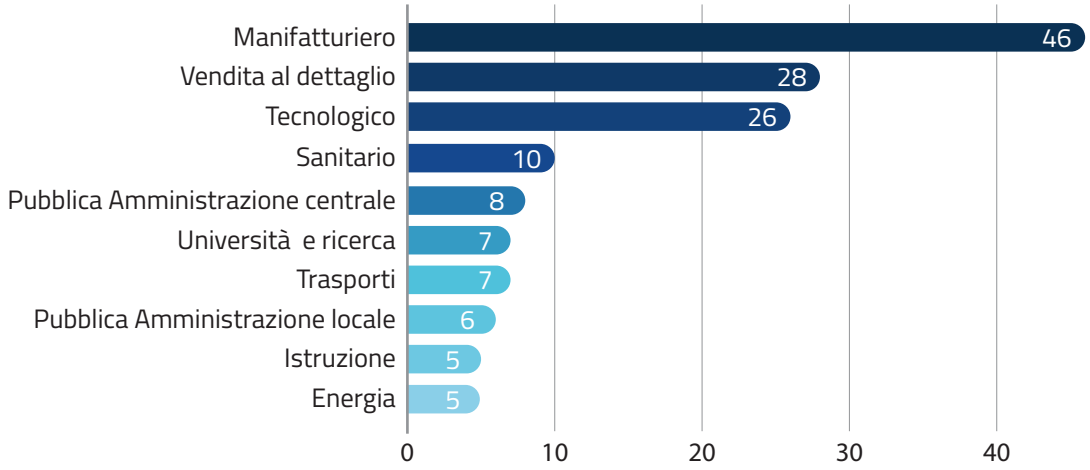


Figura 17 – Principali eventi *ransomware* per settore di attività economica della vittima (top 10)

Gli attacchi *ransomware* osservati nel 2024 in Italia sono stati condotti da almeno 40 diversi gruppi criminali, in aumento rispetto ai 20 censiti l'anno precedente. Questa crescita testimonia la capacità di tali sodalizi di rigenerarsi, nonostante le operazioni internazionali di contrasto consentano periodicamente lo smantellamento di alcune di queste organizzazioni criminali. I nuovi gruppi, spesso formati da elementi già attivi in precedenti *gang*, dimostrano una notevole flessibilità operativa, adottando modelli di affiliazione come il *Ransomware as a Service* (RaaS) per ampliare la portata delle loro azioni. Il RaaS è un vero e proprio modello di business, in cui gli sviluppatori di *ransomware* mettono a disposizione di terze parti strumenti malevoli in cambio di una percentuale dei guadagni derivanti dai riscatti. L'aumento del numero delle *gang* è potenzialmente riconducibile anche alla maggiore disponibilità di strumenti utilizzabili per lanciare attacchi *ransomware*, dal momento che è frequente il riuso di codice o parti di codice malevolo condivisi dagli stessi gruppi criminali.

I gruppi *ransomware* più attivi in termini di rivendicazioni di attacchi contro l'Italia sono risultati RansomHub, LockBit 3.0 e 8Base (Figura 18).

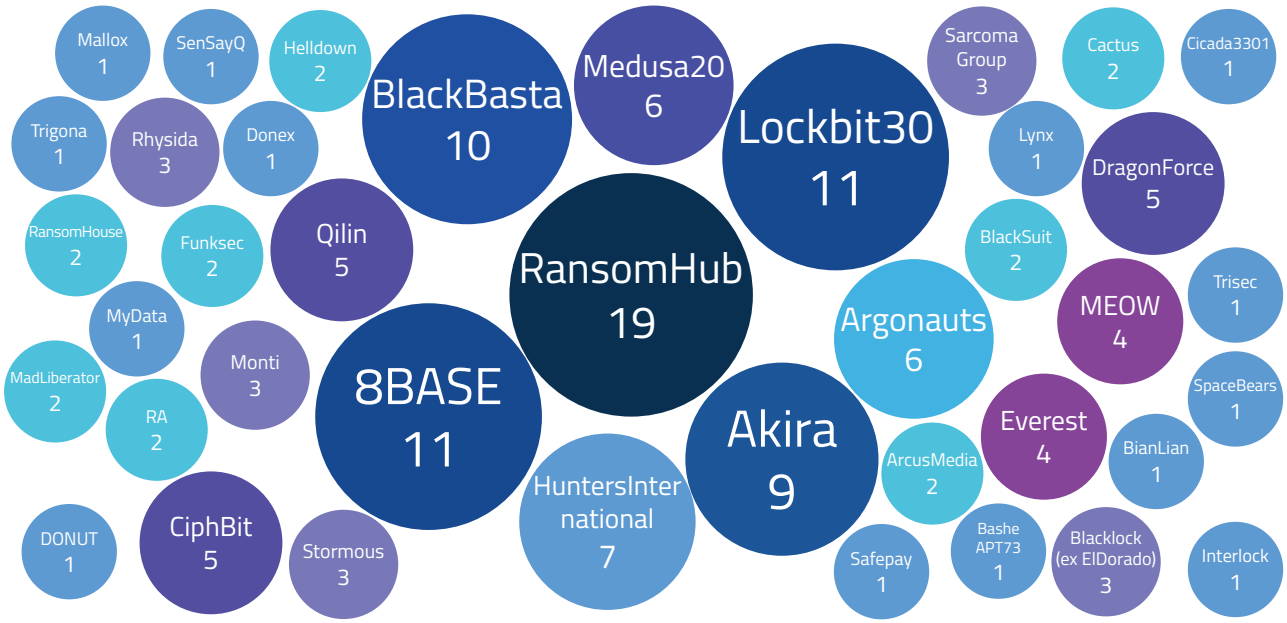


Figura 18 – Numero di rivendicazioni per gruppi *ransomware*

2.3.3 APT: le minacce avanzate e persistenti

Nel corso del 2024 sono state riscontrate attività ostili da parte di attori cosiddetti *Advanced Persistent Threat*, che conducono attacchi mirati, volti a installare malware e altri strumenti complessi nelle reti e nei sistemi bersaglio per riuscire a mantenere attivi i canali impiegati per l'esfiltrazione di informazioni di alto valore dalle infrastrutture IT della vittima. I principali intenti percepiti sono il posizionamento strategico all'interno di soggetti rilevanti e il furto di informazioni sensibili presenti nelle reti delle vittime.

Le analisi su determinati eventi e incidenti cyber hanno portato a evidenziare dei collegamenti con attività pubblicamente attribuite a gruppi noti, come APT28, APT29, Turla, APT15, Liminal Panda e Lazarus Group. In particolare, sono stati colpiti complessivamente 21 soggetti, pubblici e privati, afferenti al settore diplomatico, governativo, della difesa, dell'aerospazio, dei trasporti, delle telecomunicazioni, dell'istruzione e della tecnologia.

Si è potuto appurare che tali attori sono riusciti a compromettere reti e sistemi tramite diverse tecniche: sfruttamento di vulnerabilità o di relazioni di fiducia[1], nonché attraverso account validi e attività di *social engineering* complesse (incluso tramite *social network* professionali e interazioni dirette con i soggetti *target*). Per diversi eventi di compromissione, non è stato possibile identificare il vettore di accesso iniziale. Sono stati, inoltre, rilevati tentativi di infezione non andati a buon fine, condotti tramite campagne di *spearphishing* utilizzando e-mail scritte in maniera molto accurata, appositamente per selezionati soggetti, e un tentativo di sfruttamento di vulnerabilità.

In alcuni dei casi analizzati sono stati osservati malware non pubblicamente documentati e altamente sofisticati, anch'essi creati appositamente per la realtà *target*, sempre con la finalità di esfiltrazione di informazioni. Di particolare rilievo risulta l'impiego di reti di anonimizzazione condivise tra più attori al fine di mascherare la sorgente del traffico e rendere più difficile ricondurre l'attività a specifici gruppi.

A tale scopo, per evadere i controlli di sicurezza e occultare l'infrastruttura attaccante, è stato rilevato l'utilizzo illecito di strumenti di collaborazione *cloud*, impiegati sia come canali di comando e controllo, sia come vettori per la distribuzione di malware. Parallelamente, le analisi condotte nella gestione degli incidenti hanno evidenziato un uso esteso di strumenti *open-source* e commerciali destinati alle attività di *red teaming*, sfruttati dagli attori ostili per condurre operazioni offensive a scopo malevolo.

> ***Red team***
>
> *I red team testano la sicurezza di un'organizzazione, replicando tecniche e tattiche usate da attori malevoli. Impiegano software e framework progettati per simulare attacchi informatici in modo controllato, consentendo di identificare vulnerabilità in sistemi, reti e applicazioni.*

[1] L'accesso attraverso una relazione di fiducia con una terza parte sfrutta una connessione esistente che potrebbe essere meno protetta rispetto agli *asset* del soggetto *target*.

2.4 ALLERTAMENTO: DIFFONDERE LA CONOSCENZA DELLE MINACCE

L'ACN porta avanti attività di monitoraggio proattivo al fine di individuare e segnalare tempestivamente ai soggetti della *constituency* l'esposizione a specifiche criticità, che possono essere sfruttate, o che sono già in corso di sfruttamento. A valle dell'individuazione di tali criticità, il CSIRT Italia contatta i soggetti a rischio e, qualora risultino particolarmente diffuse, svolge opera di condivisione degli *alert*, sia tramite portale pubblico che attraverso i canali social dedicati (X, Telegram).

Nel corso del 2024 sono stati segnalati:

- 722 indirizzi web di *phishing*, ovvero pagine web artefatte, contenenti riferimenti espliciti o simili a pagine web di oltre 100 soggetti pubblici o privati della *constituency*, presumibilmente utilizzate per ingannare gli utenti e carpire credenziali;
- 550 dispositivi o servizi IT potenzialmente compromessi, ovvero per i quali è stato rilevato un comportamento associabile a un'attività malevola in corso. Relativamente a tali dispositivi o servizi sono state inviate 176 comunicazioni, di cui il 14% verso soggetti pubblici e 86% verso soggetti privati;
- 11.290 dispositivi o servizi IT che esponevano potenziali rischi, come ad esempio versioni di software vulnerabili, per i quali sono state inviate 5.197 comunicazioni. Di queste il 31% verso soggetti pubblici e 69% verso soggetti privati.

Con particolare riguardo a quest'ultima fattispecie, risulta di interesse soffermarsi sia sulle categorie di dispositivi e servizi maggiormente esposti al pericolo di sfruttamento delle vulnerabilità, sia sulle tipologie di vulnerabilità da cui origina tale rischio. Raggruppando i dispositivi e servizi a rischio segnalati per categorie (Figura 19), si evince come la categoria più esposta al pericolo sia quella delle tecnologie per il lavoro remoto (principalmente *Virtual Private Network* e *Virtual Desktop*).

Ciò è dovuto non solo al numero di vulnerabilità gravi emerse nell'ultimo anno su tali dispositivi, ma anche alla loro maggiore intrinseca esposizione ai rischi, in quanto devono essere raggiungibili direttamente tramite Internet per consentire l'accesso da remoto degli utenti.

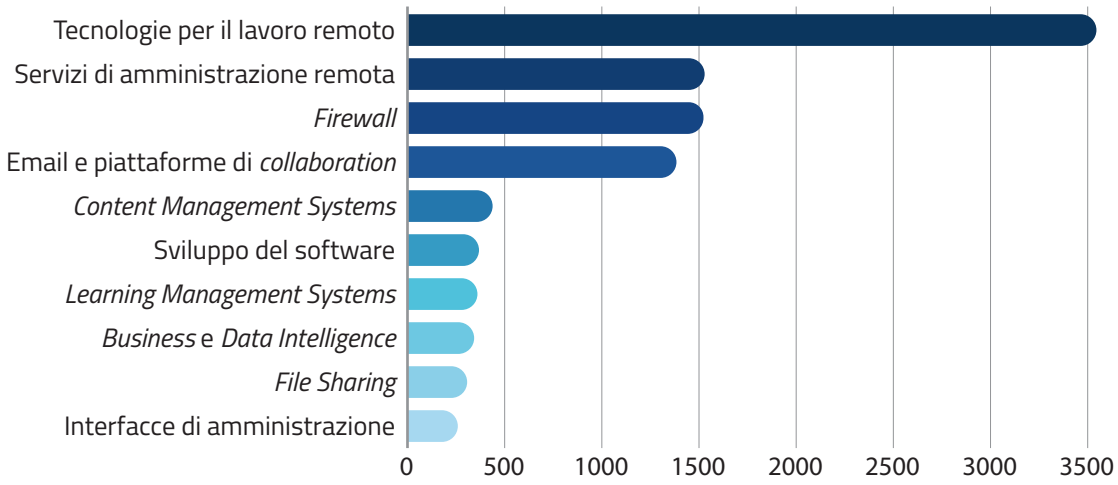


Figura 19 – Numero di asset a rischio segnalati suddivisi per categoria

Nella Figura 20, invece, gli *asset* a rischio sono divisi a seconda delle tipologie di vulnerabilità, rinvenute e segnalate ai soggetti, con la relativa specifica del livello di gravità.

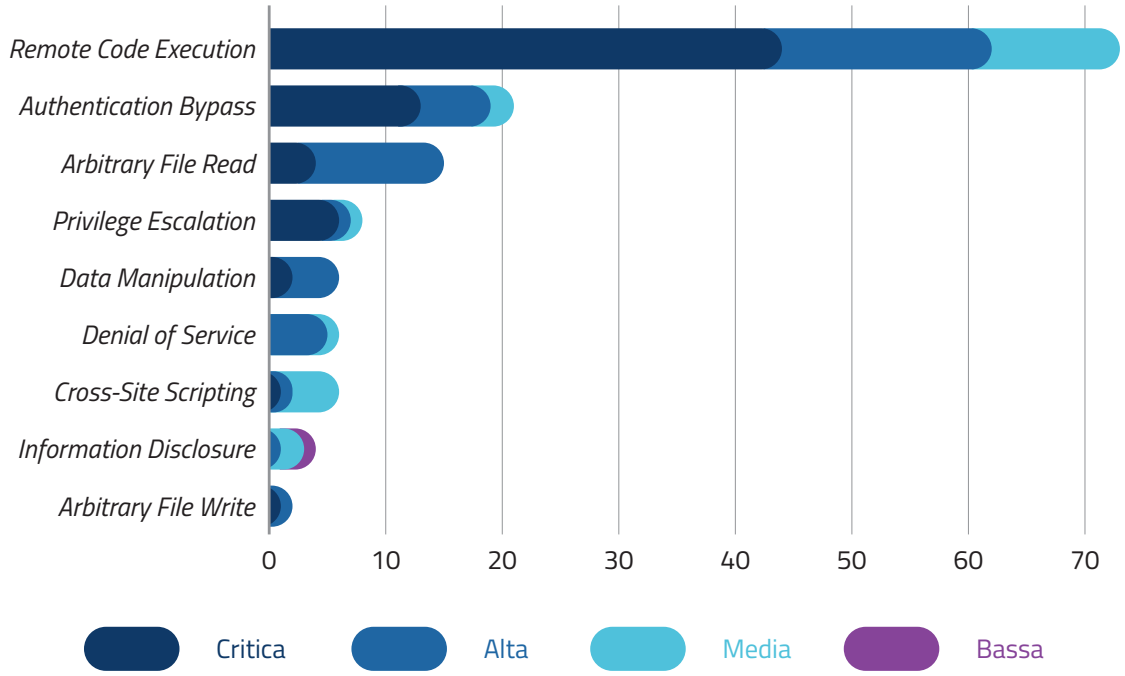


Figura 20 – Tipologia e gravità delle vulnerabilità rinvenute e segnalate negli *asset* a rischio

2.5 INTERVENTI DEL CSIRT ITALIA A SUPPORTO DELLE VITTIME DI INCIDENTE

Come stabilito dalla normativa vigente, l'Agenzia fornisce anche supporto diretto alle vittime di incidenti cibernetici, tramite specifici team del CSIRT Italia di *Digital Forensics Incident Response* (DFIR). Tale supporto si concretizza nell'affiancamento, in loco o da remoto, dei soggetti colpiti nella gestione delle criticità e degli impatti derivanti dagli incidenti, attraverso l'individuazione delle misure necessarie, sia per il contenimento immediato dell'evento, sia per il ripristino dell'erogazione dei servizi compromessi.

Questo modello di intervento, che prevede l'integrazione e l'ottimizzazione delle risorse già esistenti all'interno delle infrastrutture colpite, ha permesso in più occasioni di minimizzare l'impatto operativo, favorendo una gestione più efficiente degli incidenti e contribuendo al rafforzamento della postura di sicurezza dei soggetti interessati, migliorando la resilienza e la capacità di monitoraggio e rilevamento di minacce future.

Nel corso del 2024, l'attività di supporto operativo alle vittime è stata incrementata anche attraverso l'elaborazione di piani di risposta ad hoc, secondo un approccio metodologico che prevede più fasi. In ogni intervento è prevista una valutazione preliminare delle vulnerabilità e delle criticità presenti nelle infrastrutture compromesse. Successivamente vengono applicate strategie operative che prevedono l'acquisizione e l'analisi degli artefatti digitali, la pianificazione delle azioni di *remediation* e *recovery* e la verifica della corretta implementazione delle misure correttive. Questo processo, graduale e strutturato, ha consentito di affrontare in maniera efficace le criticità emerse.

In tale contesto, l'Agenzia ha perseguito un miglioramento continuo delle proprie metodologie operative, attraverso l'adozione di strumenti tecnologicamente avanzati e l'affinamento delle pratiche più innovative, rispondendo con maggiore efficacia alle esigenze di un panorama della minaccia cibernetica in continua evoluzione. A ciò si è aggiunto l'avvio di percorsi formativi specialistici, specifici per il personale impiegato in tali attività.

Durante il 2024 il personale tecnico è intervenuto, con le squadre DFIR, in 40 diverse occasioni. Gli interventi, che si protraggono sempre per più giorni e talvolta per settimane o mesi, sono distribuiti nel tempo come mostrato in Figura 21.

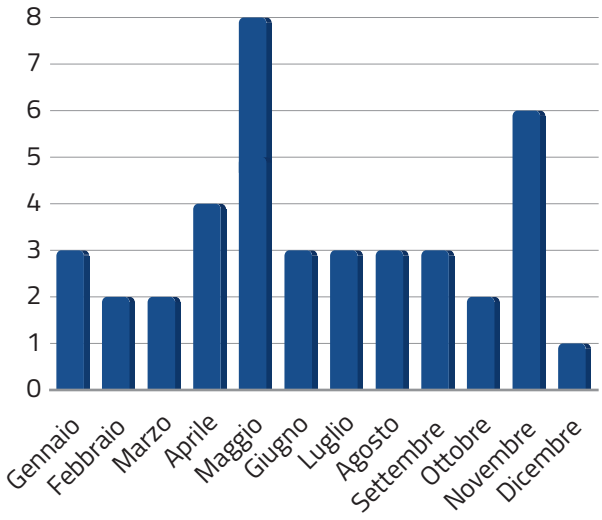


Figura 21 – Numero di interventi a supporto diretto delle vittime per data di avvio

Gli interventi a diretto supporto delle vittime hanno riguardato principalmente la Pubblica Amministrazione, il settore sanitario, quello dell'aerospazio e dell'università e ricerca (Figura 22).

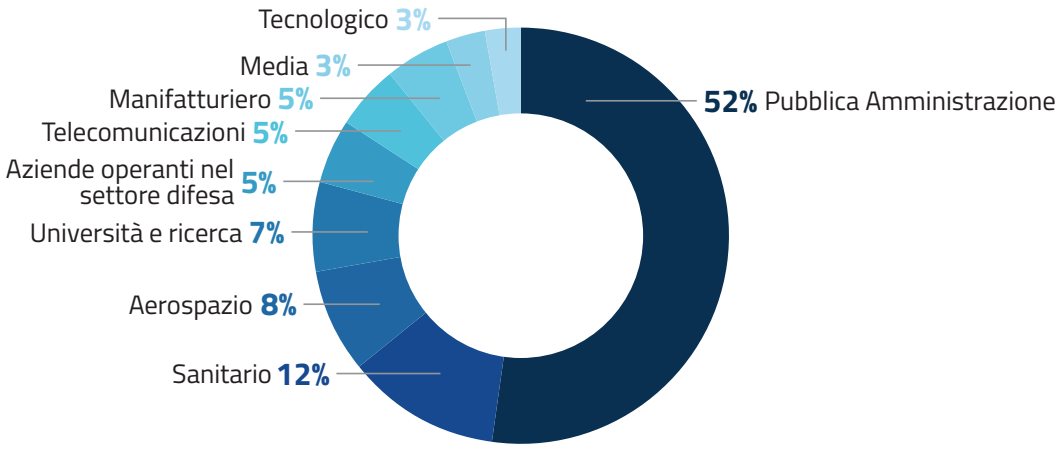


Figura 22 – Distribuzione degli interventi a supporto diretto delle vittime per settore

2.6 FOCUS PA: TIPI DI MINACCIA, OBBLIGHI DI NOTIFICA E ATTIVITÀ DI SUPPORTO

Nel corso del 2024, l'Agenzia ha gestito 756 eventi cyber ai danni di istituzioni pubbliche nazionali, in sensibile aumento rispetto ai 383 del 2023. Tale incremento appare in parte ascrivibile al modificato impianto normativo (vedasi Capitolo 1), nonché all'aumentata capacità del CSIRT Italia di rilevare eventi, incidenti e criticità.

Circa il 35% degli eventi (263) sono stati classificati come incidenti (nel 2023 si erano fermati a 85), che hanno provocato nella maggior parte dei casi il malfunzionamento dei sistemi e conseguenti blocchi o rallentamenti nell'erogazione dei servizi. La loro distribuzione nella Pubblica Amministrazione è rappresentata in Figura 23.

Considerando la frequenza e l'impatto (una media di circa 6 eventi a settimana) delle diverse tipologie di minacce, emerge come nel 2024 sia stato il DDoS il fenomeno più ricorrente nei confronti delle PA (Figura 24). Frequente altresì il *brand abuse*, seguito da azioni mirate alla compromissione dei dati, tra cui spiccano casi di esposizione non autorizzata (*information disclosure*) ed esfiltrazione di dati, spesso riconducibili a *ransomware* e malware. Come specificato in precedenza, uno stesso evento cyber può essere associato anche a più di una tipologia di minaccia.

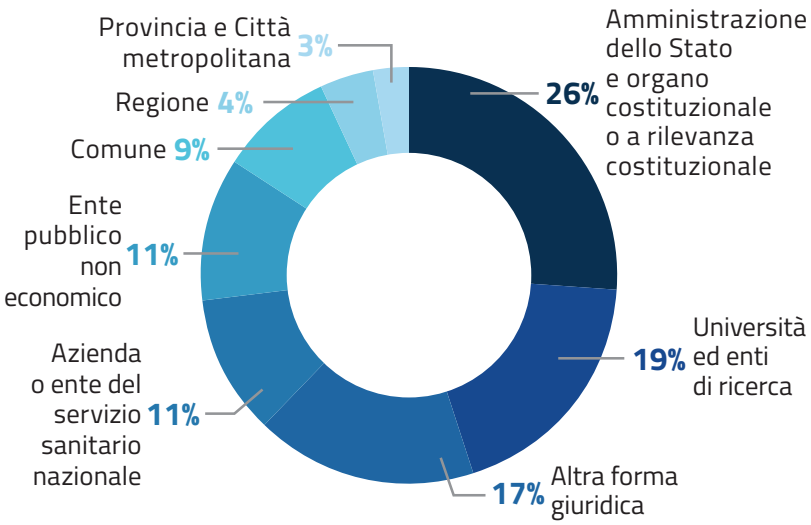


Figura 23 – Distribuzione degli eventi cyber nei settori della Pubblica Amministrazione

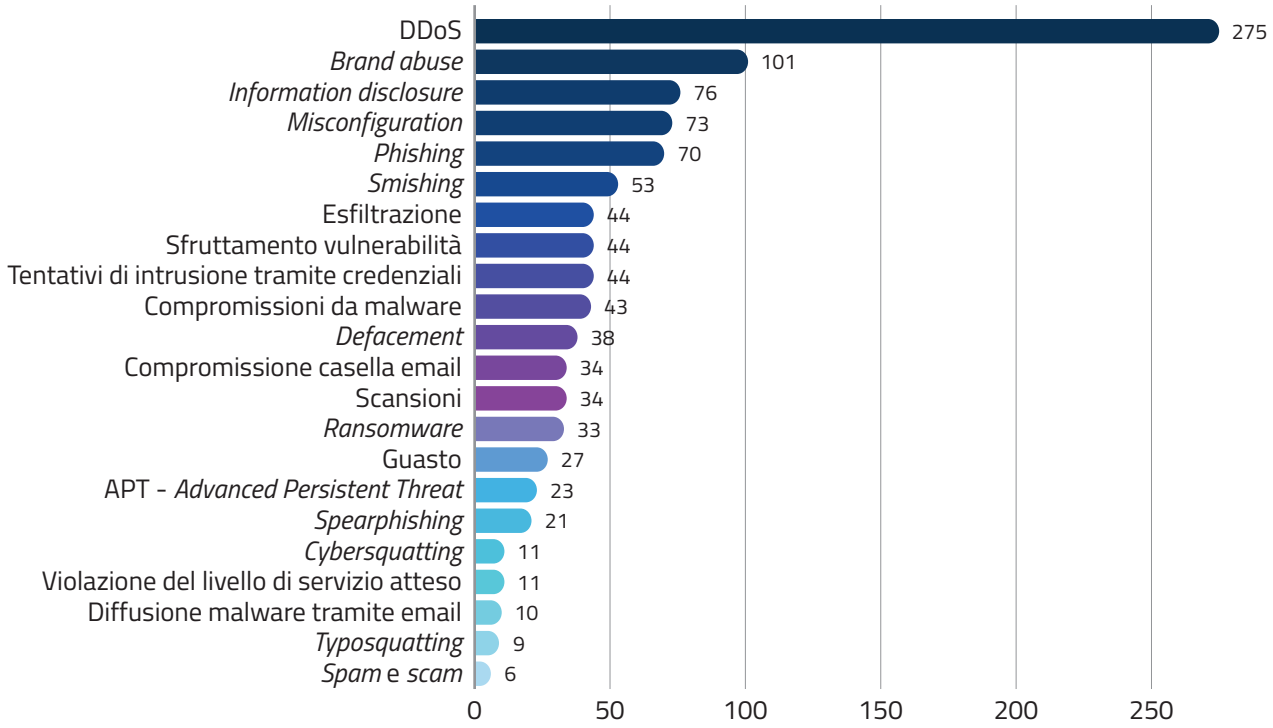


Figura 24 – Tipologie di minacce rilevate negli eventi cyber nella Pubblica Amministrazione (top 20)

In 28 casi i team dedicati del CSIRT Italia sono intervenuti direttamente per supportare i soggetti nella risposta a incidenti particolarmente complessi, avvenuti in realtà molto diverse tra loro, dalla PA centrale a strutture sanitarie ed enti universitari e culturali.

3.

L'AGENZIA NEL PANORAMA ISTITUZIONALE: CONSOLIDAMENTO DELLA COOPERAZIONE IN MATERIA CYBER

L'Agenzia, all'interno della rinnovata architettura nazionale di cybersicurezza, è chiamata a svolgere un'importante funzione di coordinamento dei diversi soggetti a vario titolo coinvolti nel garantire la sicurezza cibernetica del Paese. Tale ruolo si esplica in molteplici formati a partire da tavoli interministeriali focalizzati su una collaborazione sia a livello politico-strategico, sia a livello più operativo. Oltre al Comitato interministeriale per la cybersicurezza (CIC), che si occupa delle politiche nazionali in materia, attraverso consessi quali il Nucleo per la cybersicurezza e il Tavolo Perimetro e quello NIS, l'Agenzia riunisce i rappresentanti dei Ministeri e delle altre Amministrazioni che più direttamente si interessano ai profili cyber.

Proficuo è stato, inoltre, il dialogo con il Parlamento, rispetto alle sue funzioni di controllo e legislative. Le costanti interazioni hanno permesso di incidere sui progressi normativi in tema di cybersicurezza. Intercettare le più ampie istanze espresse dal legislatore è stato, infatti, cruciale per mantenere aggiornato il quadro regolatorio sulla cybersicurezza, nonché sul più ampio processo di digitalizzazione, che necessariamente deve essere sicura.

Particolare attenzione è stata riservata anche alla costruzione di un ecosistema in cui i soggetti privati rivestono un ruolo sinergico con quelli pubblici nell'elevare la postura cibernetica e la capacità di resilienza del nostro Paese, dal momento che il settore privato è imprescindibile per la concreta attuazione di qualunque indirizzo in tema cyber. Anche per questo l'Agenzia ha promosso o assicurato la propria partecipazione a un gran numero di eventi, nell'ambito dei quali è potuta entrare in contatto e dialogare con comunità locali, imprenditoriali, universitarie e associative. Ciò è stato favorito anche dalla sottoscrizione e dall'attuazione di accordi di vario tipo, da quelli volti allo scambio informativo a quelli per la formazione.

3.1 COORDINAMENTO INTERMINISTERIALE

3.1.1 Comitato interministeriale per la cybersicurezza

L'Agenzia nel corso del 2024 ha fornito il proprio supporto e contributo nei consessi istituzionali che ne prevedono il coinvolgimento, a partire dal già citato CIC, il comitato interministeriale con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza (vedasi box). Il CIC, che è istituito presso la Presidenza del Consiglio dei ministri, è chiamato a esprimersi per proporre gli indirizzi delle politiche di cybersicurezza, a vigilare sull'attuazione della Strategia nazionale in materia e sulla gestione economico-finanziaria dell'ACN, nonché a promuovere iniziative che favoriscano il rafforzamento della sicurezza cibernetica.

Comitato interministeriale per la cybersicurezza

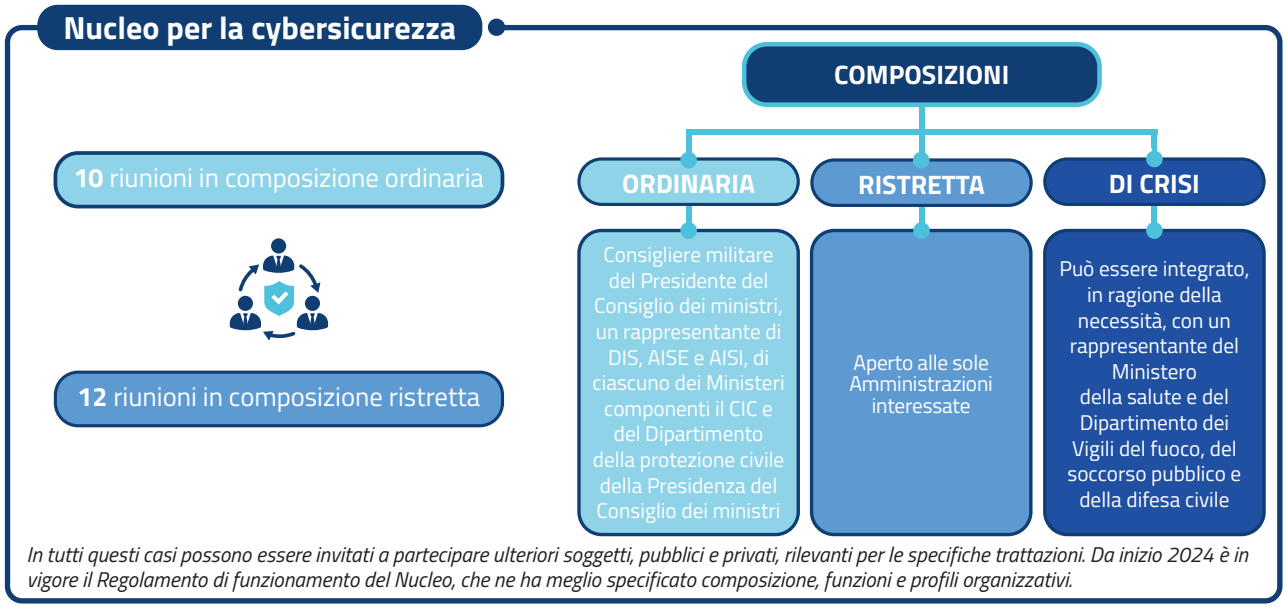
Il CIC è presieduto dal Presidente del Consiglio dei ministri ed è attualmente composto dall'Autorità delegata per la sicurezza della Repubblica, dai Ministri degli affari esteri e della cooperazione internazionale (MAECI), dell'interno, della giustizia, della difesa, dell'economia e delle finanze (MEF),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

Nell'anno in esame, il CIC è stato convocato 5 volte, nei mesi di gennaio, febbraio, giugno e dicembre. Nel corso di tali riunioni, oltre ai provvedimenti che ordinariamente richiedono il coinvolgimento del Comitato, sono stati esaminati i più rilevanti dossier in materia di sicurezza cibernetica, compresi quelli attraverso i quali si è aggiornato il quadro normativo di riferimento. Il CIC ha valutato in più occasioni aggiornamenti del Perimetro di sicurezza nazionale cibernetica, al fine di adattarne l'estensione alle esigenze evolutive della sicurezza nazionale. Nelle conseguenti proposte, per le determinazioni finali del Presidente del Consiglio dei ministri, il CIC ha puntualmente tenuto conto e recepito le indicazioni del Tavolo Perimetro operante presso l'Agenzia.

Inoltre, il Comitato ha fornito il proprio parere su due provvedimenti che hanno importanti risvolti di cybersicurezza. Uno di questi, correlato al recepimento nella normativa italiana della Direttiva NIS2, ha riguardato la c.d. clausola di salvaguardia che determina, per alcune definite entità, l'esenzione dagli obblighi della NIS2. Un altro parere ha avuto ad oggetto, in merito ai requisiti di sicurezza cyber, uno schema di decreto del Ministro della giustizia che ha disposto l'attivazione dell'archivio digitale, nonché la migrazione dei dati dalle Procure della Repubblica e il conferimento dei nuovi dati alle infrastrutture digitali interdistrettuali. Infine, il CIC ha vigilato sulla corretta programmazione e gestione economico-finanziaria dell'Agenzia, esprimendo parere favorevole sul bilancio consuntivo del 2023, sull'assestamento di bilancio 2024 e sul bilancio preventivo per l'anno 2025.

3.1.2 Nucleo per la cybersicurezza

Nel 2024, il Nucleo per la cybersicurezza (NCS) ha confermato la propria funzione quale sede primaria di coordinamento interministeriale a supporto del Presidente del Consiglio in materia di cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione a eventuali situazioni di crisi e per l'attivazione di procedure per l'allertamento. A tal fine, l'NCS ha garantito uno scambio informativo tra le diverse Amministrazioni rappresentate (vedasi box), nonché con altri *stakeholder* interessati. Ciò ha permesso di mantenere un quadro situazionale aggiornato e puntuale da poter riferire, con periodicità, al vertice politico così da assistere il processo decisionale del Governo. Il Nucleo si è riunito in 10 occasioni in composizione ordinaria e 12 volte in composizione ristretta.



In tutti questi casi possono essere invitati a partecipare ulteriori soggetti, pubblici e privati, rilevanti per le specifiche trattazioni. Da inizio 2024 è in vigore il Regolamento di funzionamento del Nucleo, che ne ha meglio specificato composizione, funzioni e profili organizzativi.

In linea generale, le sedute del Nucleo hanno dato l'opportunità all'ACN di tenere costantemente aggiornate le Amministrazioni su quanto fatto dall'Agenzia in materia di monitoraggio della minaccia cyber, rafforzamento della resilienza cibernetica del Paese, attività di certificazione, cooperazione internazionale, esercitazioni e sullo stato di attuazione di rilevanti misure della Strategia nazionale di cybersicurezza. Parimenti, le diverse Amministrazioni coinvolte hanno potuto condividere dettagli in merito alle attività di prevenzione e preparazione alle situazioni di crisi, dando vita, inoltre, a uno scambio di esperienze in tema di evoluzioni normative e tecnologiche rilevanti per la cybersicurezza, nonché di formazione.

NCS allargato agli operatori privati del settore TELCO

A dicembre si è tenuta una riunione dell'NCS in composizione ordinaria allargato a quattro primarie aziende del settore delle telecomunicazioni. Nel corso dell'incontro i rappresentanti degli operatori hanno potuto illustrare il loro approccio alla cybersicurezza, le più efficaci strategie di riduzione del rischio cyber, nonché le lezioni apprese da casi studio concreti. È stata, inoltre, l'occasione per anticipare l'istituzione dell'ISAC TELCO, una struttura di scambio informativo tra gli operatori promossa dall'ACN.

Il 2024 ha visto un più ampio dispiegamento delle capacità di scambio informativo del Nucleo, che ha sfruttato appieno la facoltà di riunirsi con composizioni a geometria variabile, adattando la composizione e tenendo conto dei temi e delle necessità che di volta in volta ha dovuto affrontare. Ciò deriva sia dalla legge istitutiva e dai suoi aggiornamenti, sia da una pianificazione di sedute più dinamiche attraverso le quali coinvolgere i diversi soggetti interessati. Ai fini di potenziare le capacità dell'NCS di svolgere le sue funzioni di preparazione e prevenzione alle situazioni di crisi, nonché di attivazione delle procedure di allertamento, sono state programmate le sedute in composizione ordinaria, seguendo tre direttrici principali. In particolare, alcune riunioni sono state dedicate ad approfondire la visione del rischio cyber di ciascuna delle Amministrazioni rappresentate nel Nucleo, con una specifica attenzione ai rispettivi assetti organizzativi, *best practice* e significativi casi studio. Un'ulteriore direttrice riguarda il confronto con gli operatori privati rappresentativi dei settori più rilevanti per la cybersicurezza, a partire da quello delle telecomunicazioni (vedasi box). La terza direttrice è dedicata ad approfondimenti tematici su questioni di interesse generale, ad opera di eminenti esperti d'area, al fine di fornire al Nucleo una base condivisa di conoscenze che permetta uno scambio tanto tecnico quanto politico-strategico.

Per quanto concerne la composizione ristretta è stato convocato per la prima volta da quando è stato introdotto, con la legge n. 90/2024, il Nucleo che include, oltre ai componenti NCS, la partecipazione di rappresentanti, a livello di vertice, della Direzione nazionale antimafia e antiterrorismo e della Banca d'Italia, nonché di eventuali ulteriori soggetti interessati come quelli del Perimetro (vedasi box). In alcuni casi, inoltre, minacce e incidenti rilevanti hanno reso necessaria una pronta reazione da parte del Nucleo, coinvolgendo i soli soggetti inte-

NCS legge n. 90/2024

Nel mese di ottobre è stata convocata la prima riunione dell'NCS nella composizione introdotta dalla legge n. 90/2024, che ha previsto la partecipazione della Direzione nazionale antimafia e antiterrorismo e della Banca d'Italia. Tale seduta ha permesso di discutere rilevanti iniziative per la sicurezza informatica del Paese, inclusa la minaccia ransomware e il tema degli accessi abusivi alle banche dati digitali.

ressati. Ciò è accaduto anche a luglio 2024, quando il rilascio di un aggiornamento di un software da parte di un operatore globale ha provocato un blocco, su scala mondiale, di sistemi e servizi informatici, con forti ripercussioni anche di tipo cinetico. Infine, il Nucleo in composizione ristretta è stato riunito anche per approfondimenti specifici, anche di respiro internazionale.

ESERCITAZIONI

L'Agenzia ha continuato a dedicare significativa attenzione alle esercitazioni di cybersicurezza, che rappresentano uno strumento imprescindibile per mettere alla prova sia a livello nazionale che internazionale la resilienza cibernetica del Paese, offrendo l'opportunità di testare e affinare i meccanismi e le procedure di gestione di eventi, incidenti e crisi cyber, sul fronte tecnico e su quello operativo. Tali attività rappresentano anche un momento consolidato di rafforzamento della collaborazione interistituzionale, agevolando il coordinamento tra Ministeri e autorità nazionali, oltre a stimolare sinergie operative tra Stati e agenzie in ambito internazionale. Il Nucleo per la cybersicurezza ha un ruolo importante in questo contesto, essendo chiamato a promuovere e coordinare lo svolgimento di esercitazioni interministeriali ovvero la partecipazione a esercitazioni internazionali.

Nel 2024 le esercitazioni in ambito di cybersicurezza hanno registrato un significativo avanzamento sia in termini di frequenza che di complessità organizzativa. Questo cambio di passo riflette l'impegno crescente verso un rafforzamento delle capacità operative e una maggiore sinergia tra attori istituzionali e privati.

ESERCITAZIONI NAZIONALI

A livello nazionale, il 2024 ha segnato l'avvio di un programma di esercitazioni periodiche denominate ACN-CyEX, a cura dell'Agenzia. Tali esercitazioni sono volte a testare la preparazione di tutte le entità coinvolte nella gestione della sicurezza informatica, rafforzare la cybersicurezza della Pubblica Amministrazione, incrementare la coesione istituzionale e la collaborazione strategica interministeriale e innalzare il livello di consapevolezza sulle minacce informatiche. Ulteriore obiettivo generale di tali iniziative è rappresentato dal consolidamento dei canali di comunicazione con l'ACN, anche tramite la promozione e la familiarizzazione con gli strumenti e i servizi offerti dall'Agenzia, obiettivo particolarmente rilevante in un contesto di innovazione del panorama normativo dato dalle importanti modifiche legislative introdotte nel 2024.

La prima di queste esercitazioni, ACN-CyEX24, si è svolta a dicembre con la partecipazione di circa 50 giocatori di tutte le Amministrazioni appartenenti al Nucleo per la cybersicurezza. Nel corso della simulazione, di tipo *table-top*, i partecipanti hanno affrontato un percorso strutturato che prevedeva discussioni tematiche sulle migliori pratiche sia procedurali che tecniche in risposta al rilevamento di un incidente informatico sui loro sistemi causato dallo sfruttamento di una vulnerabilità, segnalata tramite i servizi proattivi dell'Agenzia.

L'ACN ha fornito, inoltre, un contributo all'esercitazione EXE Flegrei 2024, organizzata dal Dipartimento della protezione civile, cui ha partecipato in veste di osservatore, anche alla luce dei risvolti cibernetici che possono presentarsi nell'ambito di crisi di natura cinetica.

ESERCITAZIONI INTERNAZIONALI

In ambito Unione Europea, l'Agenzia è stata impegnata nella fase di condotta dell'esercitazione *Cyber Europe 2024*, settima edizione della principale esercitazione di gestione crisi cyber dell'UE che si svolge ogni due anni sotto il coordinamento di ENISA e vede il coinvolgimento degli Stati membri, delle istituzioni, degli organi e delle agenzie dell'Unione, nonché delle reti di collaborazione europee di gestione crisi, come EU-CyCLONe, e di gestione degli incidenti (*CSIRTs Network*). L'Agenzia, oltre alla fase di pianificazione, ha coordinato la partecipazione alla fase di gioco di 12 soggetti nazionali dei settori energia, Pubblica Amministrazione e fornitori di servizi digitali, che hanno simulato le azioni di reazione agli eventi cibernetici di uno scenario che prevedeva l'intensificarsi delle azioni ostili sino al raggiungimento di un livello di crisi a livello europeo. In tale contesto sono state anche simulate delle riunioni del Nucleo per la cybersicurezza, esteso ai citati soggetti.

A novembre 2024, l'ACN è stata protagonista dell'organizzazione e della conduzione dell'esercitazione di EU-CyCLONe denominata *BlueOLEx 24*, tenutasi per la prima volta presso la sede dell'Agenzia, sulla base dello scenario promosso da ENISA. L'esercitazione, appuntamento annuale di vertice della rete, è finalizzata alla verifica delle modalità di interazione interne a CyCLONe, al rafforzamento della fiducia e della collaborazione tra i membri partecipanti, con l'obiettivo di predisporre una risposta altamente coordinata in caso di crisi. Durante l'esercitazione è stato giocato uno scenario collegato con quello della *Cyber Europe 2024*, simulando la gestione di una crisi cibernetica scatenata da attacchi coordinati alle infrastrutture del settore energetico negli Stati membri. I rappresentanti delle agenzie europee hanno avuto modo di testare la preparazione dell'UE in caso di crisi cyber, rafforzando i meccanismi di collaborazione a livello comunitario.

L'Agenzia ha, inoltre, partecipato all'esercitazione *EU Integrated Resolve 2024* (esercizio congiunto condotto dal Consiglio dell'UE, dalla Commissione europea e dal Servizio europeo per l'azione esterna) a supporto dell'Ufficio del Consigliere militare del Presidente del Consiglio dei ministri, che ha coordinato la partecipazione nazionale all'evento. L'esercitazione mirava a testare la preparazione e la capacità dell'UE di rispondere a crisi complesse di natura ibrida con dimensioni interne ed esterne tramite uno scenario di crisi multilivello. L'Agenzia, in risposta a determinati eventi cibernetici simulati, ha avuto modo di rafforzare le interazioni e la cooperazione con gli altri Stati membri.

L'Agenzia ha dato anche il proprio contributo all'esercitazione annuale di tipo *table-top*, svoltasi su impulso del Servizio europeo per l'azione esterna, per verificare l'applicazione del *Cyber Diplomacy Toolbox* e rafforzare la comunicazione strategica dell'azione dell'UE, al fine di migliorare la capacità di risposta collettiva alle attività cyber malevole.

A livello internazionale, in ambito NATO, l'ACN continua il suo impegno nelle attività correlate alla pianificazione dell'esercitazione strategico-procedurale *Crisis Management Exercise*, fornendo 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). A tale riguardo, anche nel 2024 l'Agenzia ha preso parte all'esercitazione denominata *Short Notice Exercise*.

Inoltre, di concerto con il Ministero della difesa, l'Agenzia ha dato il proprio contributo alla pianificazione ed esecuzione, relativamente ai profili di *cyber threat intelligence* e *situational awareness*, delle principali esercitazioni di tipo *cyber-range* organizzate dal *NATO Cooperative Cyber Defence Centre of Excellence* di Tallinn (Estonia), denominate rispettivamente *Locked Shields* e *Crossed Swords*. Per quest'ultima, in particolare, si è registrata la vittoria del team nazionale, con la partecipazione del personale dell'Agenzia, che si è classificato primo tra i c.d. *yellow team*, ovvero quelli incaricati dell'analisi delle attività offensive contro i sistemi e le infrastrutture di gara.

In ambito G7, l'Agenzia ha partecipato all'esercitazione del settore finanziario *Cross-Border Coordination Exercise*, inquadrata tra le attività previste dal *Cyber Expert Group*, gruppo di esperti di sicurezza informatica composto da rappresentanti delle autorità finanziarie dei Paesi del G7 e dell'Unione europea. L'esercitazione, la cui pianificazione nazionale è stata coordinata dalla Banca d'Italia, prevedeva la simulazione di una crisi ingenerata da attacchi cyber alle istituzioni finanziarie di Paesi del G7, con ripercussioni globali sui mercati e sull'operatività di gruppi bancari. Il personale dell'Agenzia è stato impegnato nella pianificazione ed esecuzione tramite il CSIRT Italia e con elementi di raccordo in seno al CODISE (struttura deputata al coordinamento delle crisi operative della piazza finanziaria italiana, presieduta dalla Banca d'Italia).

Nell'ambito dell'iniziativa multilaterale guidata dagli Stati Uniti, denominata *Counter Ransomware Initiative*, volta a combattere la minaccia del *ransomware* attraverso la cooperazione internazionale, l'ACN ha partecipato a un'esercitazione di livello strategico volta a simulare un attacco *ransomware* al settore sanitario negli oltre 50 Paesi partecipanti, con lo scopo di testare l'attivazione dei rispettivi processi e procedure di risposta.

3.1.3 Tavolo interministeriale per l'attuazione del Perimetro di sicurezza nazionale cibernetica

Il Tavolo interministeriale per l'attuazione del Perimetro di sicurezza nazionale cibernetica (c.d. Tavolo Perimetro) è istituito presso l'ACN e presieduto dal Direttore generale, per assicurare il raccordo tra le Amministrazioni impegnate, a vario titolo, nell'attuazione del Perimetro. In particolare, il Tavolo opera a supporto del CIC, specie in relazione all'individuazione delle reti, dei sistemi informativi e dei servizi informatici da cui dipende l'esercizio di una funzione essenziale o l'erogazione di un servizio essenziale dello Stato e dal cui malfunzionamento, interruzione, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Ciò permette di identificare i soggetti che erogano tali servizi ed esercitano tali funzioni per la loro inclusione nel Perimetro.

Nel corso delle riunioni, tenutesi nei mesi di marzo e ottobre, il Tavolo ha deliberato in merito alle proposte – sottoposte dalle Amministrazioni competenti per il settore governativo, nonché per i vari settori di attività (vedasi box) – riguardanti l'aggiornamento dell'elenco dei soggetti inclusi nel Perimetro, in risposta sia a sviluppi sul piano tecnico, sia a variazioni relative agli assetti societari. A seguito dell'adozione da parte del Presidente del Consiglio dei ministri, su proposta del CIC, dell'atto amministrativo che recepisce il citato aggiornamento, il numero di soggetti iscritti nell'elenco Perimetro è passato da 118 a 116 (anche a seguito di alcune fusioni per incorporazione).

Amministrazioni competenti per settori di attività PSNC

Interno	**Difesa**	**Spazio e aerospazio**	**Energia**	**Telecomunicazioni**
Ministero dell'interno	Ministero della difesa	Presidenza del Consiglio dei ministri	Ministero dell'ambiente e della sicurezza energetica	Ministero delle imprese e del *made in Italy*
Economia e finanza	**Trasporti**	**Servizi digitali**	**Tecnologie critiche**	**Enti previdenziali/lavoro**
Ministero dell'economia e delle finanza	Ministero delle infrastrutture e dei trasporti	Ministero delle imprese e del *made in Italy*, in raccordo con la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione	Struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione, in raccordo con il MIMIT e il MUR	Ministero del lavoro e delle politiche sociali

3.1.4 Tavolo per l'attuazione della disciplina NIS

Il Tavolo per l'attuazione della disciplina NIS (c.d. Tavolo NIS) è stato istituito con l'entrata in vigore del già citato decreto NIS2, che recepisce l'omonima direttiva (vedasi Capitolo 1). Il Tavolo, costituito in via permanente presso l'Agenzia e presieduto dal suo Direttore generale, è composto dai rappresentanti delle 9 Autorità di settore (vedasi box) e da due rappresentanti designati da Regioni e Province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. La legge prevede che il Tavolo NIS sia sempre sentito nell'iter di adozione dei provvedimenti attuativi del decreto NIS2, come effettivamente avvenuto nella riunione di insediamento del 2024 in cui il Tavolo NIS è stato sentito sui primi provvedimenti attuativi che riguardano l'organizzazione e funzionamento del Tavolo stesso, nonché le modalità di accesso alla piattaforma per la registrazione dei soggetti e le informazioni aggiuntive che gli stessi devono condividere. Il Tavolo si è pronunciato, inoltre, sul già citato provvedimento relativo all'applicazione della c.d. clausola di salvaguardia in ambito NIS2, poi sottoposto al CIC.

Autorità di settore NIS2

- Presidenza del Consiglio dei ministri
- Ministero dell'economia e delle finanze
- Ministero delle imprese e del *made in Italy*
- Ministero dell'agricoltura, della sovranità alimentare e delle foreste
- Ministero dell'ambiente e della sicurezza energetica
- Ministero delle infrastrutture e dei trasporti
- Ministero dell'università e della ricerca
- Ministero della cultura
- Ministero della salute

Il coinvolgimento del Tavolo consente di assicurare l'integrazione delle competenze espresse dalle Autorità di settore nel complesso processo di attuazione della disciplina NIS, tenendo conto anche dell'impatto a livello locale, per i settori di interesse delle Regioni e delle Province autonome. Rilevante è anche il ruolo dei tavoli, previsti dal decreto NIS2, coordinati e promossi dalle diverse Autorità di settore, quali "camere di compensazione" tra il contesto governativo e i soggetti privati, tavoli che consentono un confronto diretto tra tutte le parti, compresa l'ACN, al fine di promuovere, in particolare, il dialogo con i soggetti sulle modalità di realizzazione degli adempimenti e raccogliere eventuali elementi funzionali a una migliore applicazione della NIS2.

3.2 RAPPORTI CON IL PARLAMENTO E ALTRE ATTIVITÀ

L'ACN continua a portare avanti un'intensa collaborazione con il Parlamento, secondo la logica della massima responsabilizzazione dell'Agenzia, il cui operato deve rispondere alle esigenze del Paese tutto, tutelate dal rappresentante della sovranità popolare.

Il Parlamento ha, infatti, richiesto in più occasioni il coinvolgimento dell'ACN nelle sue attività, anche attraverso audizioni nelle quali il Direttore generale ha potuto rappresentare gli elementi disponibili dall'osservatorio dell'Agenzia. In questo ambito l'ACN ha anche assicurato la propria partecipazione a eventi istituzionali sui temi della cybersicurezza e dell'innovazione tecnologica con lo scopo di rendere il proprio contributo al dibattito in seno al legislatore. Inoltre, l'ACN ha supportato il Governo nella risposta agli atti di sindacato ispettivo con profili in materia di cybersicurezza, fornendo gli elementi di competenza.

Nella più ampia attività di produzione normativa, si è registrato poi un ampliamento del coinvolgimento dell'Agenzia, anche attraverso la richiesta di espressione di pareri, ai fini di sviluppi normativi che contemplassero i profili di cybersicurezza all'interno di provvedimenti relativi alla digitalizzazione del Paese. L'anno in esame è stato contraddistinto, infine, da un'intensa attività istituzionale dell'Agenzia che ha permesso di rafforzarne il posizionamento, promuovendo e consolidando il rapporto privilegiato con organi costituzionali, enti pubblici, organizzazioni governative, associazioni di categoria, imprese e altri *stakeholder* pubblici e privati.

3.2.1 Audizioni

L'Agenzia ha contribuito in maniera puntuale alle attività conoscitive e di formazione legislativa svolte all'interno delle Commissioni parlamentari con 6 audizioni del Direttore generale. Tali audizioni hanno permesso di poter contribuire con la propria *expertise* ai principali provvedimenti in materia cyber in esame nel 2024. L'ACN ha così potuto dare il proprio apporto alla definizione di una cornice normativa coerente con l'architettura nazionale di cybersicurezza, intervenendo, in particolare, nell'ambito dei lavori parlamentari che hanno portato all'approvazione della legge n. 90/2024. È stata, altresì, interessata nell'attività discendente della normativa comunitaria, con audizioni nell'ambito del procedimento legislativo di recepimento della Direttiva NIS2, nonché nel procedimento per la legge di delegazione europea 2024. Infine, l'Agenzia è intervenuta in audizione sul Disegno di legge recante disposizioni e delega al Governo in materia di intelligenza artificiale, oltre che in due indagini conoscitive che hanno riguardato la difesa cibernetica e la semplificazione e digitalizzazione delle procedure amministrative.

Audizioni

Commissione Affari costituzionali della Camera dei deputati

- AC 1717 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"

Commissione Difesa della Camera dei deputati

- Indagine conoscitiva sulla difesa cibernetica

Commissione Trasporti della Camera dei deputati

- AG 164 "Schema di decreto legislativo recante recepimento della direttiva (UE) 2022/2555"

Commissioni congiunte Ambiente e Affari sociali del Senato della Repubblica

- AS 1146 "Disposizioni e delega al Governo in materia di intelligenza artificiale"

Commissione Politiche dell'Unione europea del Senato della Repubblica

- AS 1258 "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea"

Commissione parlamentare per la semplificazione

- Indagine conoscitiva in materia di semplificazione e digitalizzazione delle procedure amministrative nei rapporti tra cittadino e Pubblica Amministrazione

L'ACN è, inoltre, sottoposta al controllo del Comitato parlamentare per la sicurezza della Repubblica (COPASIR) per le funzioni svolte a tutela della sicurezza nazionale nello spazio cibernetico. In tale contesto, il Presidente del Consiglio trasmette una relazione al COPASIR sull'attività svolta nell'anno precedente dall'ACN negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del Comitato. A ciò si aggiunge la facoltà del COPASIR di audire, in qualunque momento, il Direttore generale dell'Agenzia, facoltà che è stata esercitata una volta nel 2024.

3.2.2 Attività a supporto di una digitalizzazione sicura

L'ACN è stata chiamata a fornire il contributo di competenza in relazione agli aspetti di cybersicurezza coinvolti nel processo di trasformazione digitale dei processi e dei servizi della Pubblica Amministrazione. Un'efficace transizione verso una PA digitale, sicura e interoperabile richiede, infatti,

che vengano garantiti elementi fondamentali di cybersicurezza, specialmente nella creazione di piattaforme digitali a servizio dei cittadini. In questo contesto l'ACN, oltre a fornire il supporto per i profili di competenza al Piano triennale per l'informatica nella Pubblica Amministrazione e alle attività discendenti, ha reso i seguenti pareri e contributi.

Ecosistema dati sanitari

La cybersicurezza assume particolare importanza con riferimento ai dati sanitari, poiché incide necessariamente sul diritto alla salute e alla riservatezza di ciascun cittadino. Il Ministero della salute è chiamato a curare la realizzazione dell'Ecosistema dei dati sanitari (EDS), d'intesa con la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale, assicurando l'adeguatezza delle infrastrutture tecnologiche e la sicurezza cibernetica in raccordo con l'ACN. A tal fine, l'Agenzia fornisce il parere di competenza rispetto al provvedimento che individua i contenuti, le modalità di alimentazione e i soggetti che hanno accesso all'EDS, nonché le operazioni eseguibili e le misure di sicurezza per assicurare i diritti degli interessati.

Piattaforma Piracy Shield

Si è reso opportuno un coinvolgimento dell'Agenzia nella realizzazione della piattaforma per il contrasto alla pirateria online riferita agli eventi sportivi in diretta. Al riguardo, per i profili di competenza l'ACN collabora con l'AGCOM (Autorità per le garanzie nelle comunicazioni) nel Tavolo tecnico finalizzato a definire i requisiti tecnici e operativi degli strumenti necessari a consentire una tempestiva ed efficace disabilitazione dei nomi di dominio o degli indirizzi IP, attraverso la messa a punto di una piattaforma tecnologica unica con funzionamento automatizzato per tutti i destinatari dei provvedimenti di disabilitazione. A tale Tavolo partecipano i prestatori di servizi, i fornitori di accesso alla rete Internet, i detentori di diritti, i fornitori di contenuti, i fornitori di servizi di media audiovisivi e le associazioni maggiormente rappresentative preposte alla tutela del diritto d'autore e dei diritti connessi. La piattaforma Piracy Shield, gestita da AGCOM, è attiva dal febbraio 2024.

Sistema di portafoglio digitale italiano
Sistema IT-Wallet

L'ACN è stata chiamata a esprimere un parere sull'attuazione del sistema di portafoglio digitale italiano, IT-Wallet. Tale sistema prevede che siano adottate apposite Linee guida tecniche per definire, oltre alle modalità di accreditamento dei soggetti privati e agli standard tecnici di interoperabilità delle soluzioni, le misure da adottare per assicurare livelli di affidabilità, disponibilità e sicurezza adeguati. L'ACN ha, quindi, partecipato attivamente al gruppo di lavoro interistituzionale che coinvolge DTD, AgID, nonché PagoPA e Istituto Poligrafico e Zecca dello Stato (IPZS), per la stesura delle Linee guida, fornendo supporto per i temi di propria competenza.

Relativamente agli aspetti di cybersicurezza e di certificazione, l'ACN ha presidiato i gruppi di lavoro istituzionali nazionali suggerendo un approccio che includesse quanto più possibile i requisiti del già citato EUDI Wallet all'interno delle Linee guida di IT-Wallet. Tale approccio ha lo scopo di ridurre al minimo le rilavorazioni di tipo tecnico e di governance per ottenere il futuro accreditamento di IT-Wallet a livello europeo. Inoltre, l'ACN si è adoperata nell'ottica dell'armonizzazione con le altre normative nazionali ed europee illustrate nel Capitolo 1 (CSA, Direttiva NIS2, legge n. 90/2024, PSNC e Regolamento cloud per la PA).

3.2.3 Tavolo di coordinamento per l'internazionalizzazione delle imprese cyber

Oltre al rapporto con la macchina pubblica, l'Agenzia attribuisce particolare attenzione al confronto con il settore privato e al sostegno alle imprese. In tale ambito, l'ACN insieme al MAECI si è fatta promotrice dell'istituzione del Tavolo di coordinamento per l'internazionalizzazione delle imprese cyber. L'iniziativa, volta a rafforzare la presenza delle aziende nazionali sui mercati esteri, anche in Paesi avanzati, è stata lanciata a novembre 2024 con un evento che ha visto la partecipazione del MAECI, del MIMIT, dell'Agenzia ICE e di circa 90 operatori privati.

> ***Misura #50 della Strategia nazionale di cybersicurezza***
>
> *Promuovere l'internazionalizzazione delle imprese italiane che offrono prodotti e servizi di cybersecurity mediante il supporto agli investimenti, all'innovazione e alle esportazioni.*

Le imprese sono state attivamente coinvolte raccogliendone le esigenze rispetto alla proiezione all'estero del comparto tecnologico nazionale, anche attraverso l'individuazione di strumenti di sostegno all'*export* e la promozione dell'immagine del Paese come eccellenza tecnologica. Il Tavolo faciliterà la partecipazione, nella prima metà del 2025, di istituzioni e aziende selezionate alla *RSA Conference* di San Francisco, la più importante conferenza-esposizione mondiale sulla *cybersecurity*.

3.2.4 Accordi di collaborazione

L'ACN ha continuato a stipulare accordi di collaborazione con soggetti pubblici e privati con lo scopo di rafforzare la sicurezza e la resilienza cibernetiche, lo scambio di informazioni e la formazione in ambito cyber. Questi hanno permesso di perseguire, in particolare, tre linee d'indirizzo: rafforzare i rapporti internazionali con le agenzie cyber di altri Stati, il rapporto con le altre Amministrazioni pubbliche e gli spazi di cooperazione pubblico-privato.

In ambito internazionale, l'ACN ha sottoscritto nuovi protocolli d'intesa con Romania, Spagna, Governatorato dello Stato della Città del Vaticano e Albania e dato inizio a negoziati con altri Paesi importanti per la proiezione all'estero dell'Agenzia (vedasi Capitolo 6).

Quanto agli accordi conclusi con le Pubbliche Amministrazioni, è di particolare rilievo quello con il Ministero dell'istruzione e del merito che ha l'obiettivo di promuovere l'educazione informatica e cibernetica nelle scuole italiane di ogni ordine e grado. Inoltre, dando seguito alle modifiche legislative intervenute nel corso del 2024, l'accordo tra l'ACN, la Direzione nazionale antimafia e antiterrorismo e il Dipartimento della pubblica sicurezza ha permesso un efficace e costante allineamento informativo, necessario per consentire il corretto esercizio delle funzioni attribuite dalla legge.

Sono state, inoltre, stipulate le intese speditive previste dalla Direttiva del Presidente del Consiglio dei ministri del 29 dicembre 2023 in materia di resilienza cibernetica, con le Amministrazioni CIC ai fini di elevarne la postura cyber e la collaborazione con l'Agenzia in un'ottica di resilienza.

La cooperazione pubblico-privato si è esplicata con accordi con organizzazioni che operano nel campo della formazione (Università Bocconi, Fondazione Ugo Bordoni, Rete Fondazioni ITS Italia, SPES Academy Carlo Azeglio Ciampi), nonché con aziende attive nei settori d'interesse per l'Agenzia con lo scopo di consolidare la collaborazione con gli operatori economici (CDP Venture Capital SGR, Consorzio NAMEX, Google Cloud Italy, Trend Micro Italy).

3.2.5 Eventi e consessi informali

Il 2024 ha confermato un notevole dinamismo da parte dell'Agenzia in favore della sua più ampia comunità di *stakeholder* partecipando, a livello di vertice, a oltre 90 incontri con operatori privati e 66 eventi organizzati da associazioni, università e aziende.

Evento NIS2

Di particolare rilievo è stata l'organizzazione di un evento, organizzato in collaborazione con Sapienza Università di Roma, finalizzato a informare le diverse comunità interessate sulla nuova disciplina NIS. L'evento, in un'ottica di accompagnamento dei soggetti coinvolti nell'attuazione delle nuove norme, ha fornito l'occasione per promuovere la visibilità dell'entrata in vigore del decreto legislativo di recepimento della Direttiva NIS2 e della prima scadenza per i soggetti (l'obbligo di registrazione sulla piattaforma NIS messa a disposizione dall'Agenzia). L'evento, a cui sono intervenuti i responsabili della cybersicurezza delle maggiori aziende del Paese oltre a rappresentanti del mondo imprenditoriale, universitario e delle PA, ha visto la partecipazione di oltre 2.000 persone in presenza e online, essendo stato trasmesso in diretta *streaming*. Questo si pone in linea di continuità con l'evento, organizzato insieme a Confindustria già prima del recepimento della Direttiva NIS2, dal titolo "Verso la NIS – Dialogo con ACN sulle principali novità", con il quale l'Agenzia ha voluto interfacciarsi con il mondo produttivo e associativo.

L'Agenzia si è fatta, inoltre, promotrice di iniziative dedicate alla consapevolezza cyber, tra cui rivestono un ruolo importante gli eventi dedicati alle PMI, anche in collaborazione con Confindustria, nonché quelli focalizzati sul settore sanitario (vedasi Capitolo 7).

L'ACN ha contribuito anche all'organizzazione della *European Cybersecurity Challenge*, la prima edizione del campionato europeo di cybersicurezza svoltasi in Italia. L'iniziativa è stata organiz-

zata congiuntamente dall'Agenzia e dal *Cybersecurity National Lab* del CINI (Consorzio interuniversitario nazionale per l'informatica) che hanno anche accompagnato a Palazzo Chigi la nazionale italiana di *cyberdefender* prima dell'avvio della competizione (vedasi box).

La partecipazione agli eventi ha permesso all'ACN di aprirsi ad attori cruciali per raggiungere gli obiettivi di cybersicurezza, come le Pubbliche Amministrazioni locali. Si segnalano in questo ambito le attività svolte con l'Associazione nazionale dei Comuni italiani (ANCI) che hanno visto la presenza dell'Agenzia all'Assemblea annuale dell'ANCI a Torino, dove è stato anche allestito uno *stand* ACN, e a "Missione Italia", l'appuntamento dedicato al PNRR di Comuni e città per fare il punto sullo stato degli investimenti e sulle riforme che li accompagnano. L'Agenzia ha anche assicurato la propria qualificata presenza a ForumPA, nonché ad eventi primari nell'ambito della cybersicurezza, quali CyberSEC2024, ITASEC2024, Roma Digital Summit e ComoLake.

European Cybersecurity Challenge

Torino, 7-12 ottobre

Il campionato europeo di cybersicurezza, European Cybersecurity Challenge, organizzato annualmente da ENISA, è la competizione dedicata a squadre di giovani (14-24 anni) cyberdefender che si sfidano in una serie di prove di sicurezza informatica. Al campionato hanno preso parte i team di 37 Paesi, UE ed extra-UE.

Nell'ambito dell'evento si sono tenute anche delle sessioni dedicate alla promozione e allo sviluppo delle startup della rete nazionale del Cyber Innovation Network (vedasi Capitolo 5).

Con l'obiettivo di ampliare la rete di rapporti con le comunità *multi-stakeholder* sul tema della *governance* globale della cybersicurezza, l'Agenzia ha partecipato a diversi eventi e conferenze internazionali in cui si è discusso di temi di politica cyber, inclusi la *Munich Cyber Security Conference*, la *Prague Security Conference*, la *RSA Conference* di San Francisco, il *Paris Cyber Summit* e il *Global Cybersecurity Forum* di Riad.

L'ACN partecipa, infine, a *network* informali come quello dei DPO delle Autorità indipendenti, un foro di discussione costituito nel 2018, e allargato ad altri soggetti, per discutere i temi della cybersicurezza, della *privacy* e dell'interoperabilità delle banche dati. Il *network*, che si riunisce con cadenza mensile, rappresenta uno spazio per garantire la legittimità e la coerenza dell'azione amministrativa assicurata dai *matter experts* delle varie Autorità.

4.

LA SICUREZZA TECNOLOGICA: ELEMENTO CHIAVE PER PROTEGGERE LA SUPERFICIE DIGITALE DEL PAESE

L'Agenzia per la cybersicurezza nazionale annovera tra i propri compiti la verifica che gli strumenti tecnologici in uso nel Paese rispettino adeguati standard di sicurezza. Ciò costituisce un presupposto imprescindibile per proteggere la superficie digitale italiana, particolarmente per quel che riguarda i componenti ICT impiegati da soggetti critici in quanto una minaccia cyber ai loro danni potrebbe avere ripercussioni gravi per il sistema Paese nel suo complesso. Per questo motivo, l'ACN è incaricata di condurre lo scrutinio tecnologico a tutela del Perimetro di sicurezza nazionale cibernetica, nel cui alveo ricadono reti, sistemi informativi e servizi informatici cruciali per il Paese la cui compromissione potrebbe costituire una minaccia per la sicurezza nazionale.

La valutazione della rispondenza di determinate tecnologie a un adeguato livello di cybersicurezza si estende anche alla migrazione delle Pubbliche Amministrazioni al *cloud* al fine di assicurare che tale processo possa avvenire in sicurezza, ancor più per le PA che gestiscono dati di particolare rilievo. Tuttavia, la sicurezza tecnologica non è solo questione che riguarda i soggetti critici, ma deve estendersi a tutti i prodotti e servizi di largo impiego, affinché possa essere minimizzato il rischio tecnologico per il Paese. In quest'ottica l'Agenzia svolge anche le funzioni di Autorità nazionale di certificazione della cybersicurezza e di Organismo di certificazione della sicurezza informatica (OCSI). In questa veste, rilascia certificati la cui valenza travalica anche i confini nazionali. L'ACN è, inoltre, impegnata a seguire le più recenti innovazioni tecnologiche per far sì che verifiche e certificazioni siano sempre aggiornate rispetto ai più recenti sviluppi della minaccia.

4.1 SCRUTINIO TECNOLOGICO PER IL PSNC

Il Centro di valutazione e certificazione nazionale (CVCN), istituito presso l'Agenzia, si occupa dello scrutinio tecnologico previsto dalla normativa sul Perimetro di sicurezza nazionale cibernetica. Le attività di scrutinio tecnologico condotte dal CVCN nel corso del 2024 (Figura 1) si sono attestate su volumi coerenti con quelli dell'anno precedente, con l'avvio di 171 procedimenti e la conclusione di 135. Per una corretta lettura dei dati di seguito riportati, si noti che in entrambi gli anni si sono verificati dei trascinamenti dagli anni precedenti.

Un notevole incremento si è, invece, registrato sul numero di procedimenti approvati a seguito di test, che sono passati da circa 1/10 a 1/4 del totale (un aumento del 193%). L'esecuzione di test, inoltre, ha consentito di accrescere il catalogo dei prodotti valutati, a disposizione dei soggetti del PSNC.

A fine 2024, infatti, nel catalogo erano presenti 47 prodotti, di cui 33 analizzati con un livello di severità "alto", 9 "medio-alto" e 5 "medio-basso". Il livello di severità dei test indica la profondità di analisi delle prove di sicurezza e di intrusione condotte nel corso della valutazione e corrisponde a diversi profili di attaccante in termini di risorse e motivazione. Il CVCN, infatti, modula il livello di severità dei test sulla base dell'analisi del rischio elaborata e condivisa dai soggetti PSNC, nonché dell'ambiente di esercizio.

La presenza di un prodotto nel catalogo implica che su quel prodotto non saranno ripetuti test già eseguiti, ferma restando la possibilità di condurre un test integrativo a un livello di severità superiore o su elementi rilevanti nello specifico contesto d'impiego, ove non già considerati. Nel corso del 2024, per questo motivo, 10 procedimenti sono stati chiusi con prescrizioni tratte dall'esito di test effettuati in precedenza (parte dei 44 "approvati a seguito di test").

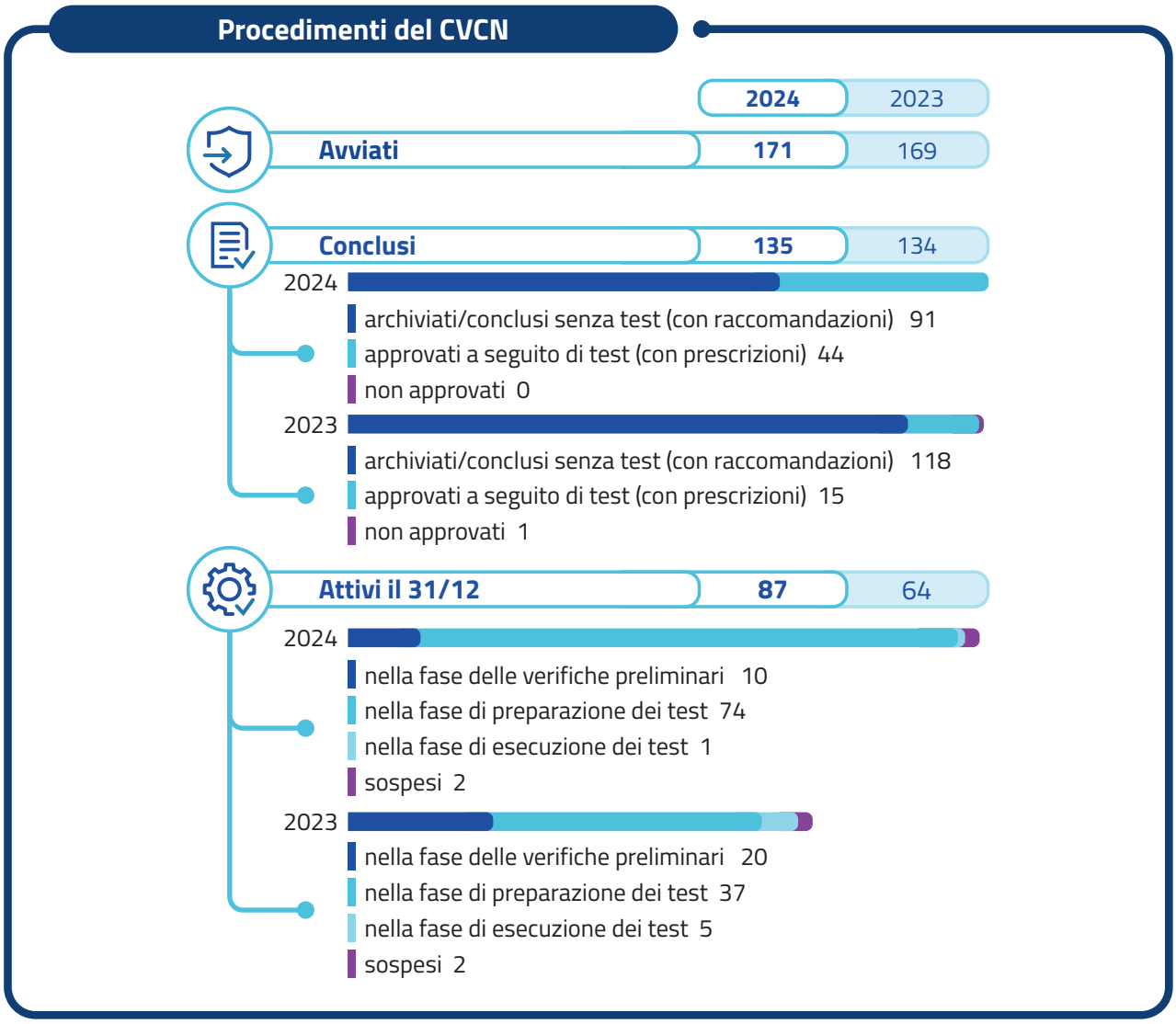


Figura 1 – Stato dei procedimenti in esame da parte del CVCN

In tale contesto, l'Agenzia ha dedicato particolare attenzione alla messa a punto di modalità di accelerazione delle attività di scrutinio che risultassero funzionali a ridurre le tempistiche dei procedimenti, così da garantire un corretto bilanciamento tra le fondamentali necessità di sicurezza a tutela del Paese e l'esigenza di rapidità degli approvvigionamenti, anche alla luce della costante evoluzione tecnologica delle infrastrutture. Il CVCN, in ambito istruttorio, ha pertanto sperimentato una procedura di *triage* grazie alla quale è possibile concludere sollecitamente procedimenti che prefigurano un rischio potenzialmente maggiore per la sicurezza nazionale e quindi postulano, oltre che una maggiore attenzione, una esigenza di più rapida definizione.

I procedimenti del CVCN hanno per oggetto le diverse categorie di beni coperte dalla disciplina Perimetro. Nel 2024 i procedimenti avviati hanno riguardato prevalentemente componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione e quelle che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati, come riportato in Figura 2.

È importante rilevare, per dar conto della significativa valenza delle attività di scrutinio riguardo al tema della prevenzione e della protezione della superficie digitale, come nel corso delle analisi

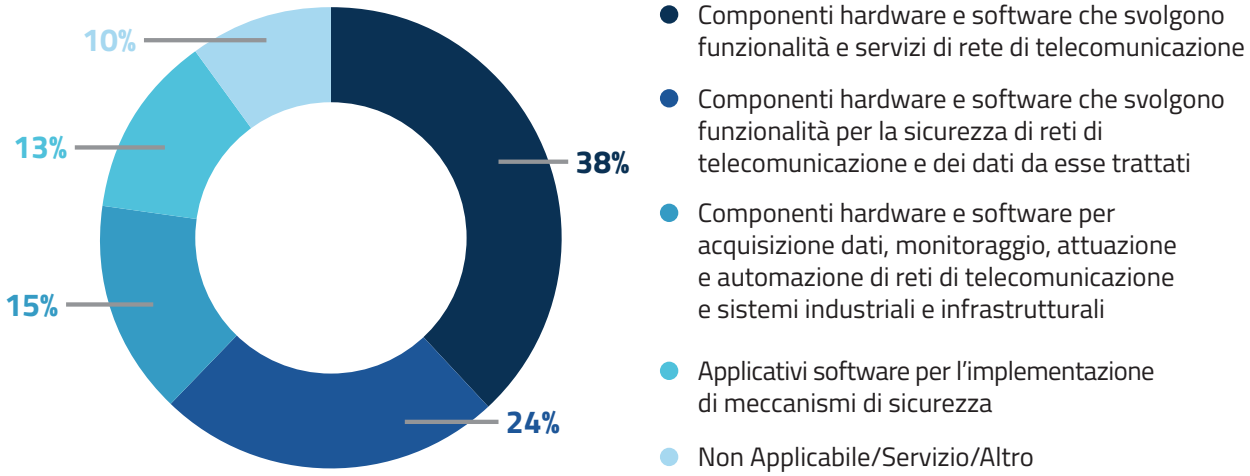


Figura 2 – Procedimenti avviati dal CVCN nel 2024 per categoria

siano state riscontrate diverse vulnerabilità, di cui alcune note (già identificate con codice CVE) e altre identificate per la prima volta dal CVCN (c.d. vulnerabilità *zero-day*). Queste ultime sono state complessivamente 40 (nel 2023 erano state 38), 25 delle quali con gravità alta o critica (Figura 3), secondo una classificazione internazionale (*Common Vulnerability Scoring System*) che prende in considerazione i possibili impatti e la facilità di sfruttamento. I dettagli delle vulnerabilità *zero-day* sono stati condivisi con il CSIRT Italia, nonché con i produttori, nell'attuazione del processo di *responsible disclosure* adottato da ACN (vedasi box). Nei casi in cui è stata identificata una vulnerabilità sono state studiate e prescritte misure di mitigazione volte a consentire l'impiego in sicurezza degli apparati analizzati all'interno del PSNC.

CVE

Il codice CVE (Common Vulnerabilities and Exposures) è un identificatore univoco, universalmente riconosciuto, assegnato a una vulnerabilità specifica in un componente software o hardware. Ogni CVE contiene una breve descrizione del problema di sicurezza e un identificativo, che aiuta a catalogare e comunicare le vulnerabilità in modo standardizzato.

Il programma CVE è gestito dal MITRE, un'organizzazione no-profit statunitense che si occupa di mantenere e aggiornare questo database. MITRE è l'autorità "radice" (c.d. CNA-CVE Numbering Authority) e può delegare la gestione delle CVE ad altre CNA più specifiche come, ad esempio, ENISA e i produttori stessi.

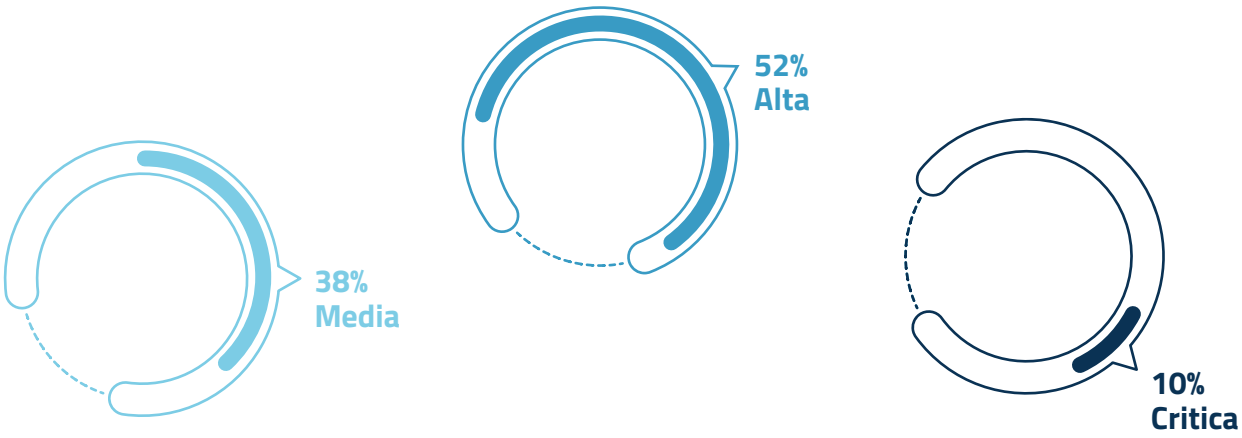


Figura 3 – Gravità delle vulnerabilità *zero-day* individuate

Delle vulnerabilità *zero-day* riscontrate, 14 sono state già corrette dal produttore (e i dettagli tecnici pubblicati con CVE), 18 sono state riconosciute e sono in corso di risoluzione da parte del produttore, mentre per le restanti 8 vulnerabilità le interlocuzioni sono ancora in corso (Figura 4).

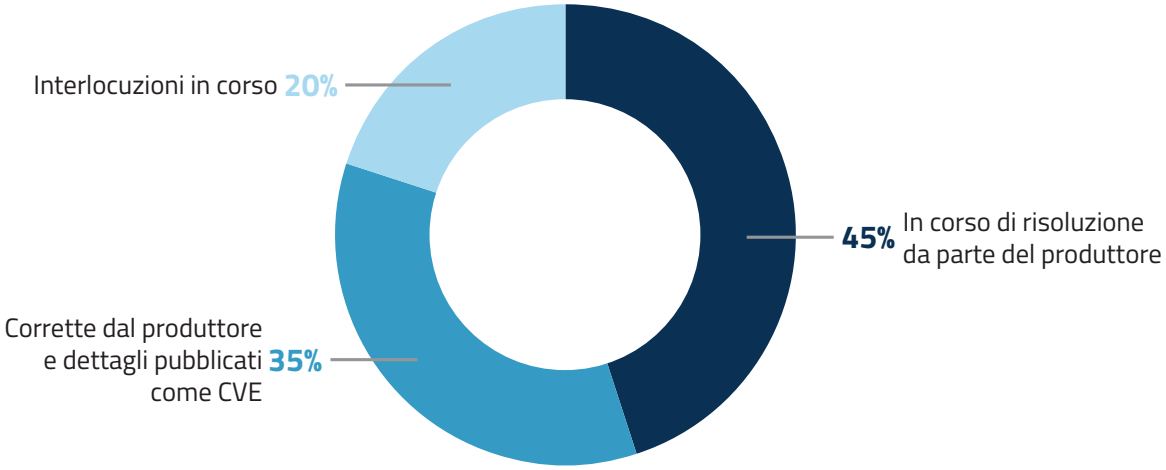


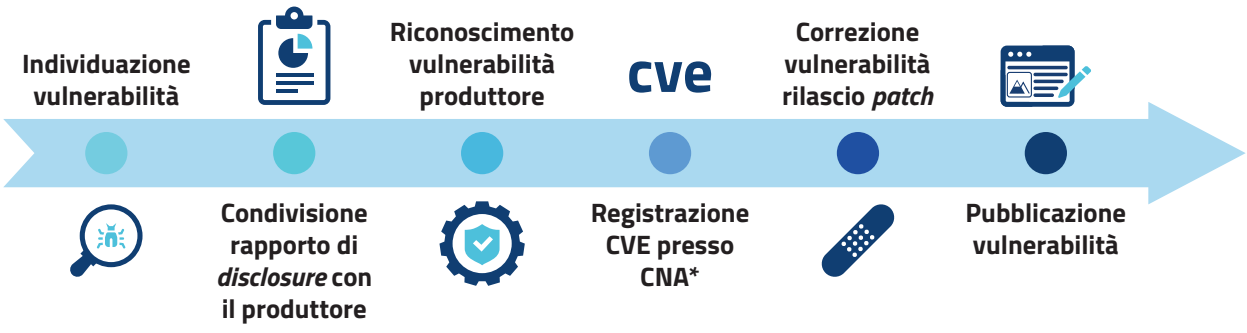
Figura 4 – Stato delle vulnerabilità *zero-day* individuate

Responsible vulnerability disclosure

La divulgazione responsabile delle vulnerabilità (c.d. responsible vulnerability disclosure) è un processo che prevede la segnalazione di vulnerabilità di sicurezza informatica ai produttori dei software o dei dispositivi in modo cooperativo e riservato. L'obiettivo è permettere a queste entità di correggere le vulnerabilità prima che possano essere sfruttate da malintenzionati.

Quando il CVCN scopre una vulnerabilità non nota, la comunica privatamente e tramite canali sicuri al produttore, dandogli il tempo necessario per risolvere il problema. Solo dopo che la vulnerabilità è stata corretta, l'informazione viene resa pubblica, garantendo così la sicurezza degli utenti e dei sistemi.

La procedura di *responsible vulnerability disclosure*

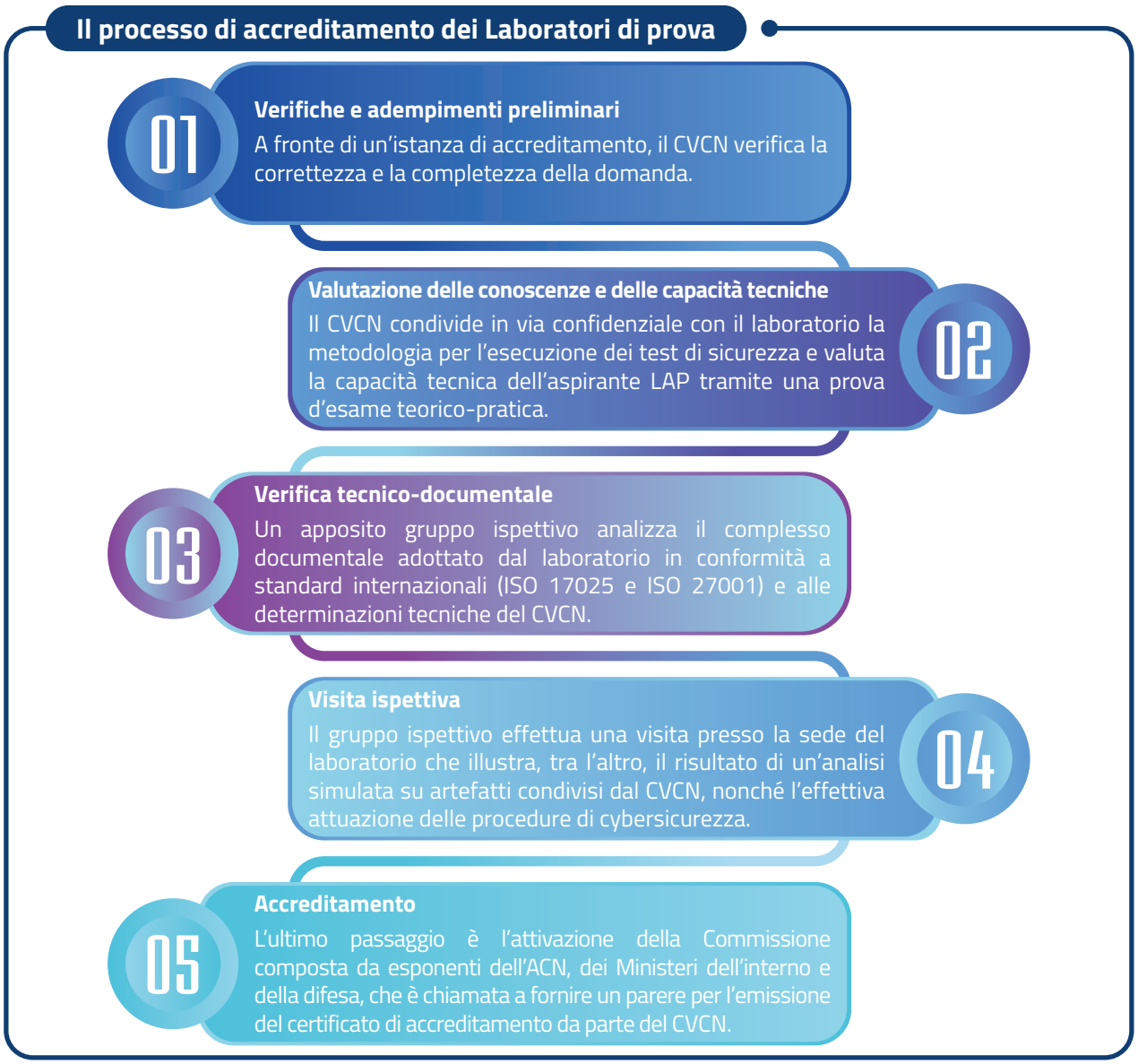


**CVE Numbering Authority: organizzazioni, autorizzate dal MITRE, che rilasciano gli identificativi CVE*

4.1.1 La rete dei laboratori a sostegno del PSNC

Il 2024 è stato un anno particolarmente intenso per quanto riguarda le attività del CVCN in materia di accreditamento dei Laboratori di prova (LAP). L'attivazione di una rete di laboratori esterni a supporto delle attività di scrutinio tecnologico dell'Agenzia è stata, peraltro, oggetto di mirate iniziative finanziate con fondi del PNRR (vedasi Capitolo 5).

Il processo di accreditamento di un laboratorio di prova è particolarmente sfidante sia per i laboratori, sia per il CVCN stesso, considerato che i requisiti soggettivi e di capacità professionale richiesti ai LAP sono molto stringenti, dovendo operare in un contesto legato alla sicurezza nazionale cibernetica.



I LAP possono essere accreditati a diversi livelli, a seconda della severità dei test che possono eseguire a supporto del CVCN. Mentre il livello alto è prerogativa del CVCN e dei Centri di valutazione (CV) del Ministero della difesa e del Ministero dell'interno, i LAP possono ricevere un certificato di accreditamento di livello medio-alto, medio-basso o basso (Figura 5), in funzione del potenziale di attacco che il laboratorio potrà essere chiamato a simulare.

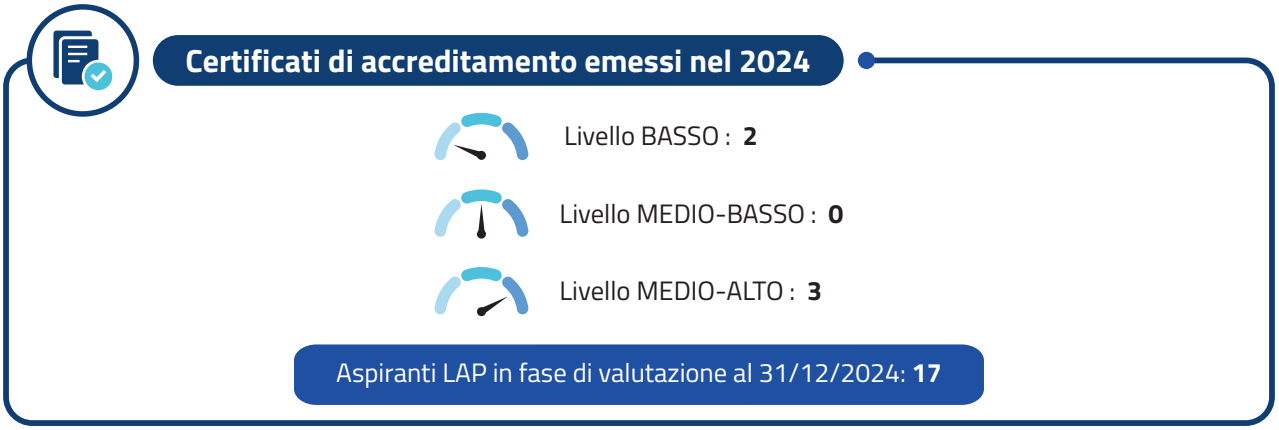


Figura 5 – Accreditamento LAP nel 2024

Nel processo di accreditamento di un laboratorio è prevista anche la verifica delle competenze del personale che opererà come valutatore all'interno del LAP (c.d. VLAP), tanto in materia normativa quanto tecnica. Nel corso del 2024 gli aspiranti VLAP che hanno superato l'esame, dimostrandosi idonei, a diversi livelli, a svolgere attività di test all'interno dei rispettivi laboratori di prova sono stati complessivamente 95.

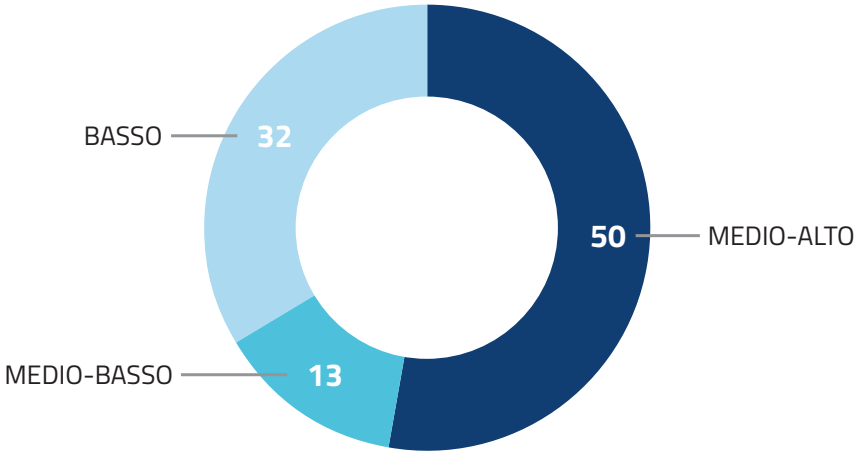


Figura 6 – VLAP valutati idonei nel 2024

Il sistema di scrutinio tecnologico nell'ambito del PSCN comprende anche i Centri di valutazione del Ministero della difesa e del Ministero dell'interno. Tali centri, che sono divenuti pienamente operativi nell'ultima parte del 2024, agiscono – ciascuno per i beni ICT di propria competenza – in maniera paritetica al CVCN, con il quale si raccordano.

4.1.2 Le attività ispettive in ambito Perimetro

Continua a operare presso l'ACN un'articolazione tecnica che svolge le attività di verifica tecnico-documentale e ispezione per gli adempimenti di cybersicurezza attribuiti all'Agenzia, nei confronti dei soggetti sia pubblici che privati, particolarmente quelli disciplinati dal PSNC. Tali attività vengono svolte in conformità con quanto previsto per gli organismi di ispezione (UNI CEI EN ISO/IEC 17020), anche al fine di offrire garanzie di imparzialità, indipendenza e riservatezza rispetto alle attività ispettive.

Per quanto attiene al 2024, nel corso dell'attività di verifica e ispezione dei Laboratori accreditati di prova, propedeutica al loro accreditamento, è stata esaminata la documentazione presentata da 15 laboratori, fornendo le relative non conformità e osservazioni necessarie all'adeguamento ai requisiti previsti dalle norme di riferimento.

Nel corso dell'anno sono state, inoltre, condotte 5 attività ispettive relative a LAP e 26 nei confronti di altrettanti soggetti appartenenti al PSNC che, sommate alle 4 eseguite nel 2023, hanno permesso di raggiungere la relativa *milestone* del PNRR.

4.2 CERTIFICAZIONI OCSI

Nel corso del 2024, l'Organismo di certificazione della sicurezza informatica ha proseguito le attività di emissione di certificati di cybersicurezza e quelle di accreditamento e vigilanza sui Laboratori per la valutazione della sicurezza (LVS), che effettuano le valutazioni sotto il controllo dello stesso OCSI.

Un primo filone di attività dell'OCSI è la gestione della valutazione e certificazione nell'ambito dello Schema nazionale di certificazione (ex DPCM 30 ottobre 2003), che riguarda beni appartenenti a diversi domini tecnologici, fra cui sistemi operativi, prodotti per le firme digitali, dispositivi per la protezione dei confini di rete, dispositivi di rete, sistemi di protezione dei dati, controllo remoto di sistemi, piattaforme *cloud, smart meter*, dispositivi multifunzione.

In tale ambito, nel 2024 l'OCSI ha rilasciato 10 certificati riconosciuti a livello internazionale. Si tratta, infatti, di certificati che hanno validità anche fuori dai confini nazionali, essendo mutuamente riconosciuti nell'ambito del CCRA (*Common Criteria Recognition Arrangement*, accordo con altri 32 organismi di certificazione mondiali) e del SOG-IS MRA (*Senior Officials Group Information Systems Security Mutual Recognition Agreement*, accordo con altre 17 agenzie governative UE ed extra UE). Al 31 dicembre 2024 erano in corso le valutazioni di 23 prodotti, le quali dovranno concludersi entro il 26 febbraio 2026, data limite stabilita dal Regolamento di esecuzione del sistema europeo EUCC, che sostituisce lo schema nazionale (vedasi Capitolo 1).

L'OCSI, inoltre, conduce le attività di verifica sugli LVS. Nel 2024 ha effettuato le verifiche di competenza su 4 laboratori già accreditati dall'OCSI, assicurando il rispetto della nuova versione dello standard CC:2022, obbligatorio dal luglio 2024.

Un ulteriore filone attiene all'attuazione del Regolamento eIDAS, concernente la disciplina dei sistemi di identità digitale, nel cui ambito si iscrive l'attività di accertamento di dispositivi per la creazione di firme/sigilli qualificati. L'OCSI è l'organismo di certificazione designato per l'Italia ai sensi del Codice dell'amministrazione digitale. In tale veste, ha emesso 7 attestazioni di conformità valide in tutta l'Unione europea.

Dietro ciascuna di queste certificazioni c'è una procedura particolarmente complessa che richiede numerosi accertamenti, sia di natura formale che tecnica. La stessa applicazione delle norme tecniche relative al processo di certificazione comporta diverse fasi, ciascuna delle quali richiede mirati approfondimenti e interazioni con le parti in causa, a garanzia dell'efficacia delle valutazioni di sicurezza e dell'imparzialità dei laboratori. OCSI monitora ciascuna di queste fasi producendo, se necessario, specifiche osservazioni e indicazioni. Un processo di certificazione può, infatti, durare diversi mesi, a seconda del livello di garanzia richiesto.

L'ACCORDO CCRA ALLA LUCE DEL NUOVO SISTEMA EUCC

L'Italia, tramite l'OCSI, aderisce all'accordo *Common Criteria Recognition Arrangement* che riunisce gli organismi responsabili degli schemi nazionali di certificazione basati sullo standard *Common Criteria* di 33 Paesi. Con l'avvio del nuovo sistema europeo di certificazione armonizzato EUCC, che estende la certificazione *Common Criteria* all'intera Unione europea, si prevede un crescente interesse nel settore, nonché la possibilità di nuove adesioni.

In vista della piena applicazione dell'EUCC e della cessazione degli schemi nazionali di certificazione dal 27 febbraio 2025, nel corso del 2024 in ambito CCRA si è ampiamente discusso del futuro assetto per il mutuo riconoscimento dei certificati internazionali *Common Criteria* tra Paesi UE ed extra-UE. Le future modalità di cooperazione sono state discusse direttamente dalla Commissione europea con i membri del CCRA, al fine di giungere a un accordo sulle modalità di mutuo riconoscimento dei certificati che tengano conto della diversa membership delle due organizzazioni. In una prima fase è stato previsto che gli Stati membri dell'UE che aderiscano al CCRA possano basarsi sull'attuale accordo CCRA per i nuovi certificati EUCC. In prospettiva, per estendere il mutuo riconoscimento dei certificati tra UE e Paesi terzi si renderà necessario prevedere nuovi accordi commerciali che la Commissione europea potrà negoziare direttamente con i Paesi terzi partecipanti al CCRA.

4.3 ATTUAZIONE DEL NUOVO REGOLAMENTO *CLOUD*

L'entrata in vigore del nuovo Regolamento unico per le infrastrutture e i servizi *cloud* per la PA (di cui si è riferito nel Capitolo 1) ha aggiornato le modalità di qualificazione e di adeguamento dei servizi *cloud* e delle infrastrutture digitali per la Pubblica Amministrazione. Il Regolamento riveste una particolare importanza perché consente di aumentare la sicurezza dei dati delle PA e dei cittadini attraverso un percorso articolato, che parte dalla classificazione dei dati e dei servizi a seconda del loro livello di criticità, per giungere alla verifica che i servizi *cloud* e le infrastrutture digitali assicurino opportuni livelli di cybersicurezza. Le procedure di verifica adottate dall'Agenzia trovano un punto di equilibrio tra tempi di risposta certi e approfondimenti a garanzia della piena conformità. Data anche la vastità della platea di soggetti su cui eseguire gli accertamenti, a un iniziale vaglio ad ampio spettro, si può accompagnare successivamente un più complesso controllo tecnico diretto.

Per la qualifica dei servizi *cloud* offerti da fornitori privati, una prima verifica ex ante viene eseguita in fase di presentazione dell'istanza di qualifica, nella quale, oltre agli elementi di natura formale, viene verificata la conformità rispetto ai requisiti, così da far emergere eventuali necessità di approfondimento. A tal fine, in fase di istanza, resa ora completamente telematica grazie all'evoluzio-

ne della piattaforma dedicata, è stato predisposto un questionario guidato. Oltre a incrementare l'efficienza dell'azione amministrativa, tale approccio permette così di acquisire una dichiarazione consapevole da parte degli istanti, facendo emergere eventuali cause ostative o elementi meritevoli di ulteriori controlli. In ogni caso, è comunque prevista la possibilità di effettuare approfondimenti nella fase di monitoraggio ex post durante l'arco di validità della qualifica, anche tramite accertamenti di carattere tecnico mediante l'accesso all'architettura fisica e logica dell'infrastruttura o dei servizi *cloud*, che possono portare eventualmente anche alla revoca della qualifica.

Per quanto riguarda l'adeguamento delle infrastrutture digitali dei fornitori privati, nonché l'adeguamento delle infrastrutture e dei servizi *cloud* delle Amministrazioni, viene effettuata una verifica di natura formale ed eventualmente una successiva opera di monitoraggio ex post, eseguita secondo modalità analoghe a quelle precedentemente descritte per il caso di qualifica.

Nel corso del 2024, anno di passaggio tra il citato regime transitorio e il regime ordinario (a partire dal 1° agosto, con l'entrata in vigore del nuovo Regolamento) - l'ACN ha trattato istanze relative alla qualifica di un totale di oltre 1.500 servizi, anche in forma aggregata (di cui più di 300 in regime ordinario), e di oltre 140 infrastrutture, per un totale di quasi 600 operatori privati. Inoltre, al 31 dicembre 2024 erano attivi più di 300 procedimenti di adeguamento di infrastrutture digitali o di qualifica di servizi *cloud* relativi a operatori privati.

Per quanto riguarda gli operatori privati, in Figura 7 vengono riportate le statistiche dei servizi *cloud* qualificati e delle infrastrutture adeguate nel 2024, rispetto allo specifico livello (da 1 a 4, in ordine crescente di criticità).

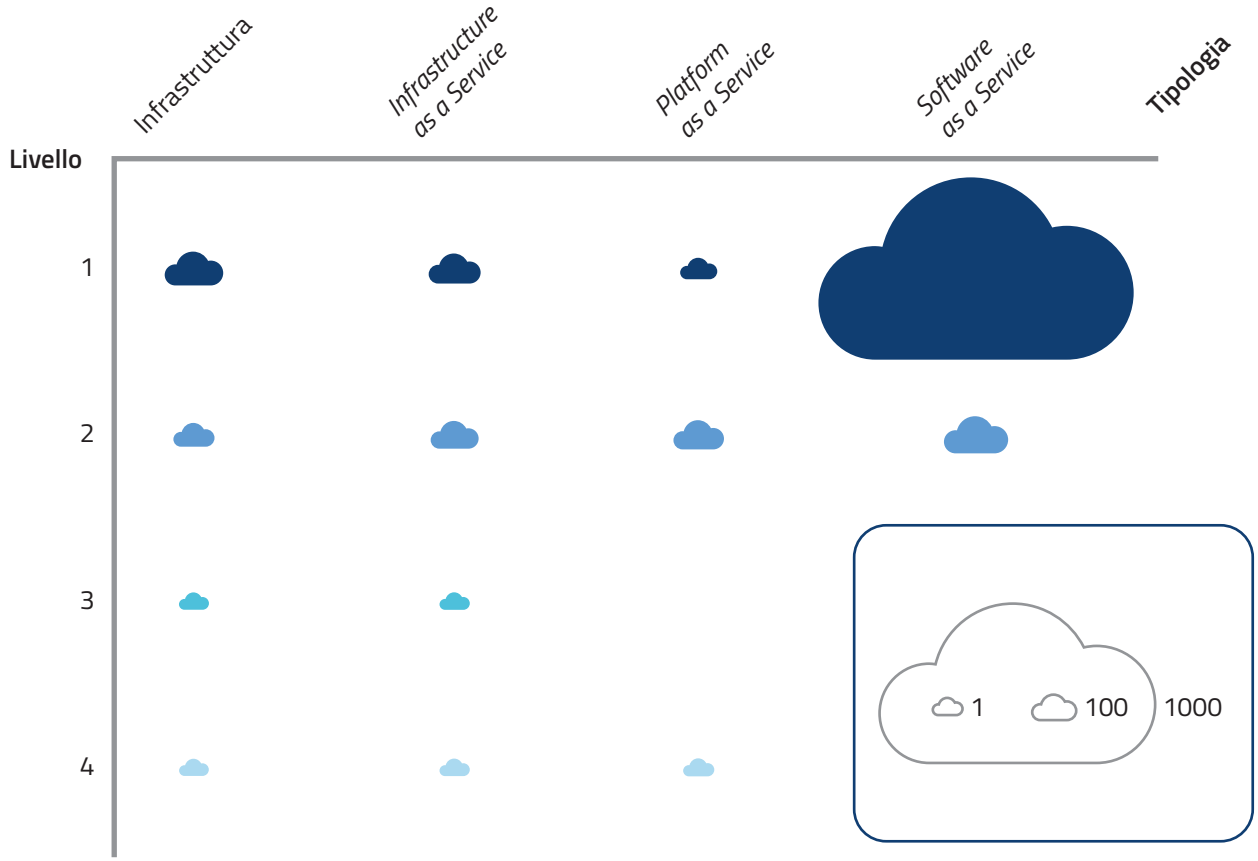


Figura 7 – Servizi *cloud* qualificati e infrastrutture adeguate forniti nel 2024

Relativamente alle Amministrazioni 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, per le quali era previsto l'obbligo di trasmettere la dichiarazione di conformità entro il 18 gennaio 2024, l'Agenzia ha effettuato almeno la verifica formale dell'istanza. Ha condotto, inoltre, il monitoraggio ex post, effettuando l'analisi tecnica preliminare su più del 20% delle dichiarazioni ricevute, eventualmente anche richiedendo integrazioni informative.

Infine, nel corso del 2024 sono proseguite le attività di supporto ai soggetti per quanto concerne il processo di classificazione dei dati e dei servizi digitali ai sensi del Regolamento *cloud*. In particolare, sono state presentate più di 300 domande di classificazione, mentre circa 130 Amministrazioni hanno richiesto di apportare aggiornamenti a una precedente classificazione.

4.4 IL RUOLO DELL'ACN NELL'ESERCIZIO DEL *GOLDEN POWER*

Nel corso del 2024, l'ACN ha continuato a fornire il proprio contributo in materia di *Golden Power*, sia per quanto riguarda la tecnologia 5G (art 1-*bis* del D.L. n. 21/2012) che negli altri settori (artt. 1 e 2). In tale ultimo ambito, l'Agenzia ha fornito un contributo su circa il 46% delle 641 notifiche presentate ai sensi degli artt. 1 e 2, attraverso la predisposizione di approfondimenti istruttori e di pareri, contribuendo anche alla definizione di prescrizioni. L' ACN ha, inoltre, fornito un contributo su circa il 30% delle 175 prenotifiche presentate.

In relazione alle notifiche per cui l'ACN ha fornito supporto, l'esito del procedimento è riportato in Figura 8.

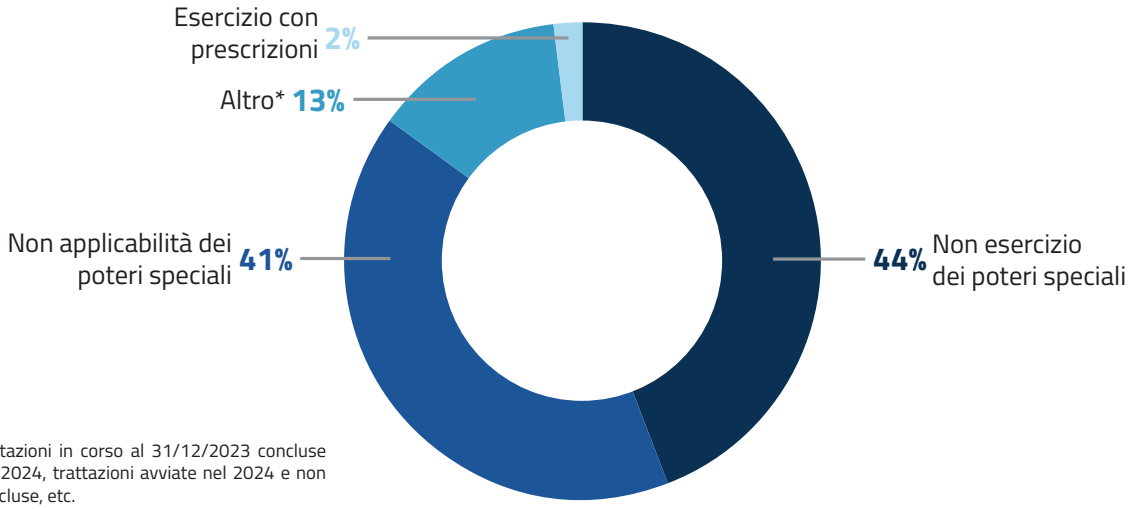
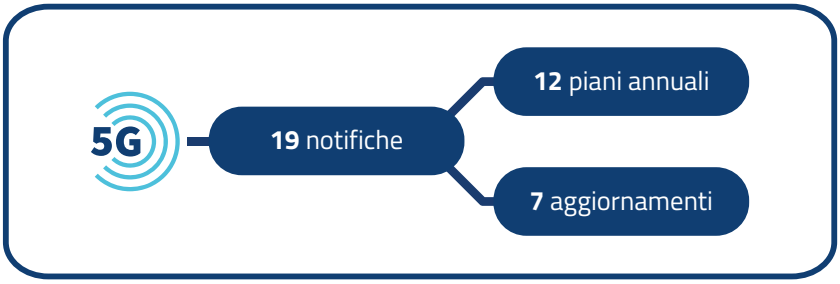


Figura 8 – Esito dei procedimenti *Golden Power* (artt. 1 e 2) cui l'ACN ha contribuito

Si segnalano 45 notifiche che hanno interessato direttamente il settore della cybersicurezza, che si sono concluse, in 17 casi, con la non applicabilità della normativa *Golden Power* e, nei restanti 28, con il non esercizio dei poteri speciali. In 11 casi è stato richiesto un approfondimento istruttorio attraverso quesiti a risposta scritta. In nessun caso il Gruppo di coordinamento ha proposto di esercitare i poteri speciali.

Tra i procedimenti di maggior rilievo trattati nel corso del 2024 si segnalano notifiche relative a settori non direttamente riconducibili al contesto della cybersicurezza, quanto a contesti manifatturieri, in particolare il settore delle macchine utensili e della robotica, e a settori relativi alle comunicazioni elettroniche e, più in generale, ai dati sensibili. La natura degli assetti tecnologici interessati in questi procedimenti ha richiesto un parere tecnico dell'ACN, che ha fornito il proprio contributo sia nelle fasi di conduzione degli approfondimenti istruttori che di definizione dei provvedimenti di esercizio dei poteri speciali.

Con riferimento specifico al settore delle comunicazioni elettroniche è di particolare rilievo l'attività svolta nell'ambito del procedimento che ha portato allo scorporo degli *asset* di rete dell'operatore TIM in favore di Fibercop. Riguardo a questo procedimento l'Agenzia ha contribuito alla definizione delle prescrizioni di carattere tecnico a presidio della sicurezza della rete, fornendo altresì pareri tecnici in sede di Comitato di monitoraggio dell'ottemperanza alle prescrizioni in capo ai diversi soggetti coinvolti nell'operazione.



Per quanto riguarda le attività svolte nel contesto dell'art. 1-bis del D.L. 21/2012, cioè quelle che riguardano le tecnologie 5G, l'ACN ha effettuato l'analisi di tutte le 19 notifiche pervenute nel corso del 2024, che comprendevano sia le notifiche dei piani annuali (12) che i loro aggiornamenti (7). Infine, con riferimento alle attività di monitoraggio previste in ambito 5G, l'ACN, quale membro del Comitato preposto, ha ricevuto e analizzato 47 relazioni di ottemperanza. Nel 2024 sono stati analizzati i piani annuali di sviluppo delle reti 5G, comprensivi di piani di acquisto di beni e servizi da parte degli operatori di telecomunicazione, riferiti all'anno 2023-2024. L'attività di monitoraggio ha visto l'analisi dello stato di implementazione delle prescrizioni imposte agli operatori di telecomunicazione in relazione ai suddetti piani.

L'attività di monitoraggio si è concentrata, in particolare, su valutazioni che riflettono sia le misure strategiche che le misure tecniche del *Toolbox* europeo sul 5G, al quale si sono ispirati i decreti di approvazione dei piani. Le misure strategiche previste dal citato *Toolbox* riguardano la valutazione delle attività di diversificazione dei fornitori nella componente di accesso radio, mentre quelle tecniche hanno per oggetto la valutazione dell'affidabilità dei componenti installati nelle reti 5G considerando, laddove possibile, l'utilizzo di componenti certificati e l'esecuzione di test di sicurezza.

4.5 LA CYBERSICUREZZA DELLE NUOVE TECNOLOGIE

Oltre alle attività nell'ambito dell'intelligenza artificiale esposte nel Capitolo 1, l'Agenzia segue con particolare attenzione gli sviluppi relativi all'evoluzione tecnologica nei campi rilevanti per la cybersicurezza. Tra questi, nel 2024 hanno rivestito un ruolo importante la crittografia, anche in relazione alla minaccia quantistica, e le reti mobili di nuova generazione.

4.5.1 Crittografia: Linee guida e prospettive

Considerato il ruolo chiave che la crittografia riveste in ambito cyber, l'ACN è impegnata per la diffusione della crittografia quale strumento di cybersicurezza. La legge n. 90/2024 ha, inoltre, istituito presso l'Agenzia il Centro nazionale di crittografia, che svolge le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato (vedasi Capitolo 1).

L'ACN ha proseguito il proprio lavoro di diffusione di informazioni e buone pratiche sulla crittografia arricchendo con ulteriori pubblicazioni, uscite a luglio 2024, la serie "Linee guida funzioni crittografiche".

Il primo dei due documenti, dal titolo "Introduzione alla crittografia e alle Linee guida", presenta la serie delle Linee guida con uno sguardo di insieme, includendo la spiegazione di alcuni concetti alla base della crittografia moderna e la presentazione di aspetti generali comuni ai vari documenti delle Linee guida. In questo documento, vengono esposte le differenze tra crittografia a chiave pubblica e crittografia simmetrica, il concetto di complessità di un algoritmo crittografico e vengono introdotte alcune nozioni di crittoanalisi, descrivendo gli obiettivi degli attaccanti e i possibili scenari di attacco.

Il secondo documento, intitolato "Cifrari a blocchi e modalità di funzionamento", è dedicato a una tipologia di algoritmi crittografici ampiamente utilizzata in vari ambiti del mondo digitale. I cifrari a blocchi sfruttano una struttura ripetuta per cifrare blocchi di messaggi sequenziali, e possono essere applicati al testo in chiaro a seconda della modalità di operazione selezionata. Nel documento viene spiegata la struttura generale dei cifrari a blocchi, con un approfondimento, in particolare, sullo standard AES (*Advanced Encryption Standard*), che rappresenta al momento l'alternativa più sicura e più utilizzata. Vengono, inoltre, evidenziati gli aspetti più critici che potrebbero compromettere la sicurezza del sistema di cifratura e presentate alcune raccomandazioni, inclusi i parametri minimi per un'implementazione sicura degli specifici algoritmi.

L'Agenzia provvederà all'espansione della serie di Linee guida, per coprire tutti i principali ambiti della crittografia moderna. Si intende, inoltre, garantire 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.

Crittografia
quantum safe

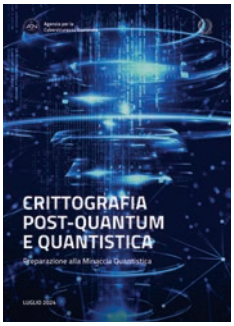
L'Agenzia è attiva anche nel campo della ricerca in ambito crittografico, particolarmente sulla minaccia presentata dallo sviluppo dei computer quantistici ai danni degli attuali schemi di crittografia a chiave pubblica (vedasi box). Vi è, infatti, il rischio concreto che nei prossimi decenni possano essere perfezionate macchine o strumentazioni in grado di effettuare attacchi quantistici sugli attuali sistemi crittografici. È dunque imperativo farsi trovare preparati, non solo per resistere a futuri attacchi diretti ai sistemi informatici in uso, ma anche per evitare che dati intercettati adesso vengano tenuti da parte per essere decifrati in futuro, quando saranno disponibili computer quantistici adatti (così da contrastare la strategia nota come *harvest now, decrypt later*). Per arginare tale minaccia, la comunità scientifica ha ideato nuovi algoritmi capaci di resistere

ad attacchi quantistici, dando vita alla cosiddetta crittografia *post-quantum,* ma molto resta ancora da fare per renderli operativi.

Algoritmo di Shor

Algoritmo per computer quantistici ideato nel 1994 dal matematico statunitense Peter Shor. Dal punto di vista teorico, permette a un computer quantistico di risolvere efficientemente i due problemi matematici alla base della sicurezza degli algoritmi di cifratura a chiave pubblica ampiamente utilizzati (la fattorizzazione di numeri interi e il logaritmo discreto).

Attualmente non esistono ancora computer quantistici con le capacità necessarie per applicare l'algoritmo ai parametri correntemente in uso e mettere quindi a rischio la crittografia moderna. Tuttavia, i grandi investimenti nella ricerca sulla computazione quantistica hanno velocizzato lo sviluppo dei computer quantistici, che potrebbero raggiungere in tempi più brevi del previsto le capacità richieste per utilizzare l'algoritmo di Shor.



L'ACN a livello nazionale fornisce consigli e raccomandazioni per una strategia di transizione verso i nuovi algoritmi *post-quantum*, passando per una fase intermedia di tipologia ibrida. A tal riguardo, a luglio 2024, è stato pubblicato un documento informativo dal titolo "Crittografia post-quantum e quantistica: preparazione alla minaccia quantistica", che riassume la situazione attuale sul tema della crittografia *quantum safe* e affronta il problema della minaccia quantistica, analizzando anche alcuni degli sviluppi internazionali in materia. L'obiettivo del documento è sensibilizzare l'opinione pubblica su un tema rilevante per la crittografia moderna e per le sue molteplici applicazioni, ribadendo l'urgenza di iniziare a lavorare per una transizione dai metodi classici potenzialmente a rischio a nuovi metodi sicuri.

Infine, la collaborazione con l'Associazione "De Componendis Cifris" è proseguita nel 2024, anche con la partecipazione all'annuale conferenza Cifris24, che ha riunito, oltre a diverse istituzioni, rilevanti contributi da parte della ricerca crittografica nazionale e internazionale.

4.5.2 Sicurezza delle reti mobili di nuova generazione

Nel corso del 2024, l'Agenzia ha intrapreso una serie di attività volte a sviluppare una capacità di valutazione della cybersicurezza delle reti di nuova generazione (5G), secondo un approccio sistemico che non si limita alla valutazione di singoli componenti, tipico delle precedenti generazioni, quanto piuttosto all'analisi integrata del loro scenario di impiego e dei profili connessi.

In tale ambito, per le finalità connesse ai compiti del CVCN, l'Agenzia intende dotarsi di strumenti per lo scrutinio tecnologico delle componenti delle reti 5G. Al riguardo, oltre a elaborare la metodologia di test, arricchita dall'esperienza maturata in ambito *Golden Power*, sono state definite le caratteristiche che dovrà avere il laboratorio specialistico 5G di prevista acquisizione.

Nella definizione dei test cui sottoporre la tecnologia 5G ha giocato un ruolo importante anche la collaborazione con l'Università Sapienza e l'Università Tor Vergata di Roma, nell'ambito della quale sono stati promossi dei progetti di ricerca dedicati.

5.

INVESTIMENTI: PER UN SOSTEGNO CONCRETO ALLA CYBERSICUREZZA DEL PAESE

Un importante filone di azione dell'ACN è stato indirizzato al rafforzamento della sicurezza e resilienza cyber del Paese, attraverso diversi programmi a sostegno del più ampio ecosistema nazionale della cybersicurezza. L'obiettivo di rendere l'Italia più sicura sotto il profilo cyber ha trovato nel programma di investimenti del Piano nazionale di ripresa e resilienza la chiave di volta per avviare il processo di sviluppo della sicurezza cibernetica nazionale. Ciò ha permesso di potenziare le capacità cyber sotto tre principali direttrici: le capacità cyber della Pubblica Amministrazione, le capacità di cyber resilienza del Paese e, infine, le capacità nazionali di scrutinio e certificazione tecnologica.

Alle risorse messe in campo dal PNRR, si aggiungono quelle che l'ACN dedica allo sviluppo del sistema produttivo, a partire da realtà innovative come le *startup* con alto potenziale di scalabilità. Rilevanti sono, inoltre, gli sforzi dedicati a dotare il Paese di strumenti tecnologici all'avanguardia con i quali assicurare una migliore protezione dalle minacce e garantirsi capacità di sfruttare in maniera positiva le evoluzioni tecnologiche di oggi e di domani. In tale quadro, rimane primaria l'esigenza di dialogare costantemente con il mondo accademico e della ricerca, in un'ottica volta a incentivare il trasferimento tecnologico e la creazione di innovazione nei settori più strategici.

5.1 LE RISORSE DEL PNRR PER LA CYBERSICUREZZA

L'Investimento 1.5 "*Cybersecurity*" della Missione 1 – Componente 1 – Asse 1 del PNRR, a titolarità del DTD e di cui l'Agenzia è soggetto attuatore, ha previsto 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, mirando a rafforzare l'ecosistema digitale nazionale potenziando le capacità dell'Agenzia e sostenendo la crescita dell'autonomia tecnologica nazionale.

Il processo virtuoso di innalzamento della resilienza e sicurezza cyber del sistema Paese, avviato con le progettualità del PNRR ha fatto sì che gli obiettivi, individuati e inizialmente avviati nel corso del 2022 e portati avanti nel 2023, siano stati accompagnati verso la conclusione durante il 2024. Le informazioni acquisite in fase di rilevazione dei fabbisogni, la definizione di modalità uniformi per la gestione degli interventi di potenziamento delle capacità cyber a livello nazionale e il dispiegamento dei servizi cyber nazionali hanno consentito e consentiranno all'Agenzia di realizzare ulteriori e specifici programmi e iniziative di trasformazione ed evoluzione dei presidi in essere, mettendo a disposizione del Paese adeguati strumenti funzionali a progetti di rilevanza strategica nazionale.

5.1.1 Stato dell'attuazione

Il citato Investimento, declinato in *milestone* e *target* europei organizzati secondo le due scadenze di dicembre 2022 e dicembre 2024, ha previsto specifiche iniziative, coordinate dall'Agenzia, che hanno permesso di raggiungere con successo tutti gli obiettivi previsti:

- ***target* finale UE M1C1-19**: realizzazione di almeno 50 interventi di potenziamento cyber. Mediante la gestione delle attività relative agli Avvisi pubblici 1, 2, 3, 7 e degli Accordi di collaborazione c.d. *Cyber Defence*, sono stati conclusi 55 interventi di potenziamento della resilienza cyber su entità pubbliche e private, in aggiunta alle 7 progettualità già completate;

- ***milestone* UE M1C1-20**: dispiego integrale dei servizi cyber nazionali. Tramite la gestione dell'Avviso 6/2023 per la realizzazione e il potenziamento di CSIRT Regionali, è stata attivata e connessa la rete dell'Agenzia, coordinata dal CSIRT Italia; è stato realizzato il sistema HyperSOC per monitoraggio e segnalazione di eventi di cybersicurezza; è stato attivato l'ISAC Italia, ovvero il servizio di condivisione e analisi specialistiche su *cyber threat intelligence* e su settori di interesse;
- ***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. Sono stati attivati 12 laboratori e 2 Centri di valutazione, mediante l'attuazione di iniziative di finanziamento indirizzate alla Pubblica Amministrazione e agli operatori economici, con l'obiettivo di costruire e consolidare le capacità nazionali di valutazione e scrutinio tecnologico della sicurezza su beni, sistemi e servizi ICT inclusi nel PSNC e sviluppare competenze e capacità specialistiche necessarie a garantire adeguati livelli di resilienza cyber per il Paese;
- ***milestone* UE M1C1-22**: esecuzione di almeno 30 ispezioni per le misure di sicurezza PSNC e NIS. È stata raggiunta la piena operatività dell'unità centrale ispettiva dell'Agenzia per le misure di sicurezza PSNC e NIS, con il completamento di 30 ispezioni.

Il via libera della Corte dei Conti

Il raggiungimento di tutti gli obiettivi previsti per il 2024 è confermato anche dalla Corte dei Conti che, con il report di cui alla Deliberazione n. 8/2025/G e con riferimento alle attività dell'Agenzia rispetto all'Investimento 1.5, ha affermato che "nel periodo preso in esame, dalla consultazione dell'applicativo Regis, componente "Avanzamento M&T", è stato possibile verificare il raggiungimento dei traguardi relativi ad un target e alle 3 milestone ampiamente descritte in Relazione, così come anche confermato in corso di istruttoria dagli Enti competenti."

A livello finanziario, a fine 2024, risultano impegnati 621,26 milioni di euro sui 623 milioni di euro disponibili (99,72%), sia mediante la realizzazione di linee di intervento gestite direttamente dall'ACN (dedicate ai propri sistemi e servizi e a quelli di altre Amministrazioni), per un totale di 207,35 milioni di euro (interventi c.d. a titolarità), sia attraverso il finanziamento a ristoro di attività condotte da soggetti terzi, per un totale di 413,91 milioni di euro (interventi c.d. a regia), come mostrato in Figura 1.

Figura 1 – Modalità di finanziamento

Tale risultato è stato possibile grazie alla stipula, fin dal 2022, di accordi bilaterali con Pubbliche Amministrazioni centrali (Accordi *Cyber Defence,* Accordi CSIRT), oltre che al finanziamento, attraverso Avvisi Pubblici, di ulteriori soggetti (Figura 2). A questi si aggiunge l'attivazione di contratti e convenzioni finalizzati a supportare l'Agenzia nello svolgimento degli interventi a titolarità.

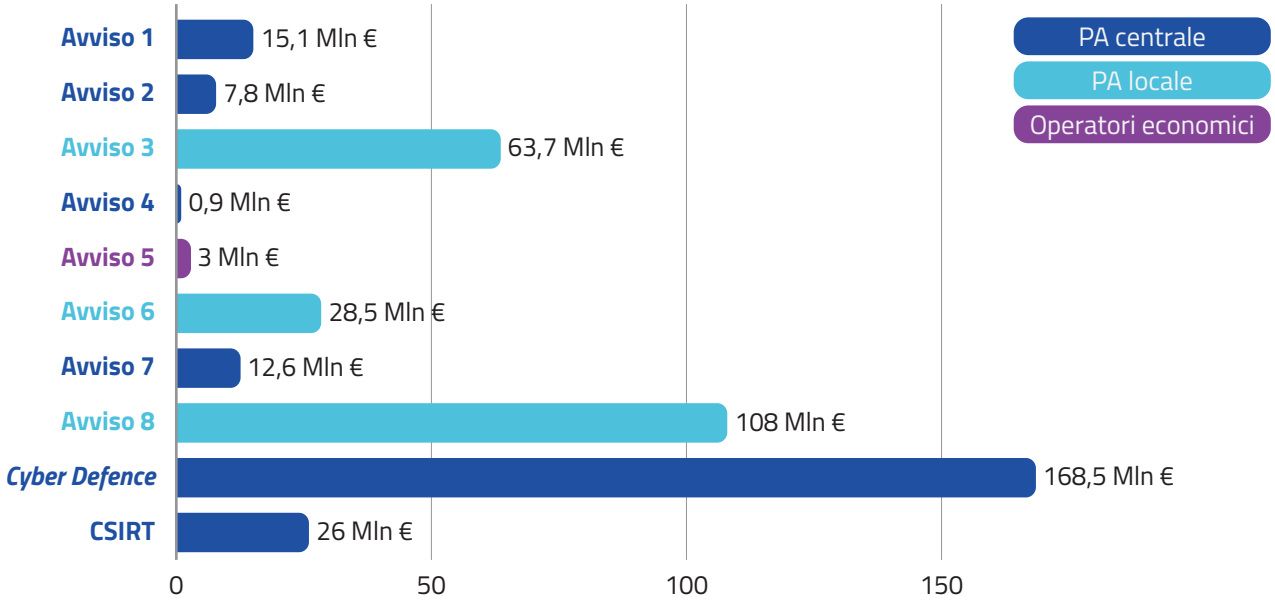


Figura 2 – Dettaglio impegni per accordi e avvisi PNRR

Il PNNR è stato il volano per mettere a terra le fondamenta necessarie per elevare la postura cyber dell'ecosistema nazionale di cybersicurezza, fondamenta sulle quali si continuerà a costruire negli anni a seguire, anche attraverso le risorse messe a disposizione dai fondi dedicati alla Strategia nazionale di cybersicurezza (vedasi Capitolo 8).

5.1.2 Potenziamento delle capacità cyber della Pubblica Amministrazione

L'obiettivo di potenziare le capacità cyber della PA (*target* M1C1-9 e M1C1-19) ha portato l'Agenzia a mettere a disposizione delle Amministrazioni pubbliche, centrali e locali, differenti iniziative di finanziamento, che hanno permesso di innalzare la protezione degli *asset* strategici nazionali, potenziando il livello di postura cyber delle Amministrazioni.

Sono stati conclusi complessivamente 62 interventi, riguardanti specifiche tipologie, quali la realizzazione o il potenziamento di centri operativi per la sicurezza (*Security Operations Center*-SOC), il miglioramento della difesa dei confini informatici e il potenziamento delle capacità interne di monitoraggio e controllo nel rispetto dei requisiti NIS e PSNC. Tutti gli interventi realizzati, in linea con i *target* europei, riguardano i settori individuati da tali normative, con focus particolare nei settori energia, assistenza sanitaria, approvvigionamento di acqua potabile, gestione dei rifiuti e delle acque reflue.

I finanziamenti messi a disposizione nel corso del 2024 hanno permesso di:

- **valutare la postura di cybersicurezza** corrente delle Amministrazioni coinvolte tramite il supporto nell'identificazione di problematiche – attuali e potenziali – sugli *asset* esposti, nonché i rischi associati alle attività svolte da ciascuna;
- **rafforzare i sistemi critici** delle Amministrazioni coinvolte mediante il supporto all'analisi delle problematiche, la prioritizzazione e implementazione delle misure preventive e di mitigazione del rischio;

- **migliorare la consapevolezza cyber** attraverso la definizione di strumenti necessari ad abilitare lo scambio informativo e l'integrazione fra l'Agenzia e i SOC delle PA coinvolte, per la rilevazione di minacce di sicurezza rilevanti a livello nazionale;
- mettere in campo diverse attività per **elevare la postura di sicurezza** riscontrata per le aree di miglioramento identificate dall'Agenzia. Tra queste si segnalano attività relative a *governance* e programmazione cyber, gestione del rischio cyber e della continuità operativa, gestione e risposta agli incidenti di sicurezza, gestione delle identità digitali e degli accessi logici, formazione e consapevolezza cyber, sicurezza delle applicazioni, dei dati e delle reti;
- **realizzare specifici interventi** che permettano di coinvolgere anche i più grandi operatori nazionali di determinati settori, anche oltre quelli sopra citati (telecomunicazioni, aerospazio, manifatturiero e tecnologico).

Nel corso del 2024, è stato pubblicato l'Avviso 8/2024, volto a supportare le Pubbliche Amministrazioni locali nella realizzazione di interventi di potenziamento della resilienza cyber con un finanziamento iniziale di 50 milioni di euro, successivamente ampliato a 108 milioni di euro. I destinatari di questo Avviso sono stati individuati dall'ACN includendo soggetti ricompresi nella legge n. 90/2024, al fine di supportarli attraverso risorse dedicate nell'implementazione degli obblighi definiti dalla nuova normativa. Tali soggetti sono i grandi Comuni (con una popolazione superiore a 100.000 abitanti), i Comuni capoluogo di Regione, le città metropolitane, le Agenzie regionali sanitarie e le Aziende ed enti di supporto al Servizio sanitario nazionale, le Autorità di sistema portuale, le Autorità di bacino distrettuale e le Agenzie regionali per la protezione dell'ambiente.

Sono pervenute 97 richieste di partecipazione dal cui esame è stata prodotta una graduatoria di 81 progetti ammessi a finanziamento (79 interamente e 2 parzialmente). A seguito del rifinanziamento, il totale dei progetti finanziati è arrivato a 87 (85 totalmente e 2 parzialmente), con la distribuzione indicata in Figura 3.

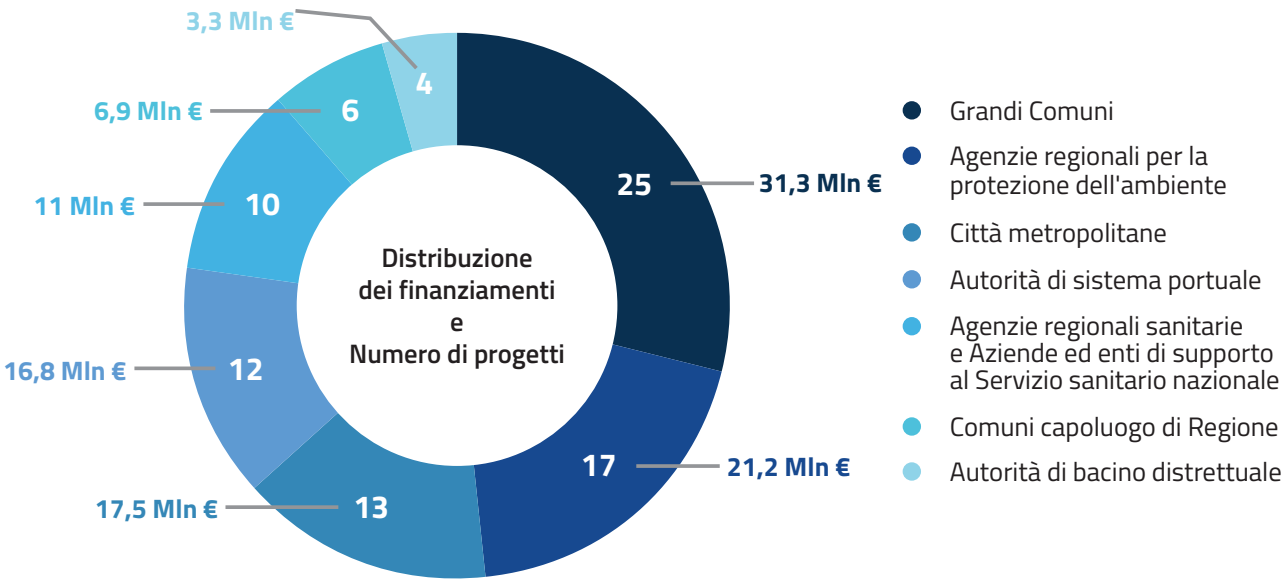


Figura 3 – Distribuzione dei finanziamenti Avviso 8 per tipologia di PAL

SVILUPPI RELATIVI AGLI AVVISI PER IL POTENZIAMENTO DELLA RESILIENZA CYBER DELLA PA

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
- **2022:** finanziati 20 progetti di 12 Amministrazioni per un totale di 15 milioni di euro.
- **2023:** rifinanziamento di 1,1 milioni di euro (portando il totale a 22 progetti).
- **2024:** completati 12 interventi di potenziamento.

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
- **2022:** finanziati interventi erogati dall'Agenzia per 12 Amministrazioni per un totale di 7,8 milioni di euro.
- **2024:** completati tutti gli 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
- **2022:** finanziati 51 progetti di 35 Amministrazioni per un totale di 45 milioni di euro.
- **2023:** rifinanziamento di 18,7 milioni di euro (portando il totale a 63,7 milioni per 75 progetti).
- **2024:** completati 22 interventi di potenziamento.

Avviso Pubblico 7/2023: per il potenziamento della resilienza cyber degli Organi costituzionali e di rilevanza costituzionale, dei Ministeri, delle Agenzie fiscali, degli Enti di regolazione dell'attività economica, delle Autorità amministrative indipendenti e degli Enti a struttura associativa.

- Aperto l'11 ottobre 2023 | Chiuso il 5 dicembre 2023
- **2024:** finanziate 25 Amministrazioni per un totale di circa 13 milioni di euro. Completati 5 interventi di potenziamento.

Avviso Pubblico 8/2024: per il potenziamento della resilienza cyber di grandi Comuni, Comuni capoluogo di Regione, Città metropolitane, Agenzie regionali sanitarie e Aziende ed enti di supporto al Servizio sanitario nazionale, Autorità di sistema portuale, Autorità di bacino distrettuale e Agenzie regionali per la protezione dell'ambiente.

- Aperto il 26 febbraio 2024 | Chiuso il 12 aprile 2024
- **2024:** finanziate 87 Amministrazioni per un totale di 108 milioni di euro.

Accordi *Cyber Defence*: per il potenziamento della resilienza cyber di Pubbliche Amministrazioni centrali.

- **2022:** stipulati 6 Accordi con Pubbliche Amministrazioni centrali, quali Ministeri dell'interno, della giustizia e della difesa, Consiglio di Stato, Comando Generale dell'Arma dei Carabinieri, Comando Generale della Guardia di Finanza, per un totale di 168,5 milioni di euro.
- **2024:** conclusi 4 interventi di potenziamento.

5.1.3 Sviluppo delle capacità di cyber resilienza nel Paese

Il secondo pilastro dell'Investimento 1.5 "*Cybersecurity*" è quello relativo allo sviluppo delle capacità di cyber resilienza in modo diffuso nel Paese, capacità identificate come 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, anche mediante sinergie con la Pubblica Amministrazione e il settore privato. Nel corso del 2024, il dispiego integrale dei servizi cyber ha permesso di innalzare il livello complessivo di resilienza cibernetica, mediante la realizzazione delle tre progettualità cardine: HyperSOC, CSIRT Italia e relativa rete, ISAC Italia e rete.

HyperSOC. È un sistema integrato per la protezione degli *asset* strategici nazionali che fornisce servizi volti a sostenere il potenziamento delle capacità di monitoraggio e analisi di eventi di sicurezza dei soggetti aderenti. Tramite l'HyperSOC l'Agenzia è in grado di comunicare, alle organizzazioni pubbliche e private che decidono di usufruire del servizio, criticità di vario tipo, come vulnerabilità, *misconfiguration* e software obsoleti. Nel 2024 l'Agenzia ha rafforzato e ampliato il progetto HyperSOC potenziando i servizi offerti, affiancando a quello già esistente per il monitoraggio esterno (*Attack Surface Monitoring*) quello di nuova introduzione per il monitoraggio interno (*Golden Set of IOC*).

L'*Attack Surface Monitoring* consente il rilevamento proattivo di criticità sul perimetro esposto dei soggetti aderenti, attraverso l'analisi e la correlazione di molteplici fonti di dati. Il servizio è facilmente configurabile dai soggetti partecipanti, a cui è richiesto di fornire l'elenco degli *asset* esposti. Attraverso una *dashboard* dedicata, i soggetti ricevono segnalazioni sulle criticità rilevate e indicazioni per la loro mitigazione.

A tale strumento si è affiancato, nel corso dell'anno, il servizio *Golden Set of IOC*, che permette il monitoraggio di indicatori di compromissione (o IOC), selezionati dall'Agenzia su scala nazionale e settoriale. Il servizio prevede un'integrazione bidirezionale tra le piattaforme dei soggetti aderenti e quelle dell'Agenzia, garantendo una condivisione automatizzata e in tempo reale degli IOC.

I dati operativi dell'HyperSOC

Nel corso del 2024, attraverso l'HyperSOC sono state condivise con i 20 soggetti che hanno aderito oltre 8.000 criticità sui servizi esposti dalle loro reti e oltre 2.500 potenziali compromissioni. Le criticità segnalate sono state di gravità alta nel 20% dei casi, media nel 35% e minore nel 45%. Quasi tutte le criticità di gravità alta segnalate attraverso l'HyperSOC (95%) sono state sanate dagli utenti e non risultavano più rilevabili al 31 dicembre 2024.

Tali attività sono state possibili grazie alla definizione, già a partire dal 2023, di quasi 1.000 indicatori volti a identificare molteplici criticità a partire dalle informazioni a disposizione dell'Agenzia. Ognuna delle criticità condivise è, inoltre, associata a un bollettino di sicurezza che riporta sia le informazioni di contesto per la comprensione del problema che i possibili impatti di sicurezza, nonché le misure di mitigazione consigliate.

Un importante tassello dell'HyperSOC è rappresentato da un'infrastruttura di *High Performance Computing* (HPC), cioè un sistema di calcolo a elevate prestazione che permetterà di supportare il potenziamento dei servizi cyber nazionali anche tramite strumenti basati su intelligenza artificiale e *machine learning*. L'IA, attraverso la capacità di elaborare rapidamente un'ingente mole di dati, presenta, infatti, enormi potenzialità per migliorare il rilevamento delle minacce cyber.

CSIRT Italia e rete nazionale di CSIRT. Si tratta di un sistema per la risposta a minacce, incidenti e crisi cyber, che si compone del CSIRT Italia e della rete di CSIRT, a supporto della *constituency* nella

gestione di minacce informatiche. Gestiscono, quindi, eventi cyber monitorati che possono avere un potenziale impatto negativo, nonché incidenti informatici che potrebbero generare situazioni di crisi a livello nazionale. Tali servizi sono realizzati mediante una stretta collaborazione tra la rete di CSIRT, la *constituency* e il CSIRT Italia, elemento centrale di integrazione anche verso il contesto europeo e internazionale delle omologhe agenzie cyber. In tale ambito, sono state completate le piattaforme a supporto del CSIRT Italia ed è stata finalizzata l'interconnessione con i CSIRT regionali, istituiti presso le Regioni e le Province autonome al fine di avere una maggiore copertura informativa sul territorio, ai quali si aggiungeranno i CSIRT delle PA centrali (vedasi box).

SVILUPPI RELATIVI AL DISPIEGAMENTO DELLA RETE DI CSIRT

Avviso Pubblico 6/2023: per il finanziamento di progetti volti a istruire o potenziare i CSIRT costituiti presso le Regioni o le Province autonome.

- Aperto l'11 agosto 2023 | Chiuso il 25 settembre 2023
- **2023:** finanziamento di 28,5 milioni di euro per un totale di 19 soggetti finanziati.
- **2024:** attivati o potenziati 12 CSIRT costituiti presso Regioni e Province autonome.

Accordi CSIRT-PAC: per il finanziamento di progetti volti a istituire o potenziare i CSIRT costituiti presso i Ministeri.

- Aperto il 17 giugno 2024 | Chiuso il 12 luglio 2024
- **2024:** predisposizione di accordi di collaborazione con 8 Ministeri. Finanziamento complessivo pari a circa 26 milioni di euro.

ISAC Italia. Il servizio di condivisione e analisi è stato lanciato nel corso del 2024 a supporto della *constituency*. Gli *Information Sharing and Analysis Center* (ISAC) sono organizzazioni finalizzate allo scambio di informazioni e conoscenze in ambito cyber, che vedono il coinvolgimento di *stakeholder* omogenei, come imprese operanti nello stesso settore di attività economica. L'ISAC Italia è stato istituito presso l'Agenzia con il fine di riunire in una rete gli ISAC settoriali già esistenti e che si costituiranno. Lo scopo dell'ISAC Italia è raccogliere, analizzare e condividere le informazioni prodotte dai vari servizi cyber nazionali in maniera bidirezionale e multisettoriale.

I servizi erogati dall'ISAC Italia sono articolati nelle seguenti categorie:

- approfondimenti: pubblicazioni, analisi settoriali e linee guida sulla gestione del rischio cyber, sulle minacce alla sicurezza informatica e sul contesto normativo vigente;
- strumenti: piattaforme e strumenti utili agli *stakeholder* per scambiare informazioni, condividere esperienze e *best practice* nonché per rafforzare le relazioni di fiducia;
- formazione ed eventi: gruppi di lavoro, seminari e conferenze volti a rafforzarne le capacità di prevenire, identificare, mitigare e contrastare rischi e minacce informatiche attuali ed emergenti.

Nel 2024 è proseguita l'attività di promozione che ha portato alla creazione dell'ISAC TELCO, che riunisce gli operatori del settore delle telecomunicazioni, e dell'ISAC CDP, che include le strutture di cybersicurezza delle società del gruppo Cassa Depositi e Prestiti (CDP). Inoltre, all'interno della

rete nazionale di ISAC settoriali, è stata avviata la collaborazione con l'ISAC dell'AISCAT, Associazione italiana società concessionarie autostrade e trafori, finalizzata alla definizione e analisi di scenari di rischio cyber.

5.1.4 Rafforzamento delle capacità cyber nazionali di scrutinio e certificazione tecnologica

Il terzo pilastro del PNRR, relativo al rafforzamento delle capacità nazionali di scrutinio e certificazione tecnologica, ha visto l'attivazione e il progressivo ampliamento della rete dei laboratori di *screening* e certificazione della cybersicurezza, con la costituzione di un totale di 12 laboratori e di 2 Centri di valutazione (vedasi Capitolo 4). In tale ambito, l'Agenzia ha attuato diverse iniziative di finanziamento indirizzate sia alla Pubblica Amministrazione che agli operatori economici, al fine di costruire e consolidare le capacità nazionali di valutazione e scrutinio tecnologico della sicurezza su beni, sistemi e servizi ICT inclusi nel Perimetro e sviluppare competenze e capacità specialistiche. Per quanto riguarda le iniziative verso la Pubblica Amministrazione, l'Agenzia ha stipulato specifici accordi attuativi con il Ministero dell'interno e della difesa, che hanno consentito l'attivazione dei Centri di valutazione a supporto del CVCN, e pubblicato l'Avviso 4/2022, che ha permesso l'attivazione, presso il MEF, del primo laboratorio accreditato di scrutinio tecnologico nell'ambito della PA già nel 2022. In relazione alle iniziative dirette agli operatori economici, l'Agenzia, con l'Avviso 5/2022, ha esteso anche ai soggetti privati la concessione di finanziamenti per la costituzione e il potenziamento di laboratori a supporto del CVCN e dei CV, portando all'attivazione, nel corso del 2024, di ulteriori 11 laboratori di scrutinio tecnologico.

5.2 PROGRAMMI INDUSTRIALI E DI INVESTIMENTO

Lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche nell'ambito della cybersicurezza è uno degli obiettivi strategici dell'Agenzia, che ha adottato un approccio caratterizzato da un forte coinvolgimento del tessuto produttivo nazionale.

Nello specifico, il *Cyber Innovation Network* (CIN) è il principale programma di collaborazione tra l'Agenzia e l'ecosistema nazionale della ricerca, dell'innovazione e dell'industria, che mira a sostenere la creazione e lo sviluppo di *startup*, nonché a facilitare il trasferimento e la valorizzazione di risultati della ricerca applicata relativi ad ambiti di interesse strategico, individuati dall'Agenda di ricerca e innovazione 2023-2026. Tale Agenda, frutto della collaborazione tra l'ACN e il Ministero dell'università e della ricerca, è il documento di indirizzo per promuovere programmi di ricerca e di investimento nel campo della cybersicurezza.

Avviato nel 2023, il CIN ha visto nel 2024 la prosecuzione delle attività nell'ambito dello sviluppo industriale, attraverso la sottoscrizione di accordi di collaborazione con i primi 5 operatori dei 19 incubatori e acceleratori selezionati nel 2023, mediante specifico Avviso. Gli operatori CIN selezionati, che includono alcuni dei primari attori dell'innovazione dell'ecosistema italiano, sono l'incubatore del Politecnico di Torino (I3P), ZestGroup (nata dalla fusione tra LVenture e Digital Magics), Nana Bianca, CDP Venture Capital Sgr e Scientifica Venture Capital (Figura 4).

Figura 4 – Distribuzione geografica degli operatori CIN

L'approccio sinergico pubblico-privato si è tradotto nel processo, a due fasi, di selezione delle *startup* ritenute meritevoli di entrare nella rete di collaborazione dell'Agenzia e di poter ricevere un finanziamento in conformità alla normativa in materia degli aiuti di Stato in regime *de minimis*. In particolare, a valle della selezione delle *startup* da ammettere ai programmi di incubazione o accelerazione degli operatori CIN, l'Agenzia individua quelle da supportare con un contributo a fondo perduto. La scelta avviene secondo criteri di valutazione basati sulla rilevanza tecnologica e sulla coerenza con i temi della citata Agenda di ricerca e innovazione, sul potenziale valore industriale ed economico, sull'impatto sociale delle proposte, nonché sulla fattibilità tecnica e sulla sostenibilità del modello di business proposto in reali contesti di impiego.

In termini di risultati, nel 2024 sono stati avviati 3 programmi congiunti dell'Agenzia (*Call4startup*) con gli operatori I3P, Nana Bianca e Scientifica Venture Capital che hanno raccolto l'interesse alla partecipazione di oltre 80 *startup*. Tra le proposte ricevute, in particolare, è emerso come l'intelligenza artificiale e la crittografia rappresentino le tecnologie di maggior interesse delle *startup* coinvolte. Le aree tematiche, tra quelle delineate nell'Agenda di ricerca e innovazione, risultate più rilevanti per i partecipanti ai programmi sono la sicurezza dei dati e *privacy*, la gestione delle minacce cibernetiche e la sicurezza delle infrastrutture digitali (Figura 5).

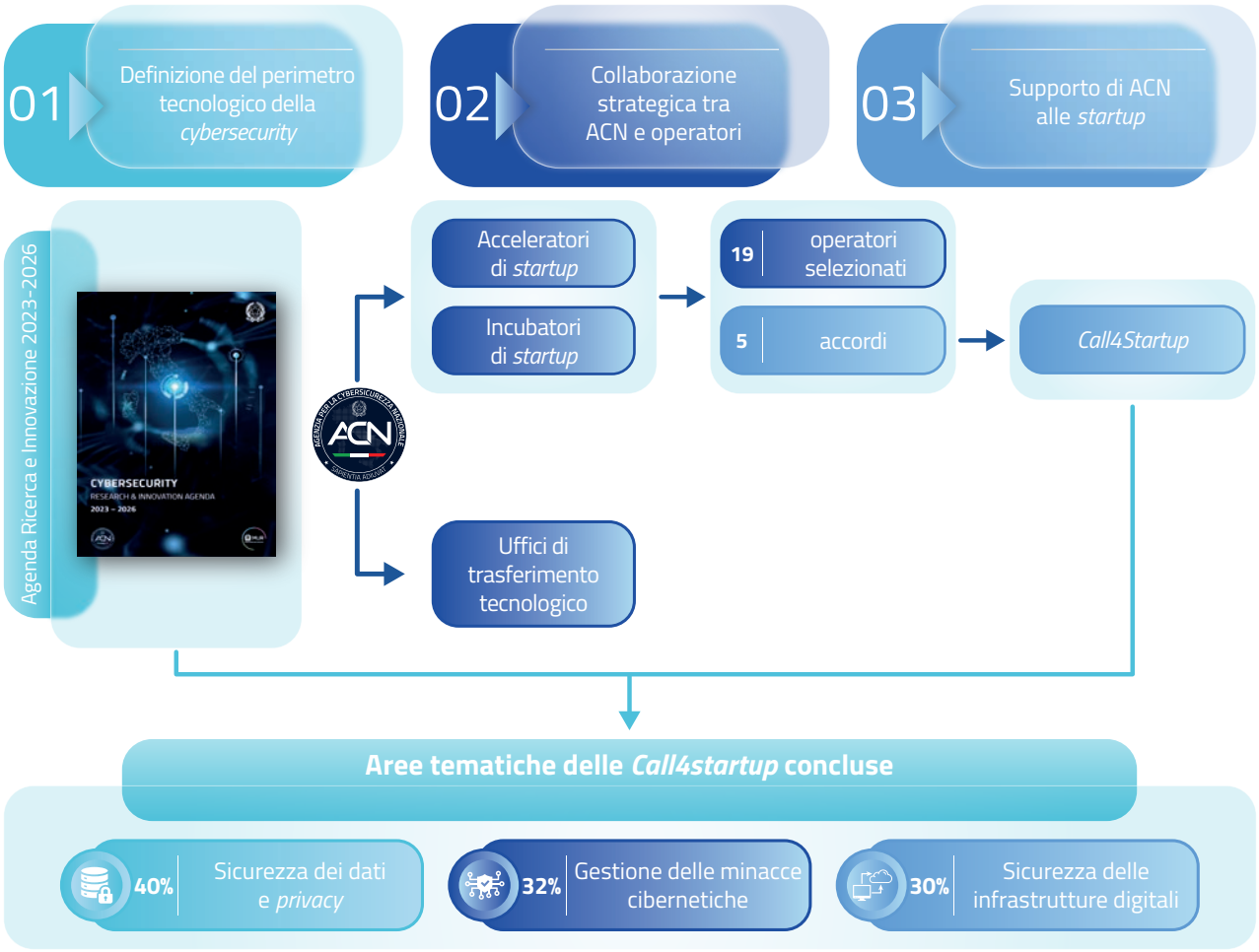


Figura 5 – Il CIN in breve

Sono stati attivati nel 2024 i primi servizi che l'Agenzia intende mettere a disposizione delle startup che entreranno nella rete del CIN. A ottobre 2024 l'Agenzia ha ospitato la sua prima iniziativa di startup matchmaking, offrendo a 14 startup, appartenenti ai 5 operatori CIN, l'opportunità di confrontarsi con potenziali investitori, partner dell'industria e utenti finali. L'iniziativa, che si è svolta nell'ambito della European Cybersecurity Challenge, ha raggiunto un gran numero di stakeholder dell'ecosistema dell'innovazione nazionale, con 95 incontri one-to-one organizzati con attori istituzionali, venture capitalist e gruppi industriali provenienti anche da altri Paesi europei.

5.3 PROGRAMMI TECNOLOGICI E DI RILEVANZA EUROPEA

Per dotare il Paese degli strumenti tecnologici più all'avanguardia nel campo della cybersicurezza, l'Agenzia ha proseguito e avviato progettualità in diversi ambiti legati alle applicazioni di cybersicurezza. In tale contesto, si sono rivelate cruciali le risorse messe a disposizione sia dal PNRR, di cui si è riferito in precedenza, che dalla Strategia nazionale di cybersicurezza 2022-2026, nonché quelle europee.

Sotto la spinta propulsiva dei finanziamenti del PNRR, è stata avviata la realizzazione della già citata infrastruttura di HPC dedicata alla cybersicurezza nazionale, a seguito del protocollo d'intesa siglato nel 2023 tra l'Agenzia e il consorzio CINECA. Nel corso del 2024 si sono concluse le attività istruttorie volte all'acquisizione, installazione e messa in esercizio del sistema di supercalcolo e sono state avviate quelle propedeutiche alla realizzazione del *data center* necessario alla funzionalità e operatività del sistema di HPC, presso il nuovo centro di calcolo del consorzio CINECA a San Giovanni a Teduccio (NA).

Si tratta di un investimento di circa 50 milioni di euro, di cui oltre 20 messi a disposizione dall'Agenzia, che permetterà di supportare il potenziamento dei servizi cyber nazionali, e in particolare dell'Hyper-SOC, sviluppando strumenti di simulazione, basati su intelligenza artificiale e *machine learning*, per potenziare le fasi di prevenzione, identificazione, risposta e predizione degli impatti di attacchi cyber.

Tramite la Strategia nazionale di cybersicurezza, sono state avviate attività rivolte tanto al settore pubblico quanto a quello privato. In particolare, rileva la promozione delle migliori pratiche di gestione dei domini di posta elettronica della Pubblica Amministrazione, attraverso un servizio di protezione dal *phishing* a tutela della sicurezza delle informazioni gestite dalla PA. Grazie alla collaborazione con IPZS, verrà, infatti, realizzato un servizio di segnalazione di *phishing*, attraverso il quale i dipendenti della Pubblica Amministrazione centrale e locale potranno far controllare e-mail sospette e ricevere un *feedback* sull'eventuale natura malevola di quanto segnalato.

Sempre in attuazione della Strategia e anche in questo caso in collaborazione con IPZS, l'Agenzia ha iniziato a lavorare per la realizzazione di prodotti e servizi ad alta affidabilità, tra cui un'infrastruttura di comunicazione nazionale. Tale iniziativa, che risponde agli interessi strategici del Paese, è finalizzata alla creazione di una piattaforma per la gestione sicura della messaggistica istantanea, per le videoconferenze *one-to-one* e per lo scambio di file, garantendo riservatezza, disponibilità e integrità dei dati tramite una piattaforma nazionale riconosciuta.

Di importanza strategica sono, inoltre, i finanziamenti europei, particolarmente quelli gestiti dal Centro europeo di competenza in cybersicurezza (vedasi Capitolo 6), nel cui quadro si incardinano i progetti ENSOC e SECURE, finanziati con fondi *Digital Europe Programme* (DEP) aggiudicati nel 2023.

Insieme alle amministrazioni di altri 6 Stati membri, l'Agenzia partecipa al progetto europeo ENSOC (*European Network of SOC* o rete europea di SOC), con un budget di 24 milioni di euro. Il progetto, in linea con quanto delineato nel *Cyber Solidarity Act*, mira alla creazione di una rete europea di SOC, con l'obiettivo di facilitare lo scambio di informazioni di cybersicurezza tra i Paesi membri partecipanti, nonché verso la Rete europea di CSIRT e ulteriori future reti di SOC europee. In particolare, il progetto consiste nello sviluppo di una piattaforma informatica transfrontaliera finalizzata a supportare l'identificazione e la prevenzione delle minacce cyber e fornire *alert* tempestivi alle autorità, nonché agli altri attori rilevanti contribuendo a rafforzare l'*European Cyber Shield*. Nel corso del 2024 sono state avviate le attività tecniche di ENSOC ed è stato bandito, nel mese di giugno, un *joint procurement* finalizzato all'approvvigionamento dei componenti infrastrutturali e tecnologici necessari all'installazione della piattaforma informatica.

Paesi del consorzio ENSOC

L'ACN ha, inoltre, promosso la costituzione di un consorzio – composto da altri 7 partner e 6 enti affiliati e coordinato dalla stessa Agenzia – che si è aggiudicato il progetto SECURE, che ha l'obiettivo di supportare le PMI europee nell'adeguamento alle previsioni del *Cyber Resilience Act* tramite l'erogazione di finanziamenti. Mediante il progetto, con un budget di 22 milioni di euro, saranno implementate due piattaforme: la prima per gestire i bandi e le candidature delle PMI per accedere ai finanziamenti, la seconda per erogare servizi alle PMI, tra cui *training*, *workshop* e materiali informativi.

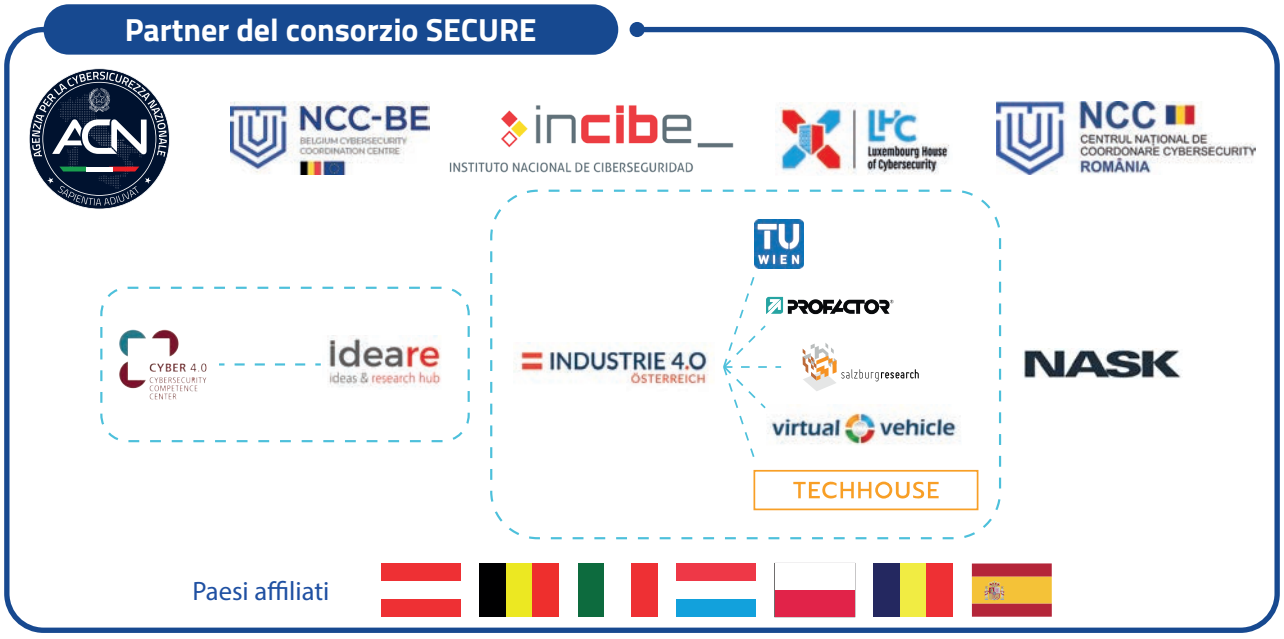


Figura 6 – Membri del consorzio SECURE

L'ACN è anche tra i promotori di un importante progetto in ambito IA, selezionato tra le sette "fabbriche di IA" europee per mettere a fattor comune capacità computazionale, dati e talenti, così da favorire lo sviluppo, l'adozione e l'utilizzo sicuro dell'intelligenza artificiale in tutta l'UE. Il progetto, denominato "*IT4LIA AI-Factory*", prevede l'installazione, presso il Tecnopolo di Bologna, di un supercalcolatore ottimizzato per l'IA, creando un ecosistema di servizi e capacità elaborativa a beneficio del mondo industriale e della ricerca. Permettendo l'accesso a un'elevata potenza computazionale, *IT4LIA AI Factory* sosterrà le evoluzioni tecnologiche dell'industria (particolarmente nei settori agroalimentare, scienze del clima e della terra, cybersicurezza e manifatturiero), oltre a contribuire allo sviluppo di *startup* e *spin-off* operanti in tali ambiti. Il progetto, che ha un budget di 430 milioni di euro, co-finanziato al 50% dalla Commissione europea e dal Governo italiano, è coordinato dal CINECA (in consorzio con Austria e Slovenia) e sostenuto da numerose e primarie istituzioni che, oltre all'ACN, includono MUR, Regione Emilia-Romagna, Istituto nazionale di fisica nucleare, Agenzia ItaliaMeteo, Fondazione per l'IA e Fondazione Bruno Kessler.

5.4 PROGRAMMI DI RICERCA

L'Agenzia, nel corso del 2024, in stretta collaborazione con il mondo accademico ha continuato a promuovere la ricerca e l'innovazione nel campo della cybersicurezza, anche a sostegno del tessuto produttivo del Paese. In particolare, tre continuano a essere le direttrici di tale percorso:

1. il costante aggiornamento del quadro di ricerca cyber, avviato nel 2023 con la pubblicazione della prima edizione della già citata Agenda di ricerca e innovazione;
2. la creazione di una rete collaborativa di soggetti di ricerca pubblici e privati che operino in sinergia con l'Agenzia per rafforzare l'ecosistema di ricerca del Paese;

3. la progettazione di un programma di investimenti in ricerca nei settori considerati strategici e in cui si riscontrano necessità di potenziamento delle capacità nazionali.

Nel 2024, l'Agenzia ha portato avanti iniziative dedicate, in particolare, alla terza di tali direttrici. Ha, infatti, pubblicato il bando per la selezione di 30 progetti di ricerca sui temi della richiamata Agenda, cui destinare il finanziamento di altrettante borse di dottorato a partire dall'anno accademico 2024/2025, per un totale di 3 milioni di euro. Tale programma mira anche a porre le basi per la creazione di una rete strutturata di collaborazioni con il mondo della ricerca accademica, prevista nella seconda delle direttrici. Ciò rappresenta, infatti, non solo un sostegno concreto a giovani ricercatori, ma anche uno strumento per coltivare sinergie con l'ecosistema di ricerca nazionale e intercettare i risultati della produzione scientifica, anche nell'ottica di promuoverne il trasferimento tecnologico verso il mondo produttivo.

La prima edizione del citato bando di dottorato, che ha avuto una considerevole partecipazione, ha portato alla selezione di 30 progetti, presentati da 17 università distribuite su tutto il territorio nazionale. Tutto ciò si pone anche in linea di continuità con la citata Agenda di ricerca e innovazione, dal momento che i progetti selezionati affrontano temi relativi a tutte le aree individuate dalla stessa. La Figura 7 descrive nel dettaglio la distribuzione dei progetti per sub-area con un focus, nella Figura 8, sulle *Emerging and Disruptive Technologies* (EDT).

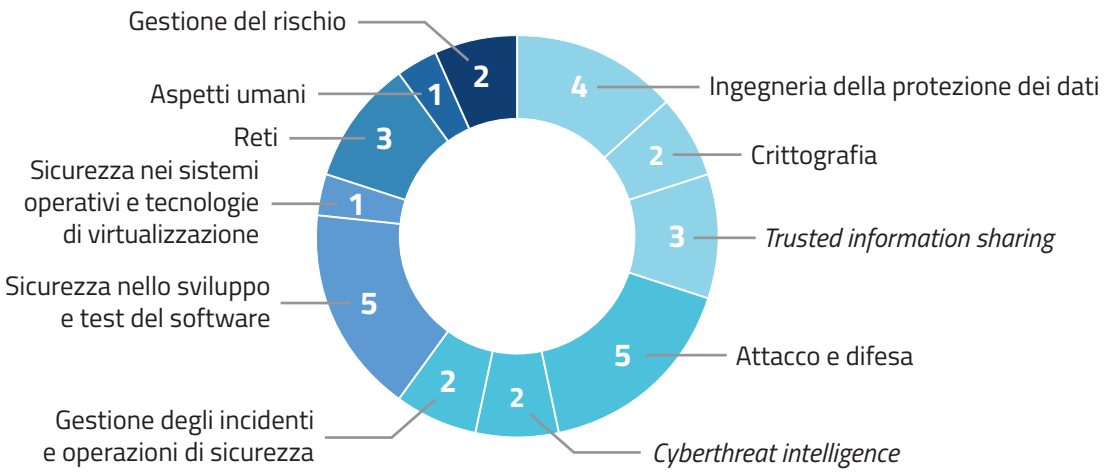


Figura 7 – Distribuzione dei progetti per sub-area dell'Agenda di ricerca e innovazione

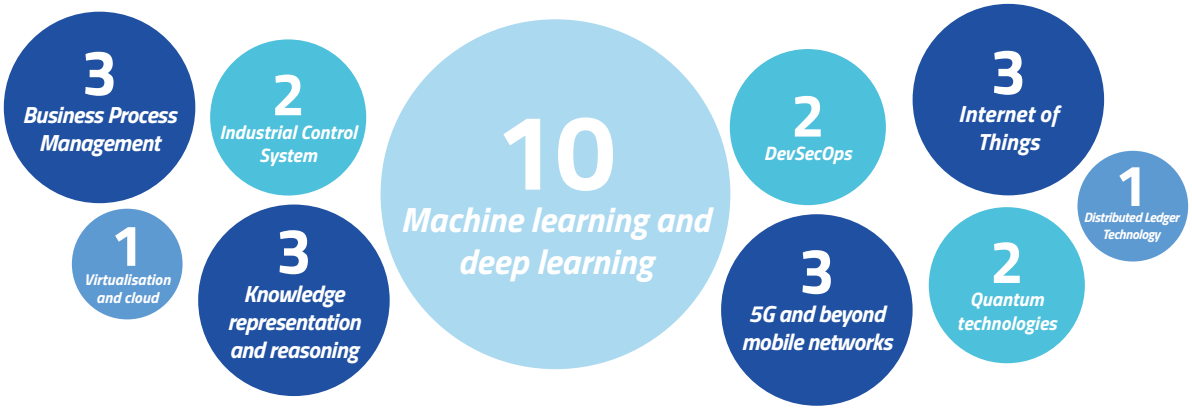


Figura 8 – Distribuzione dei progetti per EDT dell'Agenda di ricerca e innovazione

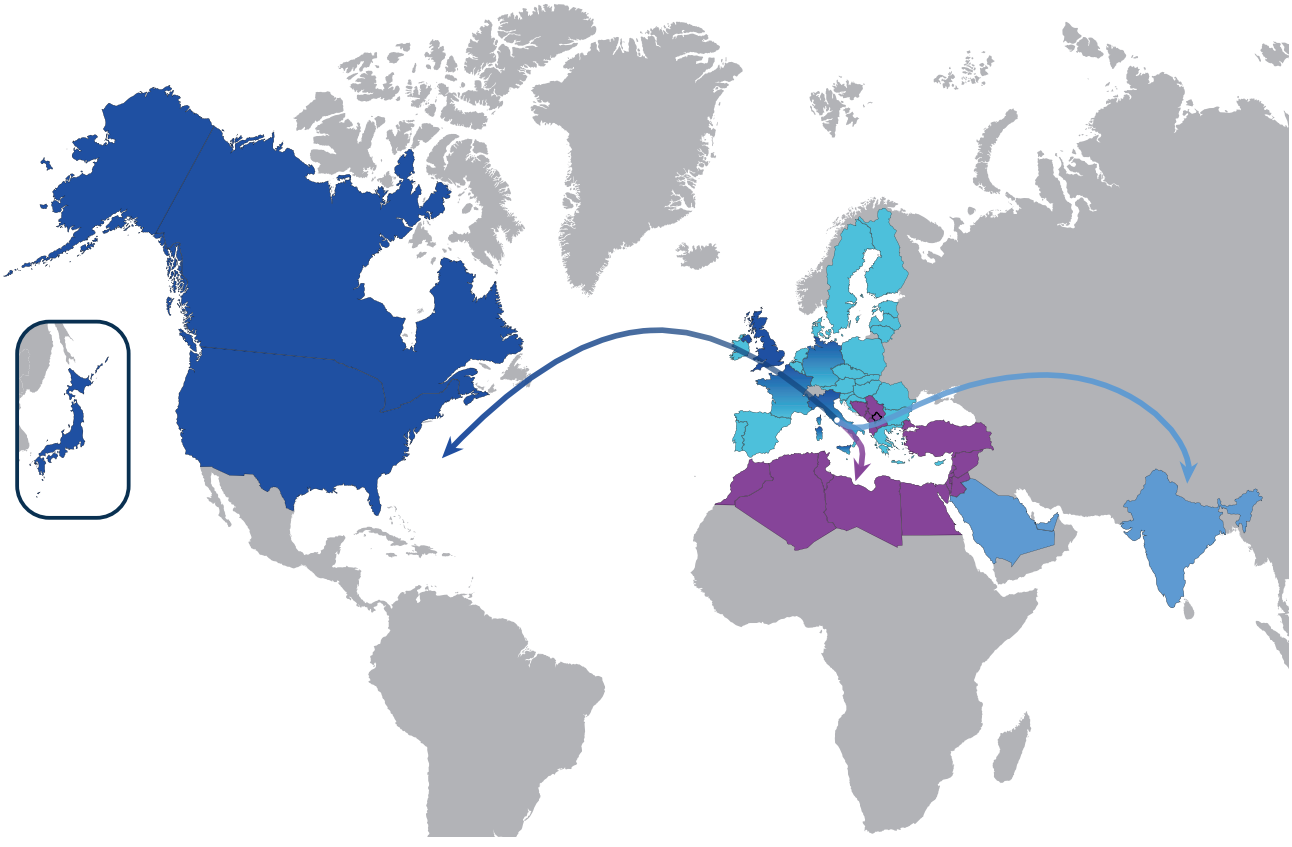
6.

COOPERAZIONE INTERNAZIONALE: DAL G7 ITALIANO UNA SPINTA PER LA COLLABORAZIONE TRA AGENZIE CYBER

La cooperazione internazionale di cybersicurezza promossa dall'Agenzia rappresenta una componente della politica estera e di sicurezza dell'Italia e uno strumento per perseguire gli interessi nazionali nel cyberspazio da una posizione adeguata alla rilevanza internazionale del Paese. In linea con le politiche del Governo e d'intesa con il MAECI, l'ACN ha promosso l'interesse nazionale nei diversi ambiti in cui si svolge la cooperazione internazionale cyber. Innanzitutto, ha continuato ad attribuire la consueta priorità alla collaborazione in sede di Unione europea, che costituisce una componente fondante della strategia di cybersicurezza del Paese, tanto a livello di *policy* quanto sul piano operativo, rappresentando un'estensione della politica nazionale in materia.

L'azione dell'Agenzia si è sviluppata secondo tre macro-direttrici, orientate verso Paesi o aree di grande importanza sotto il profilo della cybersicurezza. Si è rivolta alle agenzie e ai centri responsabili per la cybersicurezza dei Paesi del G7, con i quali si condividono interessi fondamentali in tema di sicurezza dello spazio cibernetico e di protezione degli *asset* critici per lo sviluppo della società e dell'economia. Si è indirizzata, inoltre, verso le aree del Mediterraneo allargato e dei Balcani, da sempre prioritarie per la proiezione internazionale dell'Italia. Infine, si è orientata verso i Paesi che si collocano nel c.d. corridoio IMEC (*India-Middle East Economic Corridor*), che avvicina l'India all'Europa attraverso i Paesi compresi tra il Golfo e il Mediterraneo.

L'azione lungo queste tre direttrici ha beneficiato della più importante iniziativa di politica internazionale assunta finora dall'Agenzia: la costituzione del Gruppo di lavoro G7 sulla cybersicurezza durante la Presidenza italiana del 2024.



6.1 COOPERAZIONE MULTILATERALE: IL G7 A PRESIDENZA ITALIANA E GLI ALTRI FORUM

Nell'anno della Presidenza italiana del G7, l'ACN ha contribuito a rafforzare la *governance* internazionale della cybersicurezza e la cooperazione a livello di G7 a difesa dello spazio cibernetico attraverso la costituzione del Gruppo di lavoro tra le agenzie e i centri per la cybersicurezza dei 7 Paesi e dell'Unione europea (vedasi box). L'Agenzia ha ideato, pianificato e realizzato l'iniziativa attraverso un'azione complessa, in coordinamento con lo Sherpa G7 e con il forte sostegno del MAECI, sviluppando un dialogo costruttivo con ciascun singolo partner del Gruppo. È stato necessario espandere e approfondire la rete di relazioni internazionali e coinvolgere nel dialogo interlocutori diversi, tenendo conto delle differenti architetture istituzionali che in ciascun Paese regolano la gestione delle responsabilità nel campo della sicurezza cyber.

È stato creato un formato inedito, uno spazio di cooperazione continuativa tra le agenzie dei Paesi partner G7 e dell'UE, un metodo di lavoro comune e collegiale che ha notevolmente avvicinato i partecipanti, raggiungendo un livello di interazione mai sperimentato prima. La cooperazione internazionale promossa dal Gruppo ambisce a stimolare e sostenere il dialogo politico G7 sulla sicurezza e sulla resilienza cyber, con l'obiettivo di rafforzare insieme la sicurezza nazionale e quella collettiva a vantaggio dei Paesi G7 e dell'Unione Europea.

GRUPPO DI LAVORO G7 SULLA CYBERSICUREZZA

Il Gruppo di lavoro G7 sulla cybersicurezza è un'iniziativa promossa dall'ACN durante la Presidenza italiana del G7 del 2024, con l'obiettivo di rafforzare la sicurezza e la resilienza cyber nazionale e collettiva dei Paesi partner e dell'UE. Composto dalle agenzie e dai centri per la cybersicurezza dei 7 Paesi membri e dell'Unione Europea, il Gruppo opera secondo il mandato politico ricevuto dai *leader* al Vertice di Borgo Egnazia (13-15 giugno 2024), i quali hanno espresso l'impegno a intraprendere misure concrete per rafforzare la resilienza cyber, sfruttando le sinergie con altre iniziative G7 quali l'*Ise-Shima Cyber Group*. L'azione del Gruppo si configura, infatti, come complementare alle altre attività del G7 in materia di cybersicurezza nell'ambito della *cyber diplomacy*, della sicurezza delle infrastrutture finanziarie, della resilienza tecnologica e del contrasto alla cybercriminalità. Il suo valore aggiunto risiede nell'apporto di esperienze e conoscenze specialistiche da parte di agenzie deputate alla salvaguardia e promozione della cybersicurezza e resilienza, anche per i profili di sicurezza nazionale nello spazio cibernetico.

Nel 2024 il Gruppo, presieduto dal Direttore generale dell'ACN, si è riunito a Roma a livello di vertice in due occasioni: il 16 maggio, alla Farnesina e, il 3 dicembre, presso la sede dell'ACN, con la partecipazione di tutte le agenzie e dei centri per la sicurezza e resilienza cyber dei Paesi G7, della Commissione europea ed ENISA, nonché dei Vice Consiglieri per la sicurezza nazionale di Stati Uniti e Giappone e del rappresentante del Governo canadese per la cybersicurezza. Nel corso dell'anno, il Gruppo si è, inoltre, riunito più volte a livello di punti di contatto per lo svolgimento delle attività di cooperazione di carattere operativo, compresa la discussione e il negoziato di documenti di lavoro.

La cooperazione del Gruppo si è concentrata sulla sicurezza delle catene di approvvigionamento delle infrastrutture critiche, con un focus specifico sul settore energetico, e sulla cybersicurezza dell'intelligenza artificiale. Con l'obiettivo di armonizzare i meccanismi nazionali a presidio della sicurezza delle infrastrutture critiche, il Gruppo ha svolto una ricognizione della normativa e degli standard internazionali e nazionali di cybersicurezza in materia, trovando punti di convergenza tra gli approcci e le misure adottate in ciascun Paese G7 per salvaguardare la *supply chain* di beni e servizi ICT nel settore energetico.

Sul tema della cybersicurezza dell'intelligenza artificiale, d'altro canto, il Gruppo ha voluto mettere a fattor comune le competenze e capacità dei partner al fine di comprendere meglio sia rischi e minacce derivanti dall'uso malevolo di sistemi di IA, sia le condizioni di sicurezza necessarie per beneficiare delle grandi potenzialità derivanti dall'impiego di questa tecnologia. A livello tecnico è stata, dunque, data priorità alla sicurezza delle catene di approvvigionamento delle componenti dei sistemi di IA (anche tramite le c.d. *bill of materials*) e alla protezione delle infrastrutture critiche dall'uso malevolo dell'intelligenza artificiale per attacchi cyber. Il Gruppo ha, infine, inteso avviare sinergie con altri tavoli internazionali, come ad esempio l'*AI Action Summit* e la *Counter Ransomware Initiative* (CRI).

La *Counter Ransomware Initiative* (vedasi box) è il principale foro multilaterale dedicato al contrasto al *ransomware* a cui l'ACN partecipa in rappresentanza dell'Italia, assicurando il coordinamento nazionale con le altre Amministrazioni aventi competenza in materia, in particolare il MAECI per la componente *cyber diplomacy*, i Ministeri dell'interno e della giustizia per gli aspetti di criminalità informatica e il MEF per quel che concerne il contrasto al finanziamento illecito. In stretto raccordo con queste ultime e con gli Organismi di informazione, l'ACN ha negoziato le Dichiarazioni che sono state adottate dai membri della *Counter Ransomware Initiative* nel corso del quarto Summit (Washington, 30 settembre-3 ottobre). Si tratta, nello specifico, della Dichiarazione congiunta dei partner della CRI, che enfatizza l'impegno a rafforzare la resilienza collettiva rispetto alla minaccia *ransomware*, e della Dichiarazione sulla responsabilità per attività *ransomware* malevole, che riconosce il principio secondo il quale gli attori criminali *ransomware* debbano essere ritenuti responsabili per il loro comportamento e debbano essere privati di "rifugi sicuri". Nel corso della CRI si è discusso, inoltre, del ruolo delle assicurazioni nella gestione del rischio cyber rispetto al *ransomware*, con particolare attenzione alla necessità di disincentivare il pagamento dei riscatti. L'ACN, in costante raccordo con le Amministrazioni competenti, incluso il MIMIT e l'Istituto per la vigilanza sulle assicurazioni (IVASS), e coerentemente con la linea del Governo, ha contribuito alla discussione perseguendo

Counter Ransomware Initiative

La CRI è un'iniziativa promossa dal Consiglio di sicurezza nazionale degli Stati Uniti, nata nell'ottobre del 2021 e che oggi coinvolge 63 Stati, l'Unione europea, il Consiglio d'Europa, l'Organizzazione degli Stati americani, la Commissione dell'ECOWAS e l'Interpol. Oltre a specifici progetti volti a favorire la cooperazione e lo scambio di esperienze sul tema degli attacchi ransomware, i partecipanti alla CRI si confrontano su come disarticolare il modello imprenditoriale di questi attacchi, rendendoli economicamente meno vantaggiosi. In base agli orientamenti emersi, gli attori parte della CRI si impegnano a rafforzare la protezione delle infrastrutture digitali, promuovere programmi di sensibilizzazione in materia di cybersicurezza rivolti alla popolazione, incentivare le vittime a denunciare attacchi, definire norme e linee guida su come comportarsi e negoziare in caso di attacchi ransomware e dimostrarsi non inclini a pagare i riscatti.

l'obiettivo di salvaguardare l'interesse nazionale in quest'ambito, anche a protezione degli operatori e del sistema produttivo dell'Italia.

L'attività di cooperazione internazionale dell'ACN si è svolta anche nei rilevanti consessi multilaterali presidiati dal MAECI, dove si discutono le politiche internazionali di cybersicurezza o si promuovono dedicate iniziative. In tali ambiti, l'ACN ha supportato il Ministero nella trattazione e nei negoziati di politiche e strumenti giuridici internazionali mettendo a disposizione le proprie competenze specialistiche in materia di cybersicurezza.

In ambito Nazioni Unite, in particolare, l'Agenzia ha partecipato alle 3 sessioni del Gruppo di lavoro aperto in materia di cybersicurezza (il c.d. *Open-Ended Working Group on security of and in the use of ICT* 2021-2025-OEWG) svoltesi nel 2024, contribuendo alla definizione della posizione nazionale.

L'ACN ha altresì contribuito, unitamente ai Ministeri dell'interno e della giustizia, al negoziato per la definizione della Convenzione internazionale sul contrasto all'utilizzo delle tecnologie ICT per finalità criminali (*Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes)*, adottata dall'Assemblea Generale delle Nazioni Unite nel dicembre 2024. In tale ambito, ha sostenuto l'obiettivo dell'Italia di assicurare la coerenza dell'architettura nazionale di cybersicurezza e del relativo quadro normativo e di *policy*, che dà attuazione alla Convenzione del Consiglio d'Europa sulla criminalità informatica (c.d. Convenzione di Budapest), ampiamente applicata a livello internazionale.

La sicurezza della supply chain

Nell'ambito dell'OEWG sono state discusse, tra le altre cose, proposte per affrontare a livello globale le principali criticità nell'ambito della sicurezza della supply chain per i sistemi ICT, al fine di contribuire a rafforzarne la resilienza. Si tratta di un tema di particolare rilevanza, come dimostrato dall'attenzione attribuitale in ambito G7.

Sempre a tale riguardo, l'Agenzia ha partecipato, insieme a numerose agenzie di cybersicurezza estere, al gruppo di lavoro sul tema promosso dall'omologa statunitense, la Cybersecurity and Infrastructure Security Agency (CISA). Tale gruppo si occupa di migliorare la sicurezza di prodotti e servizi ICT fin dalle fasi progettuali (la c.d. security-by-design), attraverso lo sviluppo di linee guida per l'adozione delle bill of materials, ovvero inventari delle "parti" di ciascun software con le relative specifiche, attraverso le quali incrementare la resilienza delle catene di approvvigionamento dei sistemi ICT.

L'ACN ha partecipato, inoltre, alle sessioni dell'*Informal Working Group on Cyber Issues* dell'OSCE (l'Organizzazione per la sicurezza e la cooperazione in Europa), lavorando all'obiettivo di dare attuazione alle *Confidence-Building Measures*, in particolare, alla n. 14 in materia di partnership pubblico-privato.

Con riguardo alla NATO, l'Agenzia ha continuato a seguire l'evoluzione delle politiche in materia di *cyber defence*, relativamente agli aspetti di resilienza e sicurezza cibernetica, nell'ambito del *Cyber Defence Committee*. In particolare, l'ACN ha contribuito all'esercizio e alla conferenza annuale del *Cyber Defence Pledge* e ha partecipato, assieme al MAECI e al Ministero della difesa, alla seconda edizione dell'*Annual Cyber Defence Conference*, tenutasi a Londra nel mese di novembre, che ha riunito rappresentanti in ambito politico, militare e tecnico per una discussione sulle sfide e sull'impegno della NATO in materia di difesa cyber. L'Agenzia ha partecipato, inoltre, alla prima *NATO*

Enterprise Cybersecurity Conference tenutasi a Roma presso il *NATO Defense College*, per discutere del rafforzamento dell'ecosistema cyber dell'Alleanza.

L'Agenzia ha, infine, preso parte alla *2024 Security Week* dell'Organizzazione internazionale dell'aviazione civile (*International Civil Aviation Organization*-ICAO), svoltasi in Oman nel mese di dicembre che ha adottato la Dichiarazione di Mascate sulla sicurezza e la cybersicurezza dell'aviazione civile. Tale documento afferma che la cybersicurezza è cruciale per proteggere le infrastrutture critiche e le relative catene di approvvigionamento, a fronte dei processi di innovazione tecnologica che hanno creato nuove sfide per l'aviazione.

6.2. INTEGRAZIONE EUROPEA: IMPULSO ALLE *POLICY* E ALLA COLLABORAZIONE TECNICA

La politica di cybersicurezza dell'Italia è legata a doppio filo con quella europea, data la centralità che l'Unione riveste per il nostro Paese, sia sul piano normativo che operativo. In tale ambito, l'ACN ha continuato ad assicurare la propria piena collaborazione in tutti i molteplici formati volti a potenziare la capacità dell'UE di rispondere alle diverse minacce del cyberspazio, a partire dai negoziati su nuovi atti dell'Unione fino alle interlocuzioni tecniche e alla gestione di importanti linee di finanziamento.

Innanzitutto, è stato intensificato il rapporto con la Commissione europea, attraverso colloqui con la Vice Presidente, Věra Jourová, e il Direttore generale della DG CONNECT, Roberto Viola (vedasi box). Il Direttore generale dell'Agenzia li ha incontrati a Roma, in due diverse occasioni: la prima in previsione dell'appuntamento elettorale per il rinnovo del Parlamento europeo e il secondo in occasione della già citata riunione G7.

DG CONNECT

La direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie (DG CONNECT) è il dipartimento della Commissione europea incaricato di coordinare finanziamenti, norme e iniziative politiche sul tema, contribuendo a garantire la leadership e l'indipendenza dell'UE nell'ambito delle tecnologie digitali critiche (come l'intelligenza artificiale, gli spazi comuni di dati, il calcolo ad alte prestazioni, il 5G, la microelettronica, la blockchain e la ricerca quantistica).

HWPCI

L'Agenzia ha continuato a contribuire, nell'ambito dell'*Horizontal Working Party on Cyber Issues* (HWPCI), ai negoziati sulle proposte di atti normativi UE e sui diversi aspetti di politica *cyber*, in supporto al MAECI e, in particolare, alla Rappresentanza Permanente d'Italia presso l'Unione europea. Tra i principali *dossier* esaminati dall'HWPCI nel 2024 si evidenziano, in particolare le discussioni relative al mandato di ENISA anche in vista della revisione del *Cybersecurity Act* e alla redazione del nuovo *Cyber Blueprint* per la gestione delle crisi di cybersicurezza.

Per quanto riguarda il primo punto, l'ACN ha fornito il proprio contributo nella definizione delle Conclusioni del Consiglio su ENISA (6 dicembre) dirette a semplificare l'attuale ecosistema cyber e a chiarire il mandato dell'agenzia europea, caldeggiandone il rafforzamento per favorire la cooperazione operativa e migliorare le capacità di consulenza agli Stati membri nell'attuazione di iniziative legislative e di *policy* dell'Unione. Nell'ambito del processo di revisione del *Cyber Blueprint* relativo alla risposta coordinata agli incidenti e alle crisi di cybersicurezza su vasta

scala (Raccomandazione (UE) 2017/1584) l'ACN ha contribuito al dibattito sulla definizione di chiari ruoli e responsabilità di tutti i soggetti a vario titolo coinvolti nel processo di preparazione e gestione delle crisi cyber.

All'interno del quadro vigente, l'Agenzia continua ad assicurare il proprio contributo per la prevenzione e preparazione a situazioni di crisi cibernetica in ambito UE, sia a livello operativo che tecnico, anche tramite le reti dedicate. A tale riguardo, un'importante novità è contenuta nel decreto legislativo di recepimento della Direttiva NIS2 (vedasi Capitolo 1), che ha conferito all'Agenzia e al Ministero della difesa il ruolo di autorità nazionali per la gestione di incidenti e crisi di cybersicurezza su vasta scala, ciascuno per gli ambiti di competenza, prevedendo per l'ACN anche compiti di coordinamento. Ciò contribuirà a rendere operativi i meccanismi per affrontare, a diversi livelli, le crisi cyber che possono interessare l'Unione.

Nel quadro della gestione delle crisi a livello UE, l'Agenzia rappresenta l'Italia nella rete EU-CyCLONe, istituita nel 2020 e formalizzata dalla citata Direttiva NIS2 al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala e di garantire il regolare scambio di informazioni tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione.

Nel corso del 2024, l'ACN ha preso parte attivamente alle riunioni di coordinamento con le altre agenzie dei Paesi UE deputate alla gestione delle crisi cyber su vasta scala, culminate con l'esercitazione *BlueOLEx 24*, ospitata proprio dall'ACN a Roma (vedasi Capitolo 3). L'iniziativa è stata pianificata nel corso dell'anno da un gruppo di lavoro dedicato, coordinato dall'Agenzia insieme al Lussemburgo. Inoltre, sono proseguite le attività di definizione delle modalità di funzionamento di EU-CyCLONe tramite l'adozione del regolamento interno che definisce la politica di condivisione delle informazioni. Sono continuati, inoltre, i lavori di revisione delle procedure operative standard, sui processi di gestione crisi e di collaborazione con il livello politico e tecnico in ambito UE. L'Agenzia ha contribuito, infine, all'elaborazione della prima relazione al Parlamento europeo e al Consiglio sulla valutazione del lavoro della rete.

Nel 2024 l'ACN, con il CSIRT Italia, ha continuato a collaborare all'interno del *CSIRTs Network*, la Rete di CSIRT dei 27 Stati membri dell'Unione istituita con la Direttiva NIS e ulteriormente rafforzata dalla NIS2. La rete prosegue nella propria attività di sviluppo e rafforzamento della cybersicurezza a livello europeo al fine di proteggere le infrastrutture critiche e i servizi essenziali da attacchi informatici.

In tale rete di carattere tecnico il CSIRT Italia si interfaccia, tramite canali dedicati, con gli omologhi degli altri Paesi UE attraverso reciproci scambi informativi e un tempestivo coordinamento della risposta operativa agli incidenti, oltre che fornendo supporto nella gestione di incidenti transfrontalieri e, in prospettiva, nella *coordinated vulnerability disclosure*. Il CSIRT Italia ha assicurato la partecipazione a tutti gli incontri del *CSIRTs Network* e alle riunioni plenarie per discutere e analizzare minacce informatiche, vulnerabilità e incidenti di sicurezza. Ha, inoltre, partecipato attivamente ai diversi gruppi di lavoro, con l'obiettivo di migliorare le procedure e gli strumenti in uso della rete.

NIS Cooperation Group

Con l'entrata in vigore della Direttiva NIS2, il mandato del Gruppo di cooperazione NIS è stato esteso e rafforzato, al fine di favorire la discussione a livello UE tra le Autorità nazionali competenti NIS e i Punti di contatto NIS degli Stati membri, della Commissione e di ENISA, per le tematiche inerenti alla cybersicurezza. L'Agenzia ha preso parte attivamente alle 4 riunioni plenarie annuali, nonché ai gruppi di lavoro, assicurando la co-presidenza dei gruppi dedicati alle telecomunicazioni, alla gestione di incidenti e crisi su vasta scala, alle valutazioni del rischio e alla sicurezza della *supply chain*. Ha, inoltre, contribuito alla riorganizzazione dei gruppi di lavoro, adeguandoli alle aspettative che discendono dalla nuova disciplina NIS. Con l'istituzione del nuovo gruppo di lavoro dedicato alla crittografia *post-quantum* questi sono giunti a 17.

Notevole attenzione è stata dedicata alle azioni strutturali di mitigazione dei rischi cyber derivanti dal contesto geopolitico. A tale riguardo, si è discusso, in particolare, della sicurezza e resilienza cyber del settore delle telecomunicazioni, emanando raccomandazioni sia di carattere strategico che tecnico, oltre che esaminando i rischi intersettoriali che riguardano le telecomunicazioni e l'energia elettrica. È proseguita, inoltre, l'analisi di rischi e opportunità legate ai cavi sottomarini nonché alle catene di approvvigionamento. In vista delle elezioni europee di giugno 2024, il Gruppo ha, altresì, approfondito le implicazioni di cybersicurezza delle tecnologie usate ai fini elettorali, anche alla luce della minaccia ibrida.

Non da ultimo, il tema che ha maggiormente impegnato il Gruppo nel corso del 2024 è stato il recepimento della Direttiva NIS2, fornendo supporto agli Stati membri specialmente per quel che concerne i settori infrastrutture digitali e servizi digitali, anche tramite una specifica raccomandazione. Sempre nell'ambito delle infrastrutture digitali, l'ACN partecipa anche alla *European Competent Authority on Secure Electronic Communication* (ECASEC), che è attualmente impegnata a traghettare il complesso e articolato settore delle telecomunicazioni dalla precedente disciplina contenuta nel Codice europeo delle comunicazioni elettroniche al nuovo paradigma orizzontale declinato dalla Direttiva NIS2.

European Cybersecurity Certification Group

L'Agenzia, in qualità di Autorità nazionale per la certificazione di cybersicurezza, partecipa alle attività dell'*European Cybersecurity Certification Group* (ECCG), istituito dal *Cybersecurity Act*. L'ECCG è chiamato a proporre eventuali nuovi ambiti per possibili futuri schemi di certificazione della cybersicurezza, a fornire la propria opinione sulle proposte di atti di esecuzione per gli schemi europei di certificazione della cybersicurezza e a gestire quelli già avviati. Il 2024 è stato un anno particolarmente intenso, considerando l'avvio del primo schema di certificazione della cybersicurezza (il già citato EUCC), nonché il consolidamento di regole e procedure dell'ECCG. L'Agenzia ha contribuito, in particolare, all'aggiornamento dell'atto di esecuzione di EUCC per l'inclusione di standard tecnici aggiornati e linee guida operative, alla transizione dal circuito di mutuo riconoscimento di certificati europei emessi dagli schemi nazionali al nuovo schema europeo, nonché a predisporre soluzioni a breve termine per conservare i benefici dell'accordo di mutuo riconoscimento internazionale dei certificati di cybersicurezza di prodotti ICT emessi da schemi nazionali.

Sempre all'interno dell'ECCG, inoltre, l'ACN ha contribuito alla proposta di revisione del CSA volta a includere i servizi di sicurezza gestiti quali possibile oggetto di certificazione. Si tratta di servizi di

cybersicurezza che sostengono l'intero ciclo degli incidenti di cybersicurezza, dalla preparazione, prevenzione, rilevamento, e analisi, alla mitigazione degli incidenti, risposta e *recovery*. La modifica è stata recepita nel Regolamento (UE) 2025/37, il cui testo è stato approvato il 19 dicembre 2024 e pubblicato nella Gazzetta Ufficiale dell'Unione europea del 15 gennaio 2025.

European Cybersecurity Competence Centre

L'Agenzia ha continuato a potenziare le proprie funzioni di Centro nazionale di coordinamento (NCC), a supporto del Centro europeo di competenza in cybersicurezza (*European Cybersecurity Competence Centre*-ECCC) per il rafforzamento dello sviluppo industriale, tecnologico e di ricerca in materia di *cybersecurity* anche tramite gli investimenti offerti dai programmi *Digital Europe Programme* e *Horizon Europe*.

Nell'ambito dell'NCC, l'Agenzia ha consolidato l'ecosistema nazionale di cybersicurezza aggregando organizzazioni industriali, PMI, università, enti, consorzi e altri soggetti di ricerca, nonché ulteriori portatori di interessi in materia di cybersicurezza. I soggetti aderenti alla *community* dell'NCC possono essere supportati nella partecipazione ai bandi di progetti DEP e *Horizon* e sviluppare sinergie con gli altri *stakeholder* a livello nazionale ed europeo. Nel corso del 2024 l'Agenzia, in qualità di NCC, ha organizzato 5 eventi (un *matchmaking* tra *startup* e investitori, due *training*, un *Info Day* e una sessione di approfondimento sulle opportunità di finanziamento europee in cybersicurezza).

Nel 2024, inoltre, l'Agenzia – oltre a proseguire nell'attuazione dei progetti ENSOC e SECURE (vedasi Capitolo 5) – ha ottenuto il finanziamento per altri due progetti grazie all'aggiudicazione di nuovi bandi DEP. Uno di questi è il progetto EUSAiR, che mira a creare spazi di sperimentazione normativa per testare i sistemi di intelligenza artificiale e accompagnare l'attuazione dell'*AI Act* (vedasi Capitolo 1). L'altro è il progetto AKADIMOS, per la creazione di una piattaforma comune per la formazione cyber nell'UE (vedasi Capitolo 7).

L'NCC continua, altresì, ad assicurare la rappresentanza italiana nel *Governing Board* dell'ECCC, nell'attuazione della missione e degli obiettivi del Centro, prendendo parte anche ai gruppi di lavoro tematici, al fine di assicurare un'adeguata e costante valorizzazione degli interessi nazionali in materia di cybersicurezza.

ENISA

L'ACN ha continuato a sostenere convintamente le attività di ENISA (l'Agenzia dell'Unione europea per la cybersicurezza), assicurando la rappresentanza nel suo *Management Board* e nella rete dei funzionari di collegamento (*National Liaison Officer*). Ha, in particolare, partecipato ai lavori in merito a:

- *EU Cybersecurity Index*, indice volto a valutare i livelli di maturità cyber dell'UE e degli Stati membri in 4 aree (*policy*, capacità, operatività, sviluppo del mercato e del settore industriale). L'esercizio, che ha visto l'ACN nel ruolo di coordinatore del contributo nazionale per il 2024, fornirà una panoramica sulla cybersicurezza dell'Unione, con l'obiettivo di potenziarla. Gli esiti dell'esercizio, che dopo due edizioni pilota è entrato nella fase ufficiale, confluiranno nella Relazione sullo stato della cybersicurezza nell'Unione, presentata da ENISA al Parlamento europeo con cadenza biennale, ai sensi della Direttiva NIS2. L'Italia ha ottenuto

un punteggio complessivo superiore alla media UE, particolarmente per quel che riguarda indicatori che vanno dalla resilienza degli enti importanti ed essenziali alla cooperazione internazionale e dal monitoraggio della minaccia al contrasto al *cybercrime*.

- *National Cybersecurity Strategies*, il gruppo di esperti incaricati di costituire una piattaforma per lo scambio di buone pratiche e di supportare gli Stati membri nell'implementazione delle rispettive strategie nazionali di cybersicurezza. In tale contesto, l'ACN ha presentato il quadro di *governance* e la strategia nazionale vigente, inclusi gli strumenti finanziari a disposizione e i risultati sinora raggiunti.
- *Cyber Europe Planners*, impegnato nella pianificazione e nell'esecuzione della già citata esercitazione paneuropea di gestione crisi, *Cyber Europe 2024* (vedasi Capitolo 3).

Ulteriori formati

L'ACN ha dato il proprio apporto anche in merito al futuro impianto della cooperazione civile-militare dell'UE in ambito cyber, particolarmente in relazione alla proposta di creazione di un Centro di coordinamento per la cybersicurezza dell'Unione (*EU Cyber Defence Coordination Centre*), destinato a divenire un punto di raccolta e coordinamento informativo a beneficio della Conferenza dei Comandanti cyber dell'Unione. Sempre in materia di difesa cyber, l'ACN ha fornito la propria prospettiva nell'esercizio annuale del *Cyber Census*, questionario relativo allo stato di attuazione, a livello nazionale, della politica UE sulla *cyber defence*.

L'ACN ha, altresì, seguito gli aspetti di sicurezza e resilienza cyber nell'ambito delle discussioni in seno all'Unione europea sulla minaccia ibrida, incluso il Rapporto sul rafforzamento della preparazione e della prontezza civile e militare dell'UE, elaborato dal Consigliere Speciale della Commissione europea, Sauli Niinistö (vedasi box).

Rapporto sul rafforzamento della preparazione e della prontezza civile e militare dell'UE

Il 30 ottobre 2024 la Presidente della Commissione europea, Ursula von der Leyen, e l'ex Presidente finlandese, Sauli Niinistö, hanno presentato il rapporto "Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness", volto a migliorare la preparazione e la resilienza dell'UE a fronte di minacce globali sempre più complesse, sulla base di un approccio multi-rischio che coinvolga l'intera società e ogni livello di governo. Il rapporto propone un approccio integrato di risposta comune europea alle crisi, sia di natura cyber che militare che ibrida. Una particolare importanza è attribuita alla protezione quale elemento indispensabile per la capacità dell'Unione di esercitare deterrenza, alla necessità di estendere il quadro di resilienza delle infrastrutture critiche stabilito dalle Direttive CER e NIS2 ad altri settori rilevanti, nonché al rafforzamento della cooperazione con la NATO per una risposta coordinata in tempi di crisi.

L'Agenzia ha, infine, preso parte a tutte le riunioni del *Cybersecurity Directors Meeting*, formato unico nel suo genere, che riunisce i direttori delle agenzie dell'UE e di alcuni Paesi terzi (Regno Unito, Svizzera e altri all'occasione invitati come osservatori) per discutere e promuovere iniziative di politica internazionale ed europea di cybersicurezza, favorendo il coordinamento tra i partecipanti. In tale ambito, sono stati approfonditi *dossier* prioritari per l'Agenzia, quali la cybersicurezza e l'IA, l'implementazione della Direttiva NIS2, il rafforzamento della gestione e risposta a minacce e crisi cyber e il supporto allo sviluppo di capacità cyber, oltre al cruciale tema della crittografia *post-quantum*.

ATTIVITÀ INTERNAZIONALI SULLA CRITTOGRAFIA *POST-QUANTUM*

L'Agenzia è attivamente coinvolta nella transizione verso algoritmi crittografici resistenti alla minaccia quantistica (vedasi Capitolo 4), collaborando a tutti i livelli con le diverse controparti internazionali.

A livello UE, un importante sviluppo è stato rappresentanto dalla pubblicazione da parte della Commissione europea, ad aprile 2024, di una Raccomandazione per la stesura di una tabella di marcia coordinata per la transizione alla crittografia *post-quantum*. In tale raccomandazione, gli Stati membri sono incoraggiati a formare un gruppo di lavoro ad hoc, in seno al Gruppo di cooperazione NIS, per programmare la transizione verso sistemi *post-quantum* mettendo a fattor comune le esperienze di tutti gli Stati membri. È stato, dunque, istituito il *Work Stream on Post-Quantum Cryptography*, inaugurato con un incontro a settembre 2024.

In parallelo, nell'ambito del *Cybersecurity Directors Meeting*, l'Agenzia ha sottoscritto, insieme a 18 Stati membri dell'UE, il paper condiviso "*Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography*". Nato su impulso dell'agenzia cyber tedesca, il documento ribadisce l'urgenza di avviare un percorso di transizione comune a tutta l'Unione per la sostituzione delle attuali soluzioni crittografiche con degli algoritmi *post-quantum* validati dalla comunità scientifica.

L'ACN continua ad aggiornarsi rispetto agli sviluppi internazionali sulla crittografia, con particolare riguardo al processo di standardizzazione *post-quantum* del *National Institute of Standards and Technology* statunitense. A tale riguardo, ad aprile 2024, l'Agenzia è stata rappresentata alla relazione annuale del NIST a Washington sul processo di standardizzazione dei nuovi algoritmi, in cui sono stati discussi i prossimi passi che l'amministrazione USA intende seguire per arginare la minaccia quantistica.

In ambito NATO, infine, l'Agenzia partecipa, insieme al MAECI e al Ministero della difesa, alla *Transatlantic Quantum Community*, che riunisce esperti di tecnologie quantistiche provenienti dai governi, dal settore produttivo, dal mondo accademico, dagli enti di finanziamento e dagli istituti di ricerca. A novembre 2024, l'Agenzia ha partecipato alla prima sessione plenaria della *community*, oltre ai lavori preparatori nel cui ambito sono stati definiti e avviati molteplici filoni progettuali focalizzati, tra gli altri, all'individuazione di casi d'uso civili-militari per le tecnologie quantistiche.

6.3 COOPERAZIONE BILATERALE: AMPLIAMENTO DEI PARTNER

Nel corso del 2024, lo sviluppo del dialogo e la costruzione di rapporti di collaborazione tra l'Agenzia e le principali omologhe autorità di cybersicurezza di altri Paesi si sono significativamente intensificati. Sono cresciute, per quantità e qualità, tanto le interazioni di natura tecnico-operativa, quanto le iniziative per coordinare politiche di cybersicurezza. Un'azione che ha coinvolto l'ACN a partire dai suoi vertici e che le ha consentito di stabilire partnership strategiche, destinate a consolidarsi nel tempo, nonché di aumentare la propria capacità di incidere sulle politiche di cybersicurezza e di contribuire a plasmare la politica e la cooperazione internazionale in questo settore.

I numerosi incontri di alto livello con i vertici di autorità e agenzie di cybersicurezza hanno svolto un ruolo chiave in tal senso. Tra questi, vanno menzionati i colloqui e le interazioni del Direttore generale con numerosi interlocutori, oltre ai già citati vertici UE. Si sono svolti incontri con la Vice Consigliera per la sicurezza nazionale con delega per il cyber e le tecnologie emergenti al Consiglio nazionale di sicurezza degli Stati Uniti, la Direttrice dell'Agenzia per la cybersicurezza e la sicurezza delle infrastrutture degli Stati Uniti, il Vice Ministro per l'industria del Canada e l'Alto funzionario del Governo canadese per la cybersicurezza, la Presidente dell'Ufficio federale per la sicurezza informatica (BSI) della Germania, il Segretario Generale della difesa e della sicurezza nazionale della Francia, il Direttore generale dell'Agenzia spagnola di cybersicurezza, il Ministro per la protezione civile e la pianificazione della gestione delle emergenze del Ministero della difesa della Svezia, il Governatore per l'Autorità nazionale per la cybersicurezza dell'Arabia Saudita, la Ministra per le comunicazioni e la digitalizzazione del Ghana.

Altrettanto importanti al fine di costruire la rete di collaborazioni bilaterali dell'ACN con agenzie di Paesi *like-minded* sono stati i molteplici incontri di natura operativa tra le varie articolazioni dell'ACN e le omologhe istituzioni estere, organizzati anche grazie alla collaborazione delle Ambasciate straniere in Italia e della rete diplomatica e consolare nazionale all'estero.

Il già citato Gruppo di lavoro G7 sulla cybersicurezza ha dato, inoltre, impulso a più intense collaborazioni operative con le singole agenzie partner. In particolare, l'Agenzia ha rafforzato la cooperazione con le agenzie di Germania (BSI), Francia (ANSSI), Unione europea (ENISA) e Stati Uniti (CISA). Sono state avviate regolari e frequenti consultazioni su metodologie e migliori pratiche per affrontare le comuni sfide di cybersicurezza e per definire posizioni condivise su questioni di politica internazionale cyber. Ne sono evidenza il comune orientamento sulla transizione alla crittografia *post-quantum* espresso nel già citato documento, ovvero l'avvio di un tavolo di lavoro informale con l'agenzia francese per la condivisione di esperienze sulla gestione della cybersicurezza di grandi eventi, in vista delle Olimpiadi invernali di Milano-Cortina 2026.

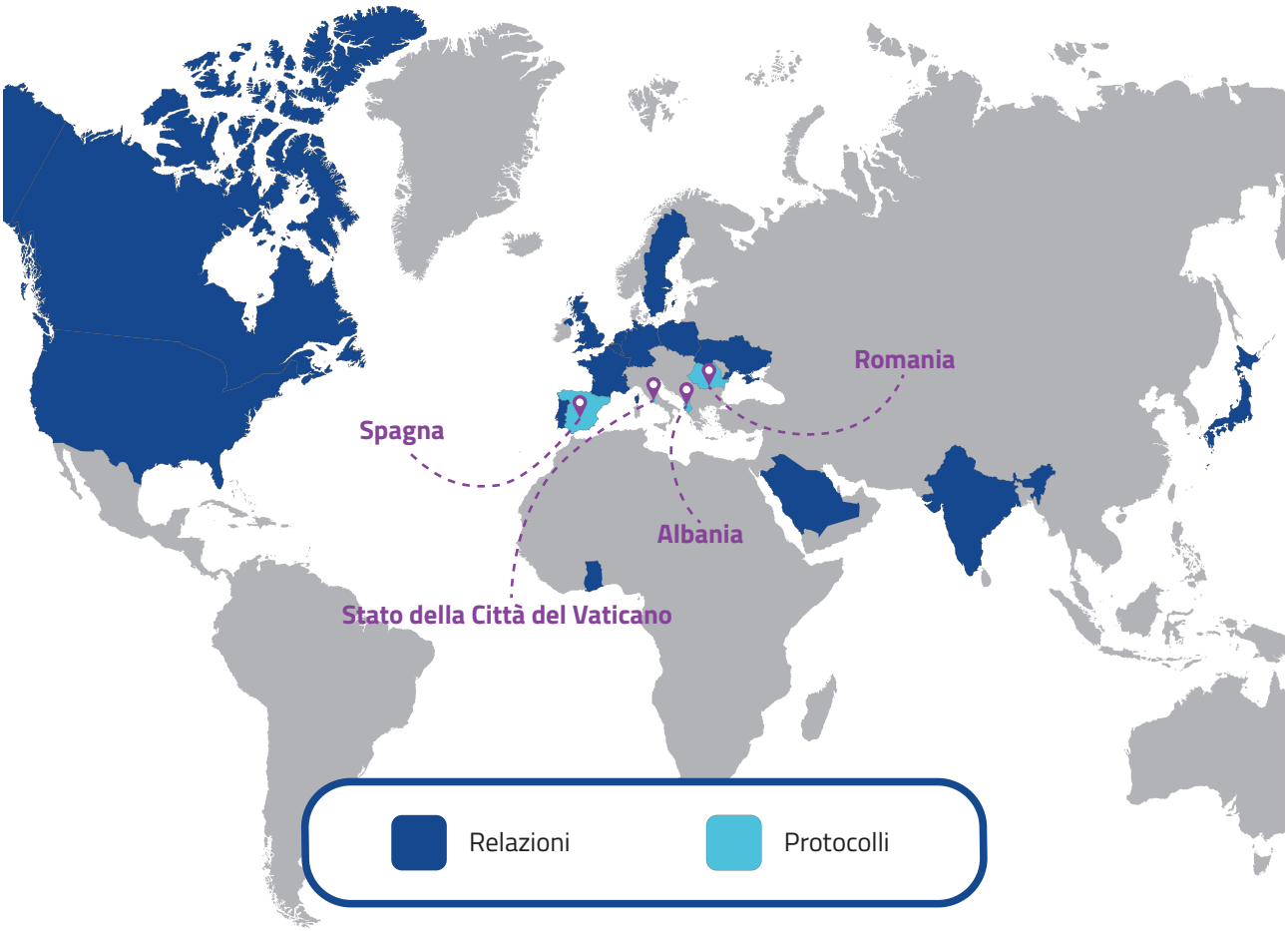
Allargando la collaborazione con le agenzie cyber dei Paesi G7 (e in particolare la britannica NCSC, la canadese CCCS e la giapponese NISC) l'ACN – che è la più giovane tra le agenzie G7 – è ancor più in condizione di dialogare con i principali *player* di cybersicurezza *like-minded* dal Nord Atlantico al Pacifico su temi di decisiva importanza per la sicurezza dell'Italia, quali la cybersicurezza dell'intelligenza artificiale, la protezione di infrastrutture critiche transfrontaliere, il contrasto al *ransomware*, la sicurezza dei dati a supporto dell'autonomia strategica e della sovranità digitale.

Alla collaborazione sviluppata con i partner G7, si aggiungono quelle che l'ACN ha stabilito con i centri per la cybersicurezza di Albania, Romania, Spagna e con il Governatorato dello Stato della Città del Vaticano, attraverso la sottoscrizione di 4 nuovi protocolli d'intesa internazionali. I protocolli definiscono una cornice di cooperazione che, complessivamente, guarda alla sicurezza dell'Europa e del Mediterraneo, consentendo di perseguire obiettivi condivisi di cybersicurezza regionale. Tale cornice incentiva lo scambio di informazioni sulle minacce e sugli incidenti cyber, favorisce la condivisione di buone prassi ed esperienze, agevola la pianificazione di esercitazioni

congiunte, la definizione di programmi di formazione e di sviluppo di soluzioni tecnologiche per accrescere le competenze e le capacità di prevenzione e risposta.

L'Agenzia ha sviluppato collaborazioni anche con centri cyber di altri Paesi dell'UE. In particolare, oltre all'Istituto nazionale per la cybersicurezza (INCIBE) della Spagna, con il Centro per la cybersicurezza del Belgio (CCB) e con il Centro nazionale di cybersicurezza del Portogallo (CNCS), l'Istituto nazionale di ricerca della Polonia (NASK), il Centro nazionale di cybersicurezza dei Paesi Bassi (NCSC), nonché la *House for cybersecurity* del Lussemburgo e la Direzione nazionale per la sicurezza informatica della Romania soprattutto nell'ambito dei consorzi ENSOC e SECURE (vedasi Capitolo 5) per la realizzazione di una piattaforma europea per il rilevamento di minacce e lo scambio di informazioni di cybersicurezza a livello europeo.

A supporto dell'azione di politica estera e di sicurezza nazionale dell'Italia, l'Agenzia ha, inoltre, avviato contatti con le autorità per la cybersicurezza dell'India – tramite la partecipazione al primo *India-Italy Cyber Dialogue* svoltosi nel mese di ottobre – dell'Arabia Saudita e dell'Ucraina.



La propensione dell'ACN allo sviluppo di rapporti internazionali risponde anche all'obiettivo di favorire, da un lato, programmi di ricerca e sviluppo tecnologico e, dall'altro, iniziative di c.d. *cyber capacity building* volte, cioè, allo sviluppo e al potenziamento delle capacità tecnologiche e delle competenze cyber di Paesi, organizzazioni o comunità per affrontare le sfide in ambito cibernetico. La crescente importanza del *capacity building* per la proiezione internazionale dell'Agenzia e del Paese ha trovato riscontro nella prima Conferenza nazionale sul *cyber capacity building* organizzata dall'ACN e dal MAECI (vedasi box). In tale ambito, inoltre, nel corso del 2024 l'ACN ha rivolto le proprie attività verso funzionari e dirigenti pubblici di diverse aree considerate prioritarie: Balcani (Albania, Bosnia ed Erzegovina, Kosovo, Macedonia del Nord, Montenegro e Serbia), Africa e Medio Oriente (in particolare Giordania) e America Latina (Repubblica Domenicana e Uruguay, nel quadro del progetto europeo di *capacity building EU CyberNet*).

Ecosistema nazionale di cyber capacity building

In collaborazione con il MAECI, l'ACN ha organizzato la prima Conferenza nazionale sul cyber capacity building, svoltasi alla Farnesina il 2 luglio. L'evento ha riunito rappresentanti di enti pubblici, privati e del mondo accademico per dare vita a un ecosistema nazionale a favore di Paesi terzi che consenta di soddisfare le crescenti richieste di collaborazione che pervengono in quest'ambito sul piano internazionale. I lavori hanno permesso di approfondire le priorità operative e geografiche del cyber capacity building (Balcani, Mediterraneo allargato e Africa, America Latina) e il necessario sostegno all'internazionalizzazione del sistema cyber italiano ed europeo, con particolare riguardo al partenariato pubblico-privato.

7.

IL FATTORE UMANO: FORMAZIONE E PROMOZIONE DELLA CULTURA DELLA CYBERSICUREZZA

Il fattore umano è assolutamente imprescindibile per proteggere la superficie digitale del Paese, poiché anche i migliori presidi tecnologici richiedono sempre il coinvolgimento delle persone, sia come professionisti sia come utenti. L'ACN lavora per diffondere le competenze cyber a tutti i livelli per garantire una forza lavoro adeguatamente formata e una cittadinanza consapevole di come utilizzare in sicurezza gli strumenti informatici.

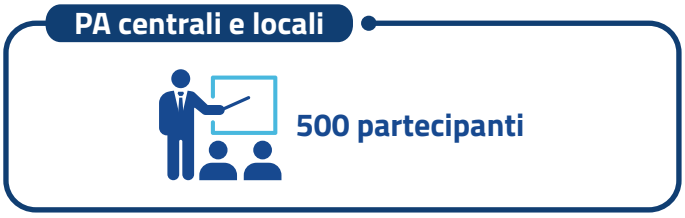
La formazione e la promozione della cultura della cybersicurezza sono stati individuati dalla Strategia nazionale di cybersicurezza 2022-2026 quali fattori abilitanti necessari per raggiungere gli obiettivi di protezione, risposta e sviluppo previsti dalla Strategia medesima.

Il confine tra le attività di formazione e quelle volte alla promozione della cultura cyber è estremamente labile e necessita di una visione olistica; tuttavia, nei paragrafi che seguono si è comunque provveduto a differenziare le attività e le iniziative formative da quelle che invece presentano una connotazione più spiccatamente divulgativa.

7.1 LE INIZIATIVE DI FORMAZIONE

La formazione in cybersicurezza è cruciale nell'era digitale attuale, specie in relazione alle nuove tecnologie. Le iniziative realizzate dall'Agenzia nel corso del 2024 sono state principalmente volte ad avviare un processo utile a stimolare la creazione di una forza lavoro nazionale, composta da soggetti esperti in possesso delle capacità e delle competenze necessarie per poter essere applicate a beneficio delle imprese e delle Amministrazioni pubbliche. Ciò, sia con riferimento alle tecnologie informatiche in generale, sia a quelle relative alla sicurezza cibernetica in particolare.

Nel 2024 l'Agenzia ha dato specifico impulso all'attività di formazione rivolta ai giovani e alla PA. Rispetto a quest'ultima, è proseguita la collaborazione con la Scuola nazionale dell'Amministrazione (SNA), organizzando corsi, di livello base e avanzato, rivolti a dipendenti delle PA, centrali e locali, con oltre 500 partecipanti. Tenuto conto della rilevanza sia in termini numerici sia per i servizi ai cittadini dei quasi 8.000 Comuni italiani, sono state intraprese numerose iniziative formative con l'Associazione nazionale dei Comuni italiani. In questo contesto, l'Agenzia ha contribuito all'avvio della piattaforma di formazione online predisposta dall'ANCI (Accademia dei Comuni digitali), realizzando un ciclo di seminari volti a illustrare le più recenti disposizioni introdotte dalla legge n. 90/2024 per il rafforzamento dei livelli di sicurezza cibernetica di tutte le Pubbliche Amministrazioni, comprese quelle locali. Tale formazione è stata anche erogata in occasione del convegno nazionale organizzato dall'ANCI che ha visto la partecipazione di una vastissima platea di soggetti.



Sono state poi svolte attività di formazione nei confronti di altre Amministrazioni quali il Corpo nazionale dei Vigili del fuoco, la Marina militare e la Banca d'Italia.

Unitamente al CINI, alcuni esperti dell'Agenzia hanno partecipato a incontri di formazione destinati ai docenti degli istituti scolastici di secondo grado.

7.1.1 Accordi e protocolli d'intesa in ambito formazione

Al fine di potenziare le attività di formazione sono stati stipulati accordi e protocolli d'intesa. Si riportano di seguito alcuni accordi significativi dell'importanza attribuita alla formazione ai diversi livelli: scolastico, di alta specializzazione tecnologica, post-diploma e universitario. In questo contesto, assume particolare rilievo per preparare le nuove generazioni ad affrontare il mondo digitale, il protocollo d'intesa siglato con il Ministero dell'istruzione e del merito, volto a promuovere l'educazione informatica e cibernetica nelle scuole italiane di ogni ordine e grado.

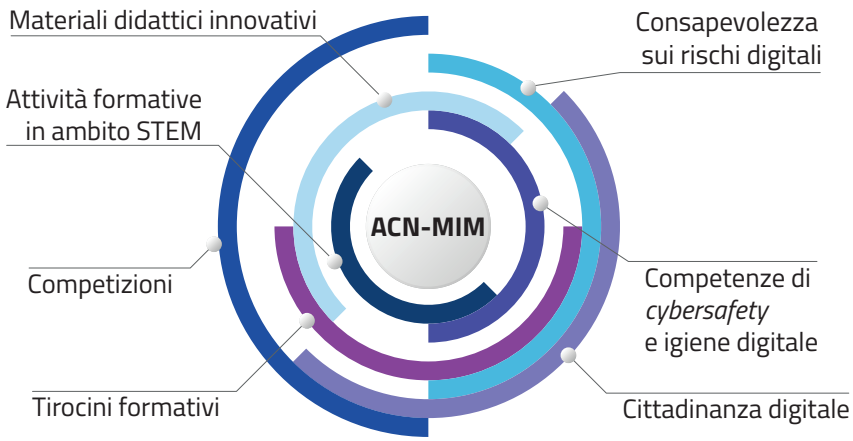


Figura 1 – I principali settori di collaborazione tra ACN e MIM

Tale accordo si pone l'obiettivo di realizzare un ampio ventaglio di iniziative rivolte a studenti, insegnanti e genitori, per: diffondere la consapevolezza sui rischi digitali, inclusi il cyberbullismo, l'accesso a contenuti inappropriati e le minacce alla *privacy*; promuovere le competenze di *cybersafety* e igiene digitale, insegnando comportamenti sicuri nell'uso delle tecnologie e dei dispositivi digitali; favorire la cittadinanza digitale, integrando la cybersicurezza nei percorsi di educazione civica; orientare gli studenti verso discipline STEM, con particolare attenzione alla sicurezza informatica attraverso la realizzazione di competizioni e attività formative. Il protocollo prevede, anche, la formazione continua per gli insegnanti, la creazione di materiali didattici innovativi per supportare l'insegnamento dell'informatica e della cybersicurezza, nonché la possibilità di realizzare tirocini formativi presso l'Agenzia.

È stato stipulato un protocollo con la Rete ITS Italy al fine di svolgere in modo efficace l'attività di promozione dei percorsi di *cybersecurity* negli Istituti tecnologici superiori (Fondazioni ITS *Academy*). La Strategia nazionale di cybersicurezza pone, infatti, una specifica attenzione agli ITS, che coprono un segmento terziario, parallelo a quello universitario, realizzato in stretta collaborazione con realtà aziendali e finalizzato a un rapido inserimento dei diplomati nel mondo del lavoro, contribuendo così alla riduzione della carenza di forza lavoro qualificata.

Quanto al mondo universitario, è stato siglato un protocollo d'intesa con l'Università commerciale "Luigi Bocconi", allo scopo di collaborare alla realizzazione di iniziative volte a promuovere la formazione universitaria e professionale nel campo della cybersicurezza, a cooperare alla realizzazione di attività di formazione specifica e a definire congiuntamente obiettivi di ricerca.

7.1.2 Le attività di formazione a livello internazionale

A livello internazionale è proseguita la partecipazione dell'Agenzia ai gruppi di lavoro di ENISA e dell'ECCC (vedasi Capitolo 6), che, con il coinvolgimento di numerosi Stati membri e della Commissione europea, lavorano al fine di definire quadri di riferimento comuni per la formazione specialisti-

ca in ambito cyber. I temi trattati riguardano, tra gli altri, la revisione e arricchimento dell'ECSF (*European Cybersecurity Skill Framework*), la valutazione della possibilità di concordare schemi e procedure per la definizione di attestazioni professionali che favoriscano la portabilità e il riconoscimento delle competenze tra gli Stati membri e la costituzione di una banca dati europea delle iniziative formative nel settore della cybersicurezza, che permetta di diffondere informazioni e di favorire collaborazioni.

L'Agenzia ha partecipato alla definizione del progetto AKADIMOS, che mira a sostenere la creazione e il funzionamento della costituenda *European Cybersecurity Skills Academy*, quale punto di riferimento unico per l'Unione in materia di formazione sulla cybersicurezza. Il progetto, approvato e finanziato, su base competitiva, dal programma DEP, si propone di colmare il divario di competenze dei professionisti in ambito cyber in tutta l'UE realizzando programmi di formazione e monitoraggio. Con un budget di 4 milioni di euro finanziati al 50% dalla Commissione europea, AKADIMOS è realizzato da un consorzio composto – oltre che dall'ACN – da enti pubblici, università e centri di ricerca di 5 Paesi (Grecia, Cipro, Spagna, Slovenia e Italia).

L'ATTIVITÀ DI FORMAZIONE RIVOLTA AI GIOVANI E AGLI STUDENTI

L'attività di formazione che l'Agenzia ha svolto nei confronti dei giovani si è articolata su più piani.

In primo luogo, esperti dell'Agenzia hanno proseguito l'attività di formazione sulla sicurezza informatica rivolta alle studentesse e agli studenti di scuole primarie e secondarie di primo e secondo grado fornendo un'educazione di base in termini di igiene informatica e sui rischi legati all'uso improprio o inconsapevole di Internet. Un approccio differente è stato adottato verso gli studenti degli istituti scolastici di secondo grado con incontri d'orientamento sui percorsi di studi.

Ulteriori interventi di formazione e orientamento sono stati svolti anche in occasione di eventi dedicati agli ITS e presso l'Accademia di cybersicurezza del Lazio.

L'Agenzia ha altresì preso parte ai progetti "Generazioni Connesse" e "Patentino Digitale": il primo progetto, svolto in collaborazione con il Ministero dell'istruzione e del merito sui rischi e i pericoli della rete, è stato rivolto agli studenti di ogni ordine e grado delle scuole di tutto il territorio nazionale; il secondo invece, svolto in collaborazione con il Corecom Lazio, è stato rivolto a studenti della fascia di età 11-13 anni di 500 classi delle scuole del Lazio.

Nell'ambito della formazione rivolta a giovani e studenti nel corso del 2024, è stato avviato il progetto volto a prevedere sussidi economici allo scopo di promuovere percorsi formativi in cybersicurezza a livello post-secondario e universitario. Tali contributi verranno erogati utilizzando le risorse della Strategia nazionale di cybersicurezza e saranno destinati a studenti delle ITS Academy e delle Università iscritti a percorsi di studio dedicati alla cybersicurezza.

Unitamente al CINI sono stati svolti 14 incontri di formazione e sensibilizzazione destinati ai giovani partecipanti alle competizioni di cybersicurezza, con la presenza di oltre 5.000 discenti.

7.2 LA CONSAPEVOLEZZA

L'importanza della consapevolezza del rischio cyber è diventata sempre più evidente nel mondo digitale in cui viviamo. Con l'aumento della dipendenza dalla tecnologia e dalla connettività, le minacce informatiche si sono moltiplicate, colpendo la Pubblica Amministrazione, aziende e singoli individui. La consapevolezza del rischio cyber è quindi fondamentale per proteggere dati personali, prevenire violazioni della sicurezza e garantire la continuità operativa.

Una delle principali ragioni per cui la consapevolezza del rischio cyber è cruciale è la crescente sofisticazione degli attacchi informatici. Al riguardo, è pertanto importante che i soggetti pubblici, gli operatori privati e la società civile nel suo complesso, percepiscano il proprio ruolo quale parte attiva e responsabile all'interno del sistema Paese, attuando comportamenti sicuri e virtuosi nello spazio cibernetico.

7.2.1 Le campagne di *awareness*

Ai fini della consapevolezza sono state organizzate diverse iniziative a favore di settori rilevanti per la cybersicurezza quali la Pubblica Amministrazione, la sanità e la giustizia.

Alla luce della più volte richiamata centralità della PA per un'adeguata protezione del Paese dalle minacce cibernetiche, l'Agenzia ha collaborato con il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri a un'importante iniziativa per aumentare la consapevolezza cyber dei dipendenti della PA. Sono stati, infatti, realizzati dei moduli formativi sulla piattaforma Syllabus, composti di video, *slideshow* e infografiche, fruibili in maniera autonoma e comprensivi di domande finali di consolidamento e contenuti integrativi scaricabili. Questo corso può essere seguito da tutti i dipendenti della Pubblica Amministrazione, raggiungendo quindi una platea potenziale di 3,3 milioni di utenti.

Il settore sanitario, come illustrato nel Capitolo 2, continua a essere tra quelli maggiormente esposti e colpiti dalla minaccia cyber con conseguenze molto gravi che possono creare malfunzionamenti o disservizi anche ad attività essenziali quali il pronto soccorso, le sale operatorie, le terapie intensive o i trattamenti salvavita. Per tale ragione, è stata avviata una campagna di sensibilizzazione destinata al personale apicale delle strutture sanitarie regionali, con l'obiettivo di diffondere la consapevolezza del rischio cyber e di illustrare, altresì, i contenuti del report "La minaccia cibernetica al settore sanitario. Analisi e raccomandazioni", redatto dall'Agenzia (vedasi box). La campagna ha preso avvio a Roma, con oltre 300 partecipanti, e proseguirà nel 2025 per raggiungere tutti i capoluoghi di Regione italiani.

L'ACN dedica ormai da tempo significativa attenzione al potenziamento del livello di maturità cyber delle piccole e medie imprese (vedasi box). Nel 2024, in particolare, è stata avviata una

campagna rivolta alle PMI italiane che ha previsto la realizzazione di guide e video *tutorial* destinati a dirigenti, dipendenti e professionisti IT, dal titolo "Accendiamo la cybersicurezza. Proteggiamo le nostre imprese" (al riguardo vedasi anche il Capitolo 9). Sempre nella stessa ottica, è stato lanciato un ciclo di incontri sul territorio per promuovere la cultura della cybersicurezza e favorire la consapevolezza delle PMI, che potranno confrontarsi con gli esperti di ACN e delle istituzioni regionali sulle sfide e le opportunità legate alla digitalizzazione. Tale *roadshow*, avviato con la collaborazione di Confindustria e Confartigianato, è partito da Napoli a dicembre per poi proseguire nelle principali città italiane nel 2025.

La minaccia cibernetica al settore sanitario

Il report dedicato al settore sanitario presenta una panoramica degli eventi e degli incidenti cyber rilevati e gestiti dall'Agenzia nel periodo gennaio 2022-dicembre 2024, oltre che una sintetica analisi delle principali vulnerabilità individuate nelle infrastrutture digitali.

Il report destinato sia ai livelli dirigenziali, sia al personale tecnico delle strutture sanitarie, fornisce raccomandazioni per agevolare la mitigazione delle pratiche errate riscontrate nel corso delle attività di supporto alla gestione degli incidenti svolte dal personale tecnico del CSIRT Italia.

Nell'ambito dell'attuazione della Strategia nazionale per la cybersicurezza è stata inaugurata una campagna destinata ai magistrati volta sia ad accrescere la consapevolezza sui rischi derivanti dall'uso delle tecnologie informatiche, sia a illustrare i nuovi meccanismi di collaborazione tra Procure distrettuali, Direzione nazionale antimafia e antiterrorismo e Agenzia, come previsto dalla legge n. 90/2024. L'iniziativa ha preso avvio dalla Procura di Milano e proseguirà nel 2025.

Infine, in occasione delle festività natalizie è stata realizzata una campagna di *cyber awareness*, diffusa tramite i canali istituzionali dell'Agenzia (sito web, YouTube e LinkedIn), con l'obiettivo di fornire consigli di cybersicurezza, anche in relazione agli acquisti online.

7.2.2 Le campagne di sensibilizzazione destinate a particolari categorie professionali

Al fine di intercettare in modo capillare le diverse fasce della società civile, è stato previsto un piano di eventi di *cyber awareness* destinati a specifiche categorie professionali. L'Agenzia, tramite la collaborazione con il Consiglio nazionale forense e con il Consiglio nazionale del notariato, ha avviato un percorso di diffusione della cultura cyber nei confronti delle categorie professionali afferenti al settore legale. L'obiettivo di tali iniziative, che proseguiranno in modo mirato nel 2025, è quello di incentivare i comportamenti responsabili nello spazio cibernetico, con particolare attenzione al contrasto del diffuso fenomeno della disattenzione digitale, anche al fine di proteggere i dati personali.

Cyber Index PMI nazionale

A sostegno delle piccole e medie imprese l'ACN ha realizzato, congiuntamente con Confindustria e Generali, un indice nazionale cyber focalizzato espressamente sulle PMI. A tal fine, sono stati intervistati rappresentanti di oltre 700 PMI con l'obiettivo di aggiornare il quadro informativo sulla loro gestione del rischio cyber, nonché sulla consapevolezza e sulle opportunità di investimento in tale ambito.

8.

STRATEGIA NAZIONALE DI CYBERSICUREZZA 2022-2026: STATO DELL'ATTUAZIONE

La Strategia nazionale di cybersicurezza 2022-2026 costituisce un volano per tutto l'ecosistema nazionale di cybersicurezza ai fini dell'innalzamento dei livelli di sicurezza e resilienza cibernetiche del Paese. A partire dall'adozione del quadro strategico vigente, avvenuta nel maggio del 2022, l'ACN ha mantenuto un ruolo centrale nell'attuazione della Strategia, rispetto al cui Piano di implementazione esercita funzioni di indirizzo, coordinamento e monitoraggio.

Nel 2024, l'Agenzia ha ulteriormente rafforzato il dialogo tra le Amministrazioni, facilitandone la selezione delle priorità e la definizione delle progettualità di carattere strategico sia rispetto alla postura di sicurezza di ciascun ente, sia – in un'ottica integrata – rispetto all'ecosistema nazionale di cybersicurezza. Come si dirà oltre, l'ACN ha monitorato l'efficace utilizzo delle risorse stanziate e fornito supporto tecnico alle Amministrazioni coinvolte tanto nella fase di pianificazione quanto in quella di realizzazione degli interventi attuativi delle misure.

In un contesto di crescente complessità tecnologica e di continua evoluzione del panorama della minaccia cibernetica, l'azione dell'Agenzia è stata ispirata a un criterio di maggiore inclusività e capillarità. Per tale ragione, oltre alle Amministrazioni già individuate come "soggetti responsabili" per l'attuazione delle 82 misure del citato Piano di implementazione, il 2024 ha visto l'ampliamento della partecipazione all'attuazione della Strategia, in primis attraverso il coinvolgimento delle Regioni. Ciò per favorire, in altri termini, un approccio coordinato e multilivello nella gestione della sicurezza informatica del Paese tramite la messa a sistema di competenze e risorse, con il fine ultimo di favorire una digitalizzazione sicura.

8.1 RILEVAZIONE DEI FABBISOGNI E RISORSE ASSEGNATE

In continuità con le attività svolte nell'anno precedente, nel corso del 2024 l'ACN ha avviato una nuova rilevazione dei fabbisogni finanziari delle Amministrazioni responsabili dell'attuazione delle misure previste dal Piano di implementazione della Strategia. Tale rilevazione è avvenuta tenendo conto del cronoprogramma definito dal Manuale operativo pubblicato a fine 2022, in base al quale sono individuati gli anni di prevalente attuazione delle misure, insieme a indicatori e metriche per la misurazione del grado di avanzamento degli interventi.

Le istanze presentate dalle Amministrazioni sono state analizzate e valutate tenendo conto della coerenza degli interventi con le misure di riferimento e del contributo degli stessi al rafforzamento della sicurezza cibernetica delle singole Amministrazioni e del sistema Paese. Si è inteso, pertanto, considerare anche il potenziale impatto di tali interventi sul complessivo livello di resilienza della superficie digitale del Paese.

Fondi Strategia

Per soddisfare i fabbisogni finanziari dei soggetti responsabili delle misure, nel bilancio previsionale del Ministero dell'economia e delle finanze sono stati istituiti, a norma dell'art. 1, co. 899, della legge n. 197/2022 (legge di bilancio 2023), due fondi specifici, il Fondo per l'attuazione della Strategia nazionale di cybersicurezza e il Fondo per la gestione della cybersicurezza (c.d. "Fondi Strategia"), le cui dotazioni pluriennali assicurano uno strumento finanziario concreto ai fini dell'attuazione della Strategia nazionale.

Nello specifico, la nuova rilevazione ha visto il coinvolgimento di 39 Amministrazioni (di cui 22 Pubbliche Amministrazioni centrali e 17 Regioni) che hanno presentato interventi relativi a un

totale di 34 misure. Nel complesso, sono stati ritenuti idonei al finanziamento 107 interventi, di cui 91 a valere sul Fondo per l'attuazione della Strategia nazionale di cybersicurezza e sul Fondo per la gestione della cybersicurezza, istituiti dalla legge di bilancio 2023, ai quali si sommano gli interventi finanziati con fondi ordinari delle singole Amministrazioni e/o con fondi PNRR.

Su proposta dell'ACN e d'intesa con il Ministero dell'economia e delle finanze, è stato quindi adottato il DPCM 8 luglio 2024 che disciplina la ripartizione del Fondo per l'attuazione della Strategia nazionale di cybersicurezza e del Fondo per la gestione della cybersicurezza per il triennio 2024-2026.

Il provvedimento ha assegnato un totale di 347,6 milioni di euro, di cui 212,9 milioni di euro per l'attuazione della Strategia nazionale di cybersicurezza e 134,7 milioni di euro per la gestione della cybersicurezza (Figura 1).

Ripartizione dei Fondi

La prima ripartizione, per il triennio 2023-2025, delle risorse a valere sui fondi istituiti per l'attuazione della Strategia nazionale è stata disposta dal DPCM 9 agosto 2023, tramite cui sono stati assegnati complessivamente 66,7 milioni di euro, al fine di sostenere economicamente 39 interventi condotti da 10 Amministrazioni. Un'ulteriore ripartizione è stata operata nel 2024 con il DPCM 8 luglio 2024.

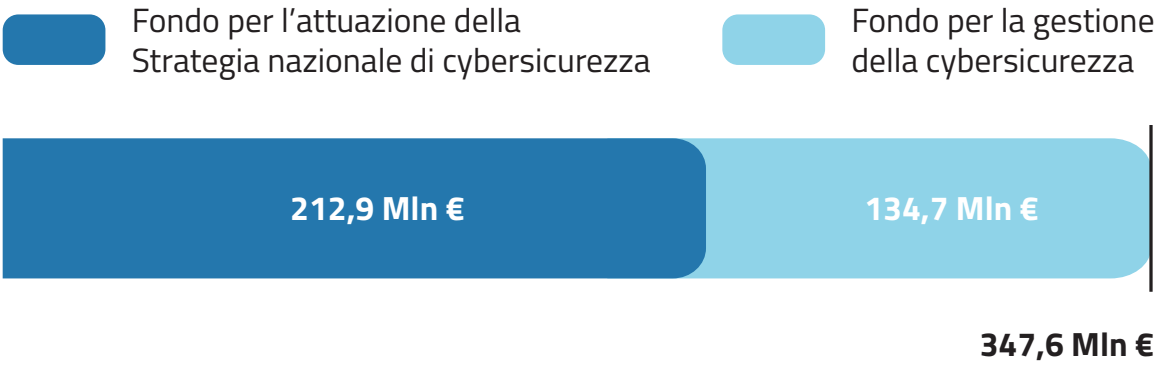


Figura 1 – Ripartizione dei Fondi Strategia 2024-2026

8.2 BENEFICIARI DELLE RISORSE

Come mostrato in Figura 2, il 79% delle risorse assegnate dal DPCM 8 luglio 2024 è stato destinato a Pubbliche Amministrazioni centrali, nelle cui prerogative rientrano funzioni specifiche in materia di cybersicurezza rispetto a settori chiave del Paese (sicurezza nazionale, politica economica, giustizia, difesa, contrasto al crimine online, protezione delle infrastrutture critiche). Se per quest'ultime appare chiara la portata sistemica degli interventi, specie in considerazione dei mandati istituzionali e del raggio d'azione, nondimeno il coinvolgimento delle Pubbliche Amministrazioni locali, in particolare le Regioni – che come evidenziato nell'immagine hanno beneficiato del 21% dei fondi assegnati – garantisce una maggiore capillarità degli interventi di attuazione della Strategia na-

zionale di cybersicurezza e un sostegno – anche a livello territoriale – per la messa in sicurezza di infrastrutture e servizi digitali utili alla cittadinanza e all'azione amministrativa.

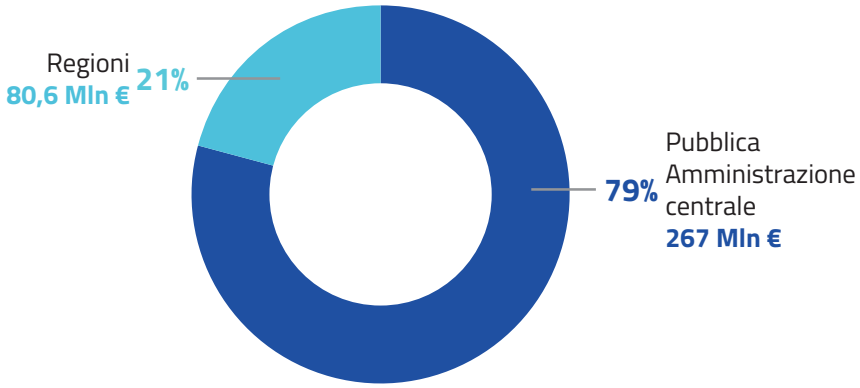


Figura 2 – Distribuzione delle risorse finanziarie tra Amministrazioni centrali e locali

La Figura 3 mostra, invece, le tipologie di Amministrazioni beneficiarie delle risorse a valere sul Fondo di attuazione della Strategia nazionale di cybersicurezza e sul Fondo per la gestione della cybersicurezza.

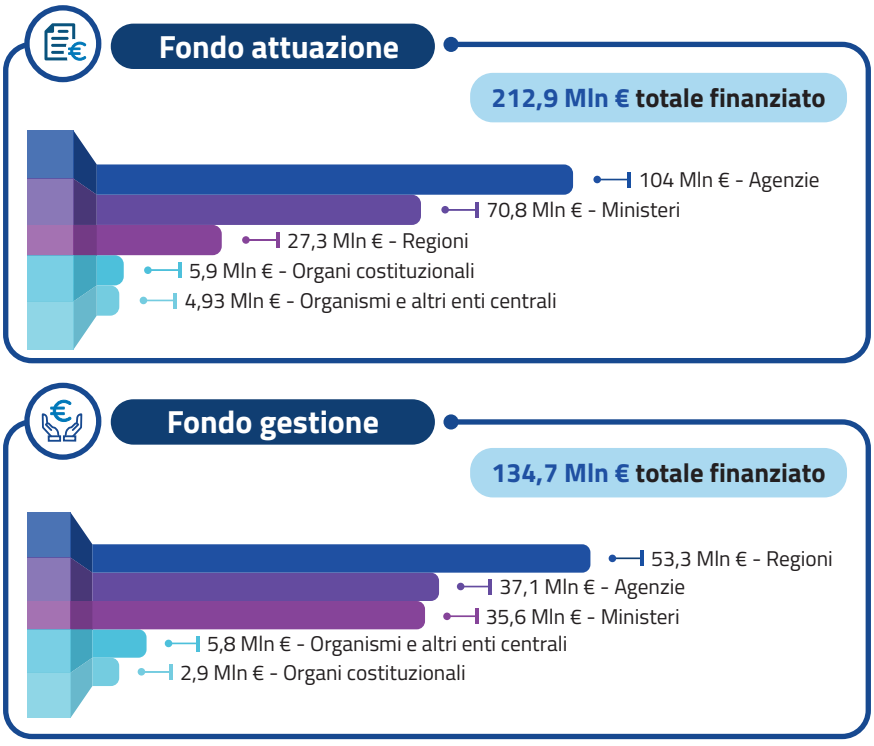


Figura 3 – Distribuzione delle risorse finanziarie per tipologia di Amministrazione beneficiaria

A quanto sopra rappresentato si aggiunge l'assegnazione al Sistema di informazione per la sicurezza della Repubblica di una quota a valere sui Fondi Strategia, che nel 2024 è stata erogata per interventi in attuazione delle misure #40 e #45 in materia di deterrenza. La dotazione del Fondo di attuazione è stata, inoltre, ridotta per il 2024 di 20 milioni di euro ai sensi dell'art. 35-*bis*, co. 2, del D.L. n. 60/2024.

Da un esame sulla distribuzione complessiva delle risorse (Figura 4), è possibile notare che la dotazione del Fondo per la gestione della cybersicurezza prevista per il 2024 è stata assegnata nella sua interezza agli interventi di attuazione delle misure della Strategia, mentre risultano ancora disponibili circa 13,2 milioni di euro a valere sul Fondo per l'attuazione della Strategia. Tali risorse contribuiranno a incrementare le disponibilità per il 2025 e potranno, pertanto, essere impiegate per il finanziamento di nuovi interventi di attuazione. Analogo meccanismo era valso per le risorse del Fondo di attuazione non assegnate tramite il DPCM 9 agosto 2023, che sono rientrate nelle disponibilità totali per il 2024, concorrendo al finanziamento degli interventi oggetto del DPCM 8 luglio 2024.

Tramite i provvedimenti fino a oggi adottati, è stato assegnato circa il 73% delle risorse disponibili sul Fondo di attuazione, mentre il Fondo per la gestione della cybersicurezza è stato oggetto di una variazione operata dalla legge di bilancio 2025, in base alla quale la dotazione del fondo sarà incrementata di 200.000 euro per il 2025 e di 1 milione di euro per ciascuno degli anni 2026 e 2027, anche per far fronte alle nuove esigenze derivanti dall'evoluzione dello scenario della minaccia cibernetica e dall'affermarsi di nuove tecnologie, come l'intelligenza artificiale.

La figura sottostante mostra lo stato dei due Fondi Strategia, specificando quante risorse siano già state assegnate e quante rimangano ancora da assegnare

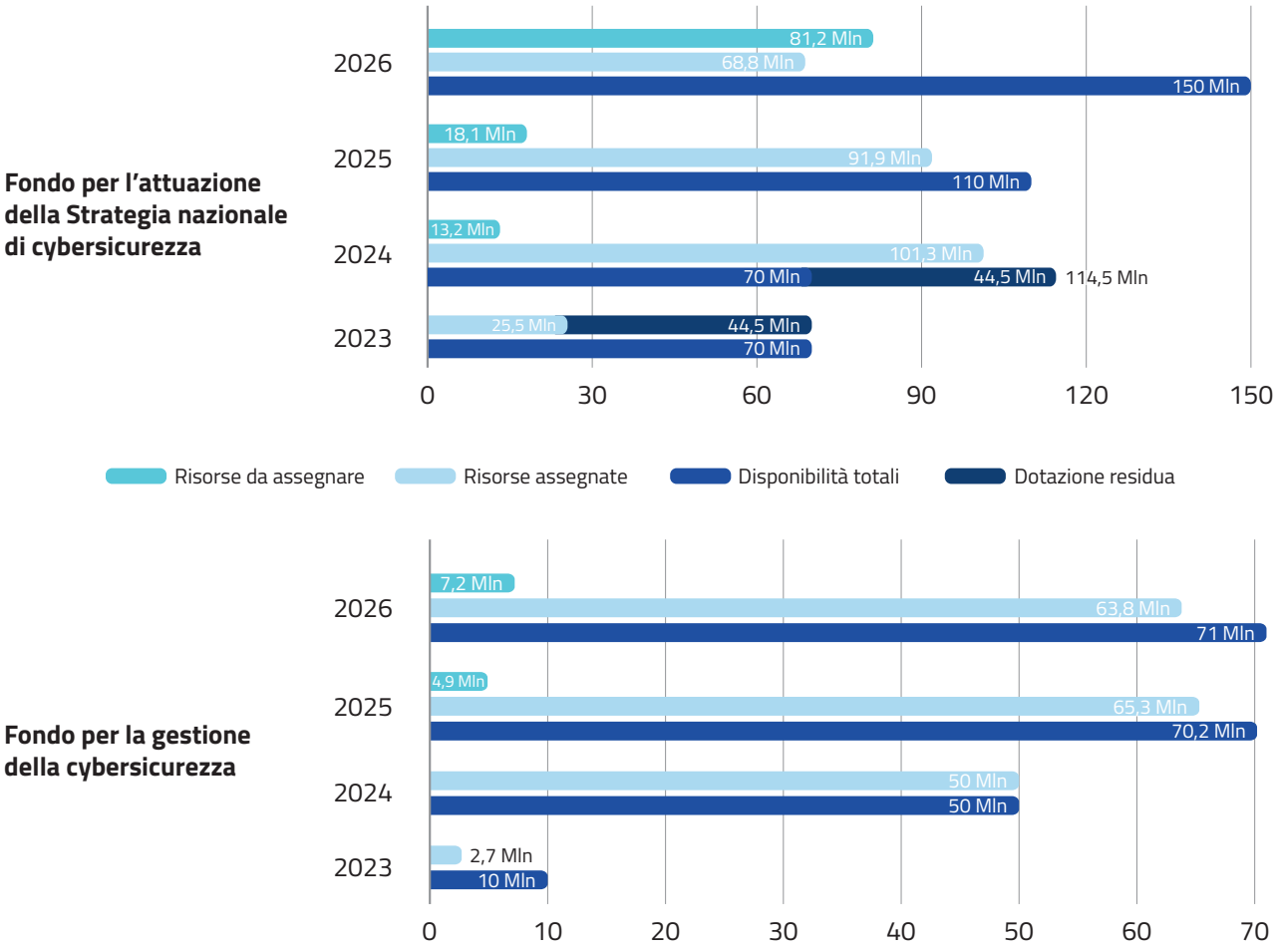


Figura 4 – Stato dei Fondi Strategia

8.3 RISULTATI RAGGIUNTI

In ossequio al ruolo di coordinamento, indirizzo e monitoraggio sull'attuazione della Strategia nazionale di cybersicurezza, l'Agenzia, durante l'anno appena trascorso, ha effettuato 3 sessioni di monitoraggio, con cadenza quadrimestrale, sugli interventi attuativi delle misure del Piano di implementazione.

Tale monitoraggio periodico – volto a tracciare l'avanzamento progettuale, il raggiungimento di risultati e l'utilizzo delle risorse finanziarie assegnate – e la rispondente rendicontazione da parte delle Amministrazioni avvengono secondo le modalità descritte nelle Linee guida definite dall'ACN. Le Linee guida, in particolare, sono finalizzate a garantire il corretto espletamento delle attività di coordinamento e monitoraggio degli interventi di attuazione delle misure.

A dicembre 2024, delle 82 misure previste dal Piano di implementazione ne risultavano avviate 69: di queste 63 in corso di realizzazione e 6 pienamente conseguite (Figura 5).

Nell'originaria pianificazione era previsto l'avvio, nel 2025, di un numero ben maggiore di misure (33), ma la proficua sinergia con le Amministrazioni e l'efficace attività di impulso hanno permesso di anticipare l'avvio di varie misure e dei relativi interventi. Le restanti 13 misure potranno essere avviate entro il 2026.

Misura da avviare: *sono in corso le attività di progettazione/approvazione degli interventi volti al raggiungimento della stessa.*

Misura in corso: *sono già stati avviati interventi e, dal monitoraggio, risulta che gli obiettivi previsti sono in fase di esecuzione.*

Misura conseguita: *tutti gli obiettivi risultano raggiunti, anche se da essi deriva una attività continuativa che viene portata avanti dal soggetto responsabile della misura.*

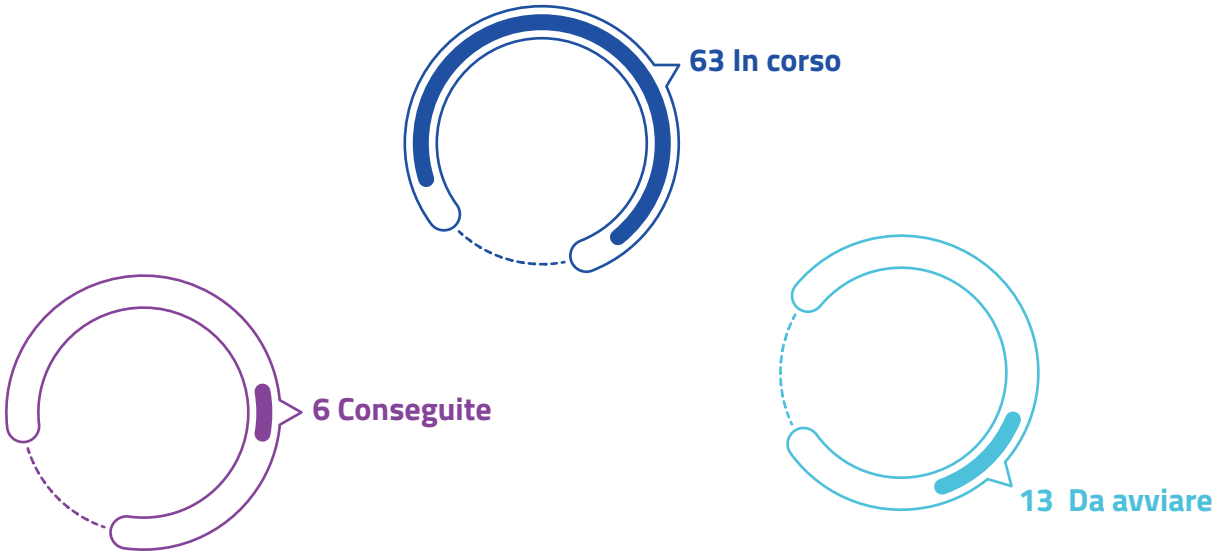


Figura 5 – Stato di implementazione delle misure della Strategia

Gli interventi proposti hanno permesso di rispondere a quasi tutte le aree tematiche individuate dal Piano di implementazione della Strategia, garantendo una maggiore completezza e coerenza nella realizzazione degli obiettivi strategici (Figura 6).

Obiettivi	Aree tematiche	Misure previste	Misure avviate	Misure conseguite
Protezione	Scrutinio tecnologico	4	4	-
	Definizione e mantenimento di un quadro giuridico nazionale aggiornato e coerente	7	5	2
	Conoscenza approfondita del quadro della minaccia cibernetica	2	2	-
	Potenziamento capacità cyber della Pubblica Amministrazione	3	3	-
	Sviluppo di capacità di protezione per le infrastrutture nazionali	5	5	-
	Promozione dell'uso della crittografia	2	1	-
	Definizione e implementazione di un piano di contrasto alla disinformazione online	1	1	-
Risposta	Sistema di gestione crisi nazionale e transnazionale	5	4	1
	Servizi cyber nazionali	8	7	1
	Esercitazioni di cybersicurezza	2	2	-
	Definizione del posizionamento e della procedura nazionale in materia di attribuzione	1	1	-
	Contrasto al *cybercrime*	4	4	-
	Capacità di deterrenza in ambito cibernetico	1	1	-
Sviluppo	Centro nazionale di coordinamento	2	2	-
	Sviluppo di tecnologia nazionale ed europea	1	-	-
	Realizzazione di un "parco nazionale della cybersicurezza"	1	-	-
	Sviluppo industriale, tecnologico e della ricerca	3	2	-
	Impulso all'innovazione tecnologica e alla digitalizzazione	6	5	-
Fattori Abilitanti	Formazione	12	8	-
	Promozione della cultura della sicurezza cibernetica	3	3	-
	Cooperazione	8	8	1
	Metriche e *Key Performance Indicators*	1	1	1
Totale complessivo		82	69	6

Figura 6 – Misure per obiettivi e aree tematiche

In relazione al primo dei 3 macro-obiettivi previsti dalla Strategia, protezione degli *asset* strategici nazionali, nel 2024, oltre alle Misure #6 e #7 (precedentemente avviate) per la definizione e il mantenimento di un quadro giuridico aggiornato e coerente, sono stati avviati ulteriori interventi nei seguenti ambiti:

- scrutinio tecnologico per l'attivazione e la formazione di unità ispettive presso i Ministeri dell'interno e della difesa (Misura #4);
- sviluppo di capacità di protezione per le infrastrutture nazionali per la promozione di un programma di collaborazione tra ACN e gli operatori IXP nazionali (Misura #17), l'implementazione di una infrastruttura di risoluzione DNS nazionale al servizio degli operatori pubblici e privati (Misura #18), il mantenimento di una piattaforma per il monitoraggio e la scansione di vulnerabilità dei servizi digitali esposti su Internet di interesse della Pubblica Amministrazione (Misura #19, precedentemente avviata), l'implementazione di un servizio di segnalazione di *phishing* per i dipendenti della Pubblica Amministrazione (Misura #20, precedentemente avviata) e, infine, il mantenimento di una soluzione per la gestione delle copie dei *backup* "a freddo" (Misura #21).

Ai fini del raggiungimento del macro-obiettivo di risposta alle minacce, agli incidenti e alle crisi cyber nazionali, nel 2024 sono stati avviati ulteriori interventi per:

- il sistema di gestione di crisi nazionale e transnazionale, per sviluppare un sistema di coordinamento continuativo con tutte le Amministrazioni che compongono l'NCS, (Misura #25, precedentemente avviata), assicurare una modalità di notifica unitaria degli incidenti di sicurezza cibernetica verso il CSIRT Italia ai fini di una più efficace capacità di risposta e allertamento, anche tramite l'emanazione di specifiche linee guida (Misura #27), nonché attività volte alla predisposizione di procedure operative per rispondere ai vari scenari della minaccia cyber per le determinazioni politiche (Misura #29);
- la realizzazione dei servizi cyber nazionali, riferiti a:
  - potenziamento dell'HyperSOC (Misura #30, precedentemente avviata) tramite ulteriori servizi di monitoraggio avanzato, quali ad esempio il rilevamento di minacce di sicurezza attraverso l'analisi e la correlazione di dati raccolti da fonti esterne,
  - realizzazione di un'infrastruttura HPC dedicata all'ACN (Misura #32) per sfruttare, attraverso una maggiore potenza di calcolo, le diverse attività in ambito cybersicurezza di interesse nazionale,
  - potenziamento dei servizi attualmente erogati dal CSIRT Italia e delle capacità della più ampia rete di CSIRT con esso integrati (Misura #33),
  - costituzione di una rete di ISAC settoriali, da integrare con l'ISAC istituito presso l'ACN (Misura #34, precedentemente avviata e Misura #35);
- il contrasto al *cybercrime*, in particolare per il rafforzamento dello scambio informativo con gli analoghi organismi europei, internazionali e degli Stati *like-minded* (Misura #43) e per la rilevazione statistica dei dati relativi ai reati informatici acquisiti dalle Forze di polizia e dall'Autorità giudiziaria (Misura #44).

Sviluppo

In relazione, poi, al macro-obiettivo dedicato allo sviluppo consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, sono stati avviati ulteriori interventi in molteplici ambiti:

- l'ACN, in qualità di NCC, ha avviato una serie di attività per sensibilizzare i portatori di interesse nazionali sui programmi di finanziamento UE (Misura #46);
- nel campo dello sviluppo industriale, tecnologico e della ricerca, sono stati, inoltre, avviati: il Tavolo di coordinamento per l'internazionalizzazione delle imprese cyber con l'obiettivo di rafforzare la presenza delle imprese nazionali sui mercati esteri (Misura #50, già avviata) e uno studio di fattibilità per una piattaforma sicura di messaggistica istantanea per la Pubblica Amministrazione (Misura #51);
- ai fini dell'impulso all'innovazione tecnologica e alla digitalizzazione, si è proceduto alla creazione dell'ecosistema a supporto dell'*AI Factory* (Misura #53), per sostenere lo sviluppo del *Cyber Innovation Network* (Misura #54) e a promuovere le attività di collaborazione con gli operatori IXP nazionali (Misura #57);
- in materia di promozione della digitalizzazione e dell'innovazione della PA in sicurezza (Misura #55), sono proseguite le attività avviate nel 2023 e sono stati presentati ulteriori progetti, anche con il coinvolgimento di Regioni e ulteriori Pubbliche Amministrazioni. Tali interventi hanno consentito il potenziamento delle capacità di risposta e *recovery* dagli attacchi informatici (vedasi box).

MISURA #55

L'attuazione della Misura #55, dedicata al rafforzamento della resilienza della Pubblica Amministrazione, continua a rappresentare un progetto particolarmente complesso, data la numerosità e varietà dei soggetti, che includono sia Amministrazioni centrali che Regioni. Nel corso del 2024, oltre ad ampliare tale platea, è proseguito il sostegno agli interventi di potenziamento delle capacità di risposta e *recovery* dagli attacchi informatici. Diverse le tipologie degli interventi, che hanno riguardato il miglioramento della sicurezza e resilienza cyber a 360 gradi: sicurezza dei dati, dei dispositivi e dei portali *cloud*; gestione degli accessi e delle autorizzazioni; aggiornamento della sicurezza di sistemi e applicazioni (*patch management*); test sulla robustezza delle difese cyber (*red team*); potenziamento di infrastrutture di *disaster recovery*, nonché di CERT/SOC; definizione e aggiornamento di *policy* e *governance* di cybersicurezza, revisione e miglioramento della *compliance* normativa e percorsi di formazione.

Fattori abilitanti

Infine, per quanto riguarda i fattori abilitanti individuati dalla Strategia 2022-2026, sono stati avviati ulteriori interventi in tema di:

- cooperazione internazionale in materia di cybersicurezza, volti al rafforzamento del ruolo dell'Italia all'interno dei consessi multilaterali e alla promozione della cooperazione dei Paesi G7 sui temi delle nuove tecnologie (Misura #75 e #76) e al sostegno ai Paesi di inte-

resse strategico (Misura #77), anche tramite la creazione di un ecosistema nazionale per attività di *cyber capacity building* verso Paesi terzi (Misura #78 e #79, già avviate nel 2023);

- formazione, per l'erogazione di borse di studio per studenti e studentesse nel campo della cybersicurezza a diversi livelli (Misura #59), il supporto alla creazione di *startup* a conduzione femminile (Misura #64), l'organizzazione di iniziative e competizioni nazionali in materia di cybersicurezza (Misura #65), le attività a favore degli studenti delle scuole secondarie superiori (Misura #66), l'attivazione di percorsi formativi specifici nell'ambito di accordi e programmi di scambio con altri Paesi e di incentivazione della mobilità internazionale (Misura #67), e, infine, interventi per la formazione e l'aggiornamento professionale in ambito cybersicurezza dei lavoratori (Misura #70);
- promozione della cultura della sicurezza cibernetica, tramite una campagna di sensibilizzazione per la promozione di competenze degli utenti e di comportamenti responsabili nello spazio cibernetico (Misura #71, precedentemente avviata), l'attivazione di corsi universitari volti a diffondere la consapevolezza in materia cyber (Misura #72), l'implementazione di una strategia per mitigare la disinformazione online e gli impatti di eventuali attività cyber offensive (Misura #73, precedentemente avviata).

Nel corso del 2025 continueranno le attività di rilevazione e monitoraggio degli interventi, con l'obiettivo di potenziare gli strumenti a supporto dei soggetti responsabili, attraverso il dialogo costante con le Amministrazioni, volto anche a misurare i benefici derivanti dall'impiego dei fondi destinati all'attuazione della Strategia nazionale di cybersicurezza. Nel 2025 sarà valutata, inoltre, la possibilità di ampliare ulteriormente il novero dei soggetti beneficiari dei finanziamenti, includendovi le Amministrazioni che svolgono un ruolo cruciale nella fornitura dei servizi pubblici essenziali, in linea con i recenti interventi normativi.

Tale aggiornamento è il primo passo verso la rivisitazione del quadro strategico vigente che si concretizzerà nell'adozione di una nuova Strategia nazionale di cybersicurezza a partire da gennaio 2027. In tale ottica, l'Agenzia mira a coinvolgere quanto più possibile i diversi portatori di interesse attraverso un processo di consultazione pubblica, così da individuare obiettivi e misure rispondenti alle mutate esigenze dell'ecosistema cyber nazionale.

9.

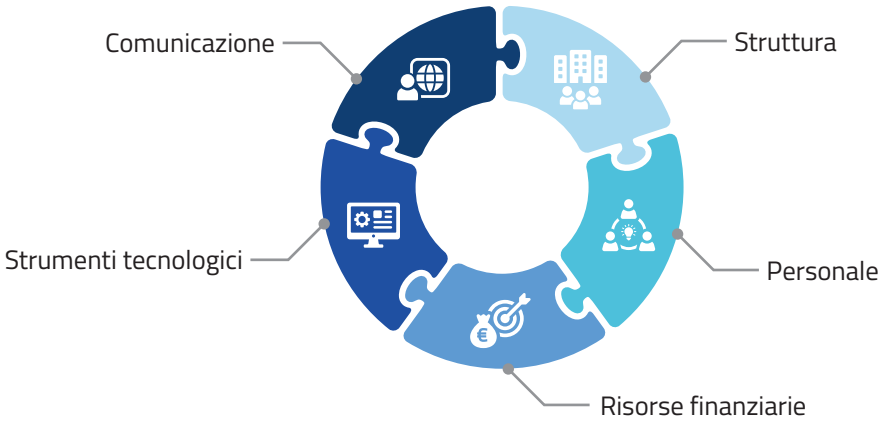
L'AGENZIA NEL 2024: IL RAFFORZAMENTO DELLA STRUTTURA

Il percorso di progressiva strutturazione dell'Agenzia per affrontare le numerose sfide illustrate in questa Relazione si è articolato nel 2024 attraverso delle linee di sviluppo che hanno interessato, in particolare, la struttura, il personale, le risorse finanziarie, gli strumenti tecnologici e la comunicazione concorrendo sinergicamente alla realizzazione della sua *mission*.

Anche a seguito del crescente ruolo affidato all'ACN, prosegue il reclutamento delle eccellenze del Paese attraverso i vari canali a disposizione, confermandola tra le Amministrazioni più giovani e specializzate a livello nazionale. L'Agenzia sta adattando la propria struttura e i propri processi in un'ottica di semplificazione, seguendo criteri di efficacia ed efficienza. Ciò si è concretizzato anche con l'acquisizione di una nuova sede, che si confà maggiormente alle proprie esigenze istituzionali.

Rilevante è, altresì, l'impegno per una corretta gestione della dotazione finanziaria, anche tramite un'attenta attività di *procurement* in aderenza alla disciplina del nuovo Codice dei contratti pubblici e alla normativa specifica prevista per le funzioni di tutela della sicurezza nazionale in ambito cibernetico assicurate dall'ACN. Gli strumenti tecnologici messi a disposizione dall'Agenzia si stanno evolvendo per meglio adattare i servizi offerti a beneficio della cybersicurezza nazionale.

Non da ultimo, si sta ampliando e approfondendo la capacità dell'ACN di comunicare l'importante lavoro portato avanti a molteplici livelli, sia attraverso un crescente utilizzo dei canali di comunicazione istituzionali, sia mediante mirate campagne di informazione e divulgazione di interesse generale.



9.1 SVILUPPO DELL'ORGANIZZAZIONE E DELLE PERSONE

Per rispondere in modo efficace e tempestivo alle molteplici sfide della cybersicurezza, sono state riconosciute all'Agenzia una peculiare collocazione istituzionale e un marcato livello di autonomia che le permettono di adottare paradigmi strategici e organizzativi utili all'assolvimento delle proprie funzioni.

Al fine di adeguare la struttura dell'ACN ai compiti istituzionali che nel tempo le sono stati assegnati e di rendere sempre più incisiva la sua azione, è stato definito il nuovo assetto organizzativo dell'Agenzia con interventi di soppressione, accorpamento e riorganizzazione dei Servizi e delle Divisioni, nonché delle Articolazioni a diretto supporto dei vertici. In Figura 1 l'organigramma in vigore dal 1 luglio 2024.

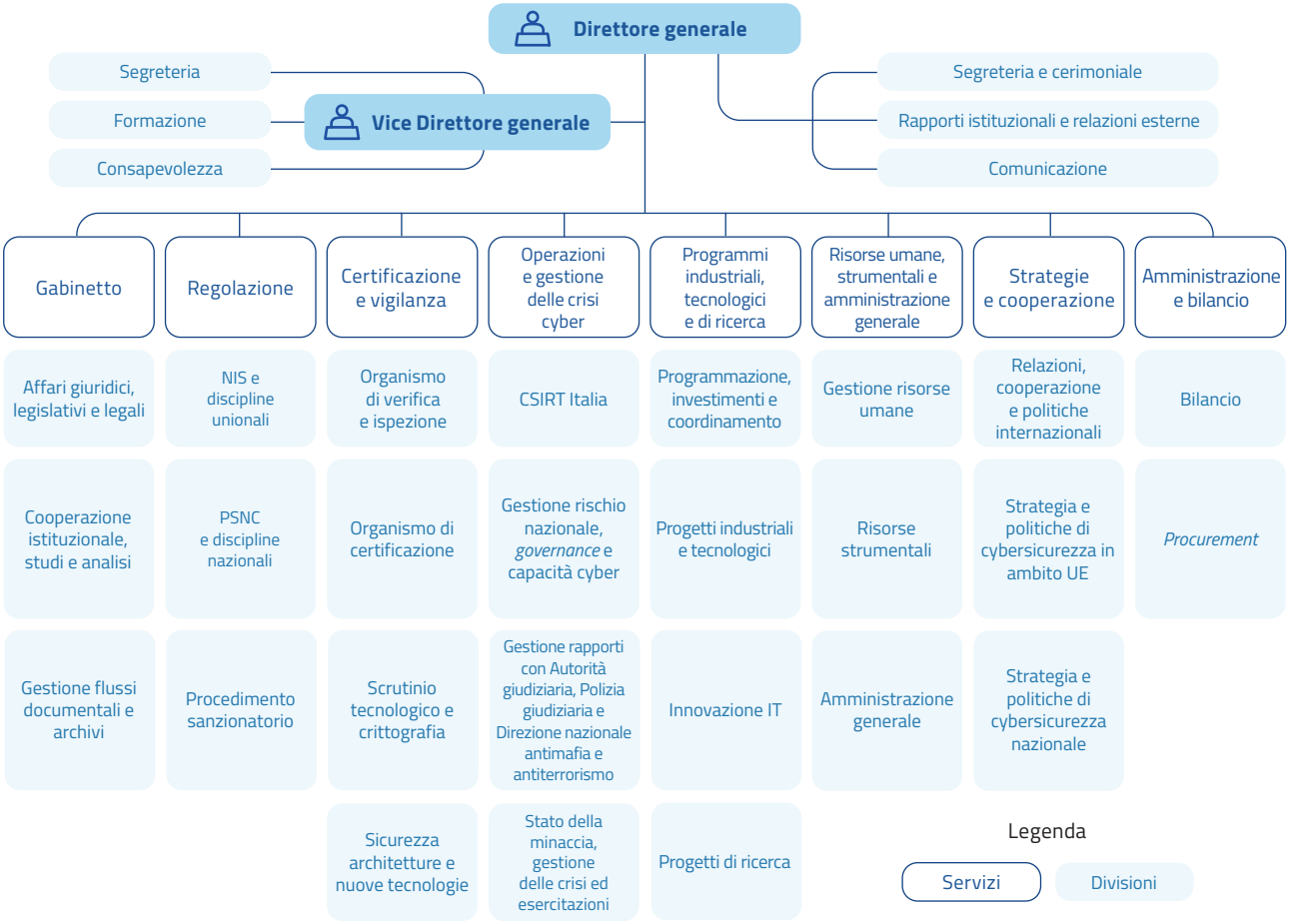


Figura 1 – Organigramma dell'ACN

L'Agenzia, per rispondere a tali necessità e per una definizione più organica dei propri obiettivi, ha adottato il Piano strategico 2024-2026. Si tratta di uno strumento che, anche in linea con la Strategia nazionale di cybersicurezza e le misure del relativo Piano di implementazione, cristallizza in un documento unico di programmazione, *governance* e coordinamento, i 5 obiettivi strategici dell'Agenzia. Tali obiettivi (vedasi box) mirano, in particolare, a creare valore pubblico per accompagnare il processo di ammodernamento delle infrastrutture, potenziando la resilienza cibernetica del Paese, riducendone il grado di vulnerabilità e, al contempo, incrementandone l'autonomia e l'indipendenza tecnologica. Da questi discendono 38 piani d'azione con l'indicazione dei responsabili, dei tempi, delle risorse, nonché dei criteri e degli indicatori per la valutazione periodica dei risultati raggiunti, delle risorse impiegate e dei progressi compiuti.

I 5 obiettivi del Piano strategico 2024-2026

1. *Protezione degli asset strategici nazionali*
2. *Risposta alle minacce, agli incidenti e alle crisi cyber nazionali e transnazionali*
3. *Sviluppo sicuro delle tecnologie digitali*
4. *Rafforzamento della cooperazione in materia di cybersicurezza*
5. *Essere un centro di ecellenza con un'organizzazione a geometrie variabili*

Sono state, altresì, intraprese specifiche attività in tema di monitoraggio e valutazione della *performance* grazie all'individuazione, tramite procedura selettiva, di un esperto in tale ambito con

funzioni di Organismo indipendente di valutazione. Tale professionista ha avviato l'azione di supporto e controllo all'interno di tutte le fasi del processo di gestione della *performance* organizzativa e individuale e fornirà supporto nell'attuazione e nel monitoraggio dei predetti obiettivi e piani, per ottimizzare i risultati dell'Agenzia in un'ottica di efficienza ed efficacia dei risultati complessivamente raggiunti da tutti gli elementi dell'organizzazione.

L'impegno per il miglior funzionamento dell'ACN, nel 2024, ha interessato in particolare il reclutamento del personale e lo sviluppo delle competenze e delle professionalità già in servizio. A tal fine è stata rideterminata la dotazione organica dell'Agenzia (con DPCM 4 luglio 2024), prevedendo un incremento progressivo fino a raggiungere un massimo di 550 unità di personale dal 2026.

Al 31 dicembre 2024, presso l'ACN erano impiegate 309 unità, un risultato che cristallizza la conclusione della fase di prima operatività raggiunto grazie a un articolato processo che ha condotto al progressivo rafforzamento dell'Agenzia. Numerosi sono gli istituti attraverso i quali sono state reclutate le risorse, secondo quanto previsto dalla normativa, come schematizzato in Figura 2. Il personale assunto a tempo indeterminato tramite concorso ha affiancato il primo nucleo di personale proveniente da altre Amministrazioni, necessario per l'iniziale operatività dell'Agenzia, e quello - sempre proveniente da altre Amministrazioni - successivamente stabilizzato, funzionale al suo rafforzamento. A ciò si aggiunge il personale assunto a tempo determinato (c.d. *vacancy*), quello in comando (o altro analogo istituto) e quello proveniente dal Ministero della difesa. A questi si sommano i vertici dell'Agenzia.

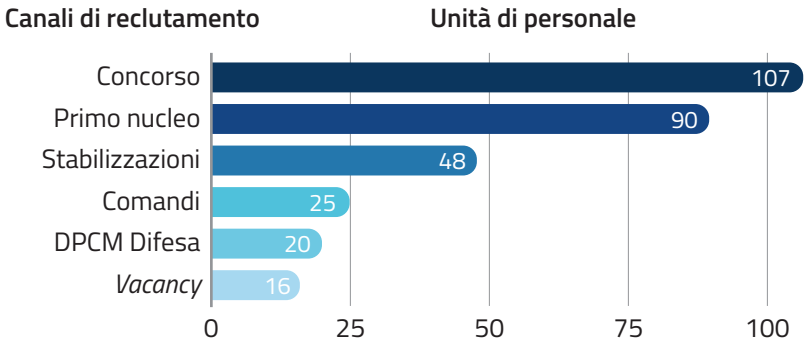


Figura 2 – Personale ACN al 31/12/2024

In particolare, nel corso del 2024, sono state portate a termine le procedure concorsuali per l'assunzione a tempo indeterminato di 60 coordinatori in possesso di un diploma di scuola media superiore con competenze ICT, nonché di 11 coordinatori iscritti all'elenco delle categorie protette della Città metropolitana di Roma Capitale in possesso di laurea nelle discipline giuridico-amministrative.

A seguito di apposite procedure selettive a evidenza pubblica per l'assunzione a tempo determinato, con contratto di diritto privato (*vacancy*), 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 2024 hanno preso servizio 2 *advisor*, rispettivamente, per supportare le attività di coordinamento e sviluppo delle relazioni internazionali, e per svolgere le funzioni di DFIR *team manager*. In favore del personale di livello non dirigenziale reclutato mediante la predetta modalità, a fine 2024 è stata indetta la procedura selettiva finalizzata alla stabilizzazione nel ruolo, dando attuazione a quanto previsto da una specifica disposizione normativa volta a rafforzare le capacità dell'Agenzia e a valorizzare le professionalità acquisite.

Grazie a specifiche intese con altri enti e istituzioni pubbliche, sono stati disposti, nel 2024, ulteriori distacchi, comandi, fuori ruolo o altre analoghe posizioni, per 19 unità, portando così il totale a 25. Infine, a seguito dell'adozione del DPCM 24 luglio 2024 che definisce le modalità per l'impiego di personale del Ministero della difesa presso l'Agenzia, hanno preso servizio 20 appartenenti all'Arma dei Carabinieri ai fini della tutela della sicurezza fisica della sede dell'ACN.

L'Agenzia, anche a seguito dei nuovi ingressi, continua a poter contare su un capitale umano particolarmente giovane e formato. In Figura 3 sono rappresentate l'età media dei dipendenti, nonché la distribuzione per titoli di studio del personale assunto, da cui si evince una netta prevalenza di personale in possesso di laurea magistrale.

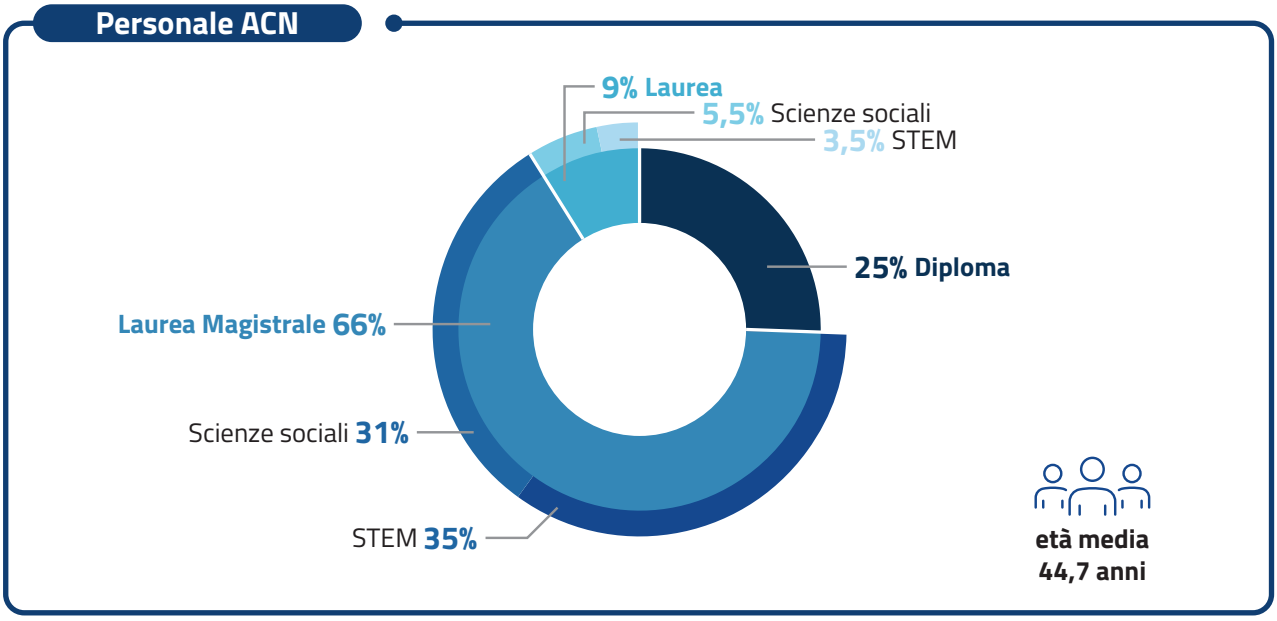


Figura 3 – Titoli di studio ed età media del personale al 31/12/2024

Inoltre, per consolidare e supportare le funzioni istituzionali dell'Agenzia, nel luglio 2024 è stato pubblicato il bando di concorso, finalizzato alla selezione di 45 esperti con orientamento giuridico, articolato in distinti profili: diritto internazionale e dell'Unione europea; diritto amministrativo; diritto delle nuove tecnologie e diritto della cybersicurezza. Sono pervenute 2.284 domande di partecipazione e a ottobre 2024 sono state svolte le prove scritte. I vincitori prenderanno servizio nel 2025, con possibilità di operare mirati scorrimenti delle graduatorie.

Nell'ambito del contingente di esperti in possesso di specifica ed elevata competenza nel campo dell'ICT, previsto dal decreto-legge istitutivo, l'ACN si è avvalsa di un ulteriore professionista per la realizzazione di progetti in materia di comunicazione e disseminazione e, in particolare, per lo svolgimento di attività di comunicazione e sensibilizzazione dei cittadini, dei professionisti, delle PMI e delle grandi imprese italiane sulle minacce digitali.

Sempre ai fini della progressiva strutturazione dell'Agenzia, è stato acquistato l'immobile di Corso d'Italia n. 41, che ha permesso l'immediata operatività istituzionale nella nuova sede, tenendo

conto della necessità di spazi per il personale già in servizio, nonché dell'incremento della dotazione organica. Trattandosi di un edificio di recente ristrutturazione e completo di tutte le dotazioni d'ufficio, nonché di impianti tecnologici e infrastrutture di rete, l'immobile è stato immediatamente fruibile per le necessità dell'Agenzia. Ciò ha consentito di evitare ulteriori spese per l'ammodernamento dell'immobile e di effettuare un celere trasferimento. Anche alla luce delle attività assicurate dall'ACN, la nuova sede è stata individuata quale luogo di interesse per la sicurezza della Repubblica ai sensi del DPCM del 12 giugno 2009, n. 7. È stato, inoltre, dato avvio alle attività volte alla tutela della salute e sicurezza nei luoghi di lavoro.

In un'ottica di rafforzamento del capitale umano, sono proseguite le iniziative formative già avviate nel precedente anno, anche nell'ambito delle collaborazioni con Banca d'Italia e con la SNA.

Sono stati, inoltre, attivati incontri di negoziazione sindacale in relazione alla modifica di alcune disposizioni riguardanti l'orario di lavoro per dare maggiore flessibilità nello svolgimento dell'attività lavorativa, così come è stato avviato il percorso di definizione di un sistema di *welfare* aziendale.

Sono state, altresì, apportate novità organizzative che hanno riguardato soprattutto la dematerializzazione delle procedure dell'Agenzia. In tale ambito, è stata tra l'altro migliorata l'efficienza del sistema di gestione documentale e protocollo informatico, anche attraverso lo sviluppo di nuove funzionalità volte in particolare alla razionalizzazione dei processi interni, producendo così una sensibile riduzione delle tempistiche amministrative e una maggiore valorizzazione delle informazioni disponibili.

Per l'espletamento di attività di natura temporanea e altamente qualificata, l'Agenzia ha indetto procedure comparative per l'affidamento di due incarichi di lavoro autonomo: rispettivamente, per l'analisi, lo studio e la regolamentazione dei rapporti tra reati informatici e incidenti cyber e per le attività connesse all'avvio della gestione e utilizzo della nuova sede.

9.2 PROGRAMMAZIONE ECONOMICO-FINANZIARIA E *PROCUREMENT*

L'ACN è dotata di autonomia contabile e finanziaria e annovera tra le proprie entrate, oltre al finanziamento ordinario, quelle ulteriori elencate nel decreto-legge istitutivo. 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.

Il bilancio d'esercizio 2023 (consuntivo) ha registrato un utile di 35.910.332 euro, che è stato destinato alla costituzione di una riserva di patrimonio netto per la copertura delle future spese di investimento in immobilizzazioni materiali funzionali ad assicurare la piena operatività dell'Agenzia. In relazione agli adempimenti di natura previsionale, nel corso del 2024 sono stati predisposti i provvedimenti di assestamento del bilancio 2024 (revisione del budget economico) e di adozione del bilancio preventivo 2025 (budget economico).

Per quanto riguarda le dimensioni economiche e finanziarie che connotano i bilanci dell'Agenzia, la dotazione ordinaria e le autorizzazioni di spesa, intervenute successivamente con specifiche

disposizioni normative, hanno delineato una progressiva crescita delle risorse finanziarie, in parallelo con la crescita strutturale dell'ACN in termini di compiti e di competenze ad essa affidati. In Figura 4 è riportato lo stanziamento annuale per l'Agenzia previsto a legislazione vigente, considerate anche le rimodulazioni intervenute da ultimo con la legge di bilancio 2025.

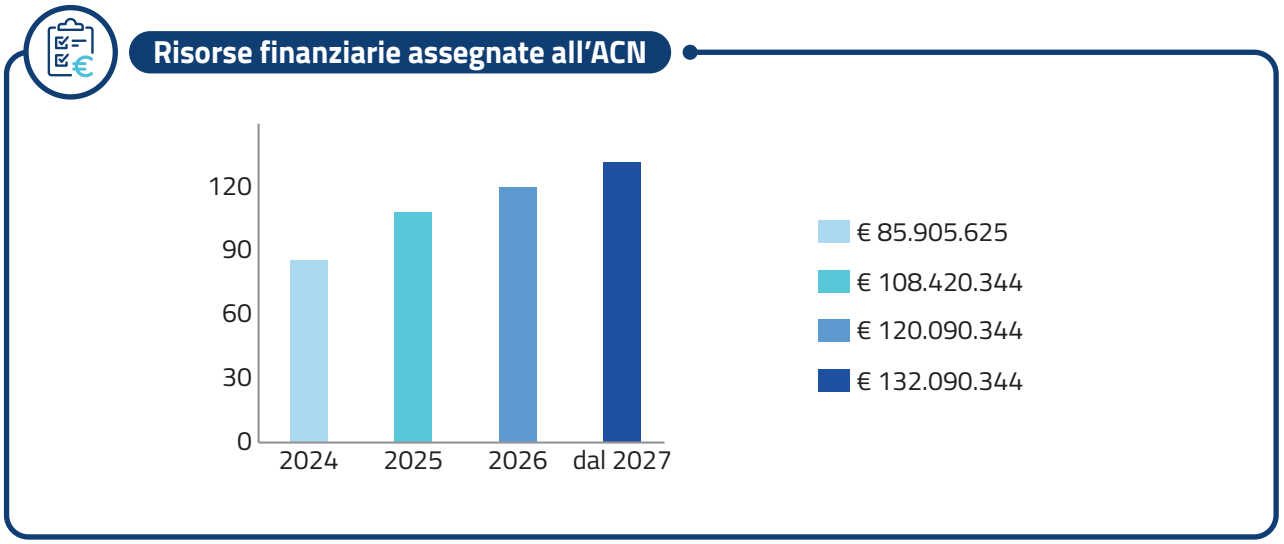


Figura 4 – Risorse finanziarie assegnate all'Agenzia

Inoltre, fino al 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 5. L'Agenzia è, altresì, destinataria di risorse da impiegare per la realizzazione di specifici obiettivi della Strategia nazionale di cybersicurezza (vedasi Capitolo 8).

Una parte delle risorse finanziarie destinate al funzionamento dell'Agenzia è stata dedicata al raggiungimento dell'obiettivo, considerato primario, della crescita di capacità e specifiche professionalità mediante il reclutamento di personale con elevate competenze nel settore della *cybersecurity*, ma anche, per altro verso, all'acquisizione di immobilizzazioni immateriali e materiali connotate dal forte contenuto di innovazione.

Ciò è avvenuto, in particolare:

- attraverso la strutturazione di una dotazione organica che possa consentire la crescita in termini numerici e lo sviluppo di percorsi di carriera che siano sostenibili finanziariamente nel medio-lungo periodo;
- mediante l'investimento nell'acquisto della nuova sede dell'Agenzia. L'acquisizione ha visto il fruttuoso utilizzo degli utili di esercizio maturati disponibili all'atto dell'approvazione del bilancio di esercizio 2023 e l'attivazione, per la restante parte, di un prestito di Cassa Depositi e Prestiti, che sarà estinto in 10 anni;
- con investimenti in ricerca e sviluppo, finanziati con fondi PNRR, grazie ai quali l'Agenzia intende dare attuazione anche a numerose misure della Strategia nazionale di cybersicurezza, come gli interventi volti alla realizzazione, allo sviluppo o all'evoluzione di applica-

zioni 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.

Nel corso del 2024, è stato notevole l'impegno dell'Agenzia in materia di contratti pubblici, per effetto di un sostanziale cambio di paradigma, dovuto alla piena operatività del nuovo Codice dei contratti pubblici, che prevede, tra le altre cose, la digitalizzazione dell'intero ciclo di vita dei contratti. In tale ambito, nel 2024 sono state avviate, e per la maggior parte concluse, oltre 90 procedure di affidamento.

Ciò è stato possibile anche grazie a significativi progressi in termini di qualificazione come stazione appaltante e di digitalizzazione dei contratti. L'Agenzia, infatti, ha ottenuto la qualificazione con riserva, ai sensi del Codice dei contratti pubblici, nel livello massimo nel settore Servizi e Forniture (SF1) e la sua conseguente iscrizione nell'Elenco delle Stazioni Appaltanti Qualificate, ferma restando la già ottenuta qualificazione di primo livello (L3) per la progettazione e l'affidamento di lavori fino a 1 milione di euro. Inoltre, la digitalizzazione dei contratti pubblici, ha rappresentato la vera grande sfida per l'ACN, favorendo una semplificazione dell'oneroso processo esistente, che va dalla programmazione alla definizione del fabbisogno e fino alla completa esecuzione del contratto.

In tale contesto, l'Agenzia ha incrementato il numero di procedure di gara sopra la soglia comunitaria, avviate anche attraverso l'utilizzo dell'apposita piattaforma messa a disposizione da CONSIP. Alcune di queste, peraltro, sono collegate all'attuazione dei progetti del PNRR, come l'acquisto di un pacchetto di prodotti software per integrare la dotazione strumentale del laboratorio del CVCN.

In maniera complementare, l'ACN si è misurata con diverse procedure di gara per l'acquisizione di beni e servizi nel difficile contemperamento tra gli interessi di tutela della sicurezza nazionale previsti dalla normativa derogatoria in materia di appalti dell'Agenzia (DPCM 1 settembre 2022, n. 166) e i vincoli stringenti posti dal PNRR. In particolare, si evidenzia la procedura relativa all'acquisizione di strumentazione hardware e software per le attività specialistiche di *digital forensics*.

9.3 IL SUPPORTO TECNOLOGICO ALL'ATTIVITÀ ISTITUZIONALE

Nel corso del 2024, l'Agenzia ha portato avanti il lavoro di sviluppo e potenziamento dei sistemi IT a supporto delle attività istituzionali, con l'obiettivo di migliorarne la sicurezza e l'efficienza, guardando anche alle normative in materia di *data protection* e di gestione dei flussi documentali. Di seguito si fa particolare riferimento ad alcune delle progettualità che sono state trattate nell'ambito della Relazione.

La piattaforma HyperSOC ha rappresentato uno dei principali ambiti di attività IT: le nuove funzionalità introdotte per la gestione degli indicatori di compromissione, per l'individuazione avanzata di minacce e per la gestione degli eventi di sicurezza hanno contribuito al potenziamento della capacità di rilevare e rispondere in tempo reale alle minacce cibernetiche. A ciò si aggiunge l'integrazione di sorgenti dati, strutturate e non, che forniscono dati aggiornati riguardo a vulnerabilità,

malware o attacchi, utili per individuare e prevenire i rischi in tempo reale, arricchendo così le informazioni disponibili per l'analisi delle minacce.

Nell'ambito delle attività del CSIRT Italia è attiva la piattaforma *Malware Information Sharing Platform* (MISP) finalizzata allo scambio di informazioni tecniche su minacce ed eventi cyber di interesse, sia per finalità preventive, sia in risposta a specifici incidenti, mediante indicatori di compromissione e informazioni di contesto. È stato, inoltre, creato sul sito web dell'Agenzia il portale CSIRT Italia, che ha previsto il rinnovamento della sezione segnalazioni, anche in attuazione delle rilevanti modifiche normative tra cui la legge n. 90/2024.

Per supportare le Pubbliche Amministrazioni nel processo continuo di gestione del rischio cyber, già dal 2023 l'ACN ha messo a disposizione delle PA la piattaforma *Cyber Risk Management*, che consente l'identificazione dei rischi, la definizione dei piani di trattamento e il relativo monitoraggio. La piattaforma è costantemente aggiornata, offrendo uno strumento utile alle PA per una gestione continuativa e sistemica del rischio.

Notevole impegno ha richiesto il Catalogo delle infrastrutture e dei servizi *cloud* che digitalizza il processo di qualificazione come definito nel nuovo Regolamento *cloud*. Il Catalogo, disponibile sul sito web dell'Agenzia, ha ulteriormente contribuito a semplificare l'accesso delle Pubbliche Amministrazioni a soluzioni *cloud* sicure e conformi ai requisiti previsti, contribuendo a creare un ambiente digitale più sicuro ed efficiente.

Inoltre, per dare attuazione ai nuovi adempimenti richiesti dalla disciplina NIS2, è stata sviluppata la piattaforma dedicata per agevolare l'assolvimento degli obblighi di registrazione previsti nei primi mesi del 2025 e, con le future implementazioni, degli adempimenti successivi di conferimento delle informazioni richieste. Attraverso la piattaforma si è realizzata la digitalizzazione del processo, istituendo un canale di interazione tra i soggetti e l'Agenzia in qualità di Autorità nazionale competente NIS. Già nelle prime settimane di operatività sono state abilitate diverse centinaia di soggetti e di utenze.

Al fine di rendere il sito web istituzionale il punto di approdo centrale per tutte le attività dell'ACN, è stato implementato appieno il portale servizi, che ha offerto accesso a oltre 3.000 organizzazioni, pubbliche e private, e a oltre 4.500 utenti.

Infine, a supporto dell'espansione del perimetro di attività e dell'organico dell'Agenzia, significativo è stato l'impegno per la rifunzionalizzazione della nuova sede istituzionale, che ha previsto il trasferimento della dotazione tecnologica già attiva nella precedente sede e l'aggiunta di nuove postazioni di lavoro.

9.4 COMUNICAZIONE

L'evoluzione della cybersicurezza in una questione centrale per la sicurezza del Paese, nonché per la sua prosperità e proiezione internazionale, ha influenzato la percezione del rischio da parte dei cittadini che utilizzano costantemente i canali informativi e social per conoscere, raccontare e commentare in tempo reale fatti di rilevanza pubblica. Per questa ragione l'Agenzia svolge un'attività fondamentale di comunicazione e relazioni con i media per fornire un'informazione chiara e puntuale della minaccia cyber e delle contromisure messe a disposizione dall'ACN.

Il rapporto con l'opinione pubblica è assicurato attraverso l'aggiornamento costante del sito istituzionale e dei canali social dell'Agenzia, con la realizzazione di articoli, post, infografiche, video, guide e documenti, e da un rapporto diretto con gli organi di stampa e televisivi per comunicare in maniera efficace le attività istituzionali che l'ACN svolge. La comunicazione ha riguardato, in particolare, l'attività di diffusione e conoscenza circa il ruolo, le funzioni e l'identità dell'ACN, nonché le iniziative strategiche che ne hanno rafforzato il posizionamento anche nel contesto internazionale.

Nel 2024 sono state realizzate circa 200 interviste a figure apicali dell'ACN, prodotti 70 comunicati stampa e organizzate 7 conferenze stampa. Due di queste sono scaturite dal Gruppo di lavoro G7 sulla cybersicurezza e hanno ricevuto copertura nelle edizioni di prima fascia serale dei telegiornali nazionali, oltre che sulle testate giornalistiche. L'attività redazionale sul sito web istituzionale ha prodotto 150 notizie, con circa 140.000 visualizzazioni. La proiezione sulla stampa e presso le agenzie di informazione ha visto oltre 2.400 lanci di agenzia con citazione dell'ACN o dei suoi vertici, circa 1.300 articoli dedicati, di cui circa 850 articoli sulle testate digitali e 450 sulla carta stampata.

L'Agenzia nel 2024 si è concentrata su attività volte a favorire la cultura digitale e facilitare la conoscenza di norme, buone pratiche e indirizzi sulla cybersicurezza, anche attraverso diverse campagne di comunicazione e la partecipazione a eventi rilevanti per l'ambito cyber.

Di particolare rilievo è stata la prima campagna di comunicazione integrata, dedicata alla consapevolezza delle PMI, dal titolo "Accendiamo la cybersicurezza. Proteggiamo le nostre imprese", realizzata insieme al Dipartimento per l'informazione e l'editoria della Presidenza del Consiglio dei ministri. Da luglio a dicembre 2024, sono stati effettuati 645 passaggi televisivi e radiofonici sulle reti RAI, le TV e le radio commerciali, permettendo di raggiungere complessivamente oltre 113 milioni di telespettatori. Sui social, invece, è stato raggiunto quasi 1 milione di visualizzazioni per i video della campagna,mentre i contenuti digitali hanno avuto quasi 21 milioni di visualizzazioni e 70.000 clic al link della pagina dedicata sul sito dell'ACN.

Molto efficace è stata anche la campagna di informazione sul nuovo Regolamento *cloud* realizzata in collaborazione con il DTD e con l'ANCI, portata avanti attraverso incontri che hanno coinvolto circa 700 rappresentanti della PA locale, attività di stampa e comunicazione e la creazione di un'apposita area web, che risulta essere la sezione più visitata dopo la pagina "Lavora con noi".

Infine, la nuova disciplina NIS2 ha visto l'Agenzia impegnata in un'articolata attività di divulgazione dei nuovi obblighi, anche attraverso una sezione dedicata del sito che ospita – tra le altre cose – 5 video informativi, che hanno raggiunto decine di migliaia di visualizzazioni sul canale YouTube dell'ACN.

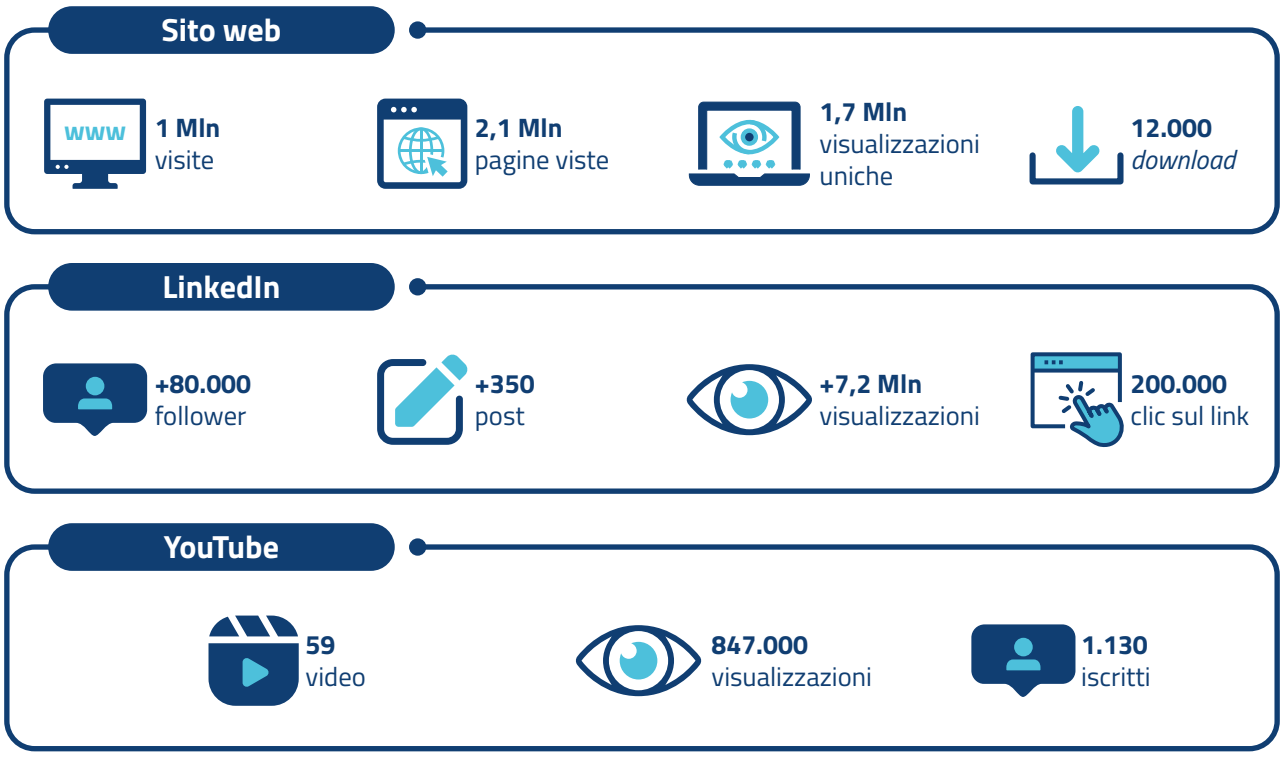
Anche tali attività hanno contribuito a una sostanziale crescita dei canali di comunicazione istituzionale. Il sito web dell'ACN ha rappresentato un punto di riferimento per tutti gli utenti – e in

particolare gli operatori più direttamente interessati dalla normativa cyber – totalizzando 1 milione di visite durante l'anno. Il sito web ha, inoltre, ampliato e diversificato la propria offerta informativa, con contenuti di approfondimento anche su CSIRT Italia, *cloud*, NCC e NIS. Sono circa 2,1 milioni le pagine viste e circa 1,7 milioni le visualizzazioni uniche, con circa 12.000 *download* di documenti. Il maggior afflusso di visitatori si è avuto in occasione di alcune specifiche attività illustrate nelle pagine precedenti:

- 12.656 visite in relazione all'evento NIS2 del 27 novembre;
- 9.801 visite in occasione del lancio della campagna in favore delle PMI;
- 5.871 visite per la pubblicazione del bando di concorso per 45 esperti con profilo giuridico.

La pagina LinkedIn ha raggiunto, a dicembre 2024, più di 80.000 follower (+54% rispetto all'anno precedente). Sono stati pubblicati oltre 350 post, triplicati rispetto all'anno precedente, e si contano oltre 7,2 milioni di visualizzazioni, circa 63.000 reazioni e quasi 1.300 condivisioni. I post hanno raggiunto oltre 3,2 milioni di utenti e prodotto quasi 200.000 clic sul link.

L'account YouTube ha subito un'impennata rispetto alla sua fase sperimentale del 2023, con la pubblicazione di 59 video, per un totale di 847.000 visualizzazioni, e 1.130 iscritti. Il video con più visualizzazioni è stato lo spot della campagna PMI, con 737.616 visualizzazioni, seguito dai tre *tutorial* per professionisti (40.278), dipendenti (22.727) e dirigenti (11.745). Segue, ancora, il video della diretta dell'evento NIS2 con 7.271 visualizzazioni.



10.

LISTA DEGLI ACRONIMI

A

AES: *Advanced Encryption Standard*

AGCOM: Autorità per le garanzie nelle comunicazioni

AgID: Agenzia per l'Italia digitale

AIFA: Agenzia italiana del farmaco

AISCAT: Associazione italiana società concessionarie autostrade e trafori

AISE: Agenzia informazioni e sicurezza esterna

AISI: Agenzia informazioni e sicurezza interna

ANCI: Associazione nazionale dei Comuni italiani

APT: *Advanced Persistent Threat*

ARERA: Autorità di regolazione per energia reti e ambiente

C

CCRA: *Common Criteria Recognition Arrangement*

CDP: Cassa Depositi e Prestiti

CER: *Critical Entities Resilience Directive*

CIC: Comitato interministeriale per la cybersicurezza

CIN: *Cyber innovation network*

CINI: Consorzio nazionale interuniversitario per l'informatica

CISA: *Cybersecurity and Infrastructure Security Agency*

CNA: *CVE Numbering Authority*

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*

CV: Centri di valutazione

CVCN: Centro di valutazione e certificazione nazionale

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

CVE: *Common Vulnerabilities and Exposures*

D

DDoS: *Distributed Denial of Service*

DEP: *Digital Europe Programme*

DFIR: *Digital Forensics Incident Response*

DG CONNECT: Direzione generale delle reti di comunicazione, dei contenuti e delle tecnologie

DNS: *Domain Name System*

DORA: *Digital Operational Resilience Act*

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

E

ECASEC: *European Competent Authority on Secure Electronic Communication*

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

ECCG: *European Cybersecurity Certification Group*

ECSF: *European Cybersecurity Skills Framework*

EDS: Ecosistema dei dati sanitari

EDT: *Emerging and Distruptive Technologies*

eIDAS: *electronic Identification, Authentication and trust Services*

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

EUCC: *European Common Criteria-based cybersecurity certification*

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

EUDI: *European Digital Identity Wallet*

F

FNCS: *Framework* nazionale per la *cyber security* e la *data protection*

G

GPDP: Garante per la protezione dei dati personali

H

HPC: *High Performance Computing*

HWPCI: *Horizontal Working Party on Cyber Issues*

I

IA: Intelligenza artificiale

ICAO: *International Civil Aviation Organization* – Organizzazione internazionale dell'aviazione civile

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

IMEC: *India-Middle East Economic Corridor*

IOC: *Indicator of Compromise* – Indicatore di compromissione

IPZS: Istituto Poligrafico e Zecca dello Stato

ISAC: *Information Sharing and Analysis Centre*

ITS: Istituti tecnologici superiori

IVASS: Istituto per la vigilanza sulle assicurazioni

IXP: *Internet Exchange Point*

L

LAP: Laboratori accreditati di prova

LVS: Laboratori di valutazione della sicurezza

M

MAECI: Ministero degli affari esteri e della cooperazione internazionale

MASE: Ministero dell'ambiente e della sicurezza energetica

MEF: Ministero dell'economia e finanze

MIM: Ministero dell'istruzione e del merito

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

MISP: *Malware Information Sharing Platform*

MIT: Ministero delle infrastrutture e dei trasporti

MUR: Ministero dell'università e della ricerca

N

NATO: Organizzazione del Trattato dell'Atlantico del Nord

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

NCCS: *Network Code on Cybersecurity*

NCS: Nucleo per la cybersicurezza

NIS: *Network and Information Systems*

NISP: Nucleo interministeriale situazione e pianificazione

NIST: *National Institute of Standards and Technology*

O

OCSI: Organismo di certificazione della sicurezza informatica

OEWG: *Open-Ended Working Group on security of and in the use of ICT 2021-2025*

OSCE: Organizzazione per la sicurezza e la cooperazione in Europa

P

PA: Pubblica Amministrazione

PMI: Piccole e medie imprese

PNRR: Piano nazionale di ripresa e resilienza

PSNC: Perimetro di sicurezza nazionale cibernetica

R

RaaS: *Ransomware as a Service*

S

SNA: Scuola nazionale dell'Amministrazione

SOC: *Security Operations Center*

SOG-IS MRA: *Senior Officials Group Information Systems Security Mutual Recognition Agreement*