Relazione annuale al Parlamento

2025

Relazione annuale al Parlamento

2025

Indice

Introduzione

La cybersicurezza ci permette di abitare il mondo nuovo prodotto dalla rivoluzione digitale, ed essendone un fattore abilitante ne è, allo stesso tempo, un elemento essenziale, indefettibile.

All'interno dell'ambiente digitale, e per mezzo di esso, operano soggetti istituzionali, economici e sociali che attraverso sistemi, reti e infrastrutture informatiche perseguono finalità che interessano cittadini, imprenditori, Pubbliche Amministrazioni, in una parola la comunità nazionale. Per questo lo spazio cibernetico va regolato e protetto.

Esso è tuttavia uno spazio mutevole, attraversato da frizioni e conflitti di natura locale e globale, che cambia in relazione alle spinte dell'innovazione tecnologica, delle abitudini di vita e di lavoro, delle modalità di produzione della ricchezza.

Negli ultimi anni la robotica, l'intelligenza artificiale, la *data science* e le piattaforme hanno enormemente accresciuto le possibilità insite nella dimensione digitale. A questo progresso, ha però corrisposto un forte aumento dell'aggressività della minaccia. Attori mossi da opportunismo economico, statuali o *state-sponsored*, nonché hacktivisti ideologicamente orientati, popolano, con diversità di intenzioni, mezzi e capacità, il cyberspazio, alimentando la criminalità cibernetica. Nuovi strumenti offensivi, o l'uso malevolo di quelli esistenti, supportato da tecnologie *disruptive*, l'ha resa ancora più temibile e lesiva.

L'Agenzia per la cybersicurezza nazionale ha il compito di garantire, nella sua essenza, la resilienza sistemica dell'Italia, con l'obbiettivo prioritario di tutelare gli interessi nazionali nella dimensione digitale.

Questo compito viene perseguito dall'Agenzia nei modi e nelle forme che la legge istitutiva, e quelle successive, le affidano, e che essa svolge in collaborazione con gli altri attori della protezione cibernetica.

Le direttrici principali di questa azione sono quelle individuate e descritte nei più rilevanti "*Index*" europei e internazionali che analizzano i fattori di successo alla base delle politiche nazionali cyber.

Essi consistono nella definizione di una strategia di *cybersecurity*; nell'esistenza di un'agenzia per la sicurezza cibernetica; nella presenza di un *Computer Security Incident Response Team* (CSIRT); nella collaborazione tra settore pubblico e settore privato; nella creazione di una forza lavoro competente e qualificata; infine, nella promozione della consapevolezza della gravità del rischio cibernetico da parte dei cittadini.

Ebbene, rispetto a questi fattori, l'Italia ha già raggiunto un livello di maturità che la colloca nel novero delle nazioni più avanzate.

Lo dimostrano i fatti che questa Relazione, al pari di quelle che l'hanno preceduta, si prefigge di illustrare.

L'Agenzia può mostrare, alla fine del 2025, di aver portato a termine, anche con il contributo, talora decisivo, di altre Amministrazioni, ben 60 delle 82 misure contenute nella Strategia nazionale di cybersicurezza; ha rafforzato significativamente la presenza al suo interno di unità ad alta specializzazione, proseguendo a strutturare Servizi e Articolazioni in coerenza con l'evoluzione del quadro giuridico nazionale e unionale; tramite il CSIRT Italia, ha profuso, nell'anno appena trascorso, un intenso impegno nel fronteggiare la minaccia, apparsa incrementale anche a causa del crescente numero di notifiche di incidenti legate all'implementazione della legge n. 90 del 2024 e della NIS2; sul piano del partenariato pubblico e privato, ha concluso accordi collaborativi con entità del mondo accademico e del mondo industriale, con feconda interposizione tra ricerca, innovazione e trasferimento tecnologico; infine, ha realizzato svariate iniziative di sensibilizzazione e formazione, rivolte ad ambiti sociali diversi, dando vita a un esercizio di pedagogia civile nei riguardi del rischio cibernetico.

L'incessante evoluzione delle tecnologie, e soprattutto l'avvento di quelle emergenti, sono alla radice del continuo rincorrersi tra sviluppo e regolazione. Il Regolamento sull'intelligenza artificiale dell'Unione europea rappresenta solo l'apice di questo fenomeno, nutrito da fermenti geopolitici, mentre già si profilano sullo sfondo ulteriori sviluppi che porteranno la regolazione a nuovi approdi, anche rivolti a semplificare l'implementazione degli obblighi di *compliance*.

L'Agenzia è fortemente interessata ai riflessi che la vicenda digitale produce in ambito regolatorio.

Nel 2025, oltre alla già accennata implementazione della NIS2, l'ACN è stata designata Autorità di vigilanza del mercato sull'intelligenza artificiale e, in tale veste, ha preso parte alle iniziative avviate in seno all'*AI Board*.

Del resto, la collaborazione costante con le istituzioni brussellesi, rivolta allo scambio e alla condivisione di conoscenze, informazioni e *best practice*, rimane fondamentale per affinare il contrasto alla minaccia cibernetica.

In Italia, l'azione difensiva dell'Agenzia – che nei *network* europei di CSIRT e CyCLoNe ha visto accresciuti il suo peso e il suo prestigio –, ha consentito di respingere e contenere, mitigandone gli effetti, migliaia di attacchi.

Nel 2025, sebbene gli eventi malevoli nel cyberspazio siano aumentati del 38%, gli incidenti, cioè gli attacchi con impatto confermato, sono cresciuti in una misura non corrispondente, solo del 7%.

Il nostro ruolo di coordinamento si è manifestato anche condividendo con gli altri attori della cybersicurezza l'andamento dei fenomeni ostili. Il Nucleo per la cybersicurezza (NCS), convocato con cadenza almeno mensile, e sempre nell'immediatezza degli eventi di maggiore allarme, ha visto costantemente l'Agenzia dare cognizione del numero incrementale degli attacchi, della superficie digitale esposta, della tipologia dei vari eventi – DDoS, *phishing*, *ransomware*, esfiltrazione di dati e credenziali, tra quelli principali –, nonché delle vulnerabilità individuate e delle campagne di allertamento condotte.

In ambito digitale, come del resto in quello fisico, la sicurezza corrisponde a un principio di prevenzione e di massima precauzione.

Lo scrutinio tecnologico effettuato a tutela del Perimetro di sicurezza nazionale cibernetica (PSNC), ha consentito alle entità della *constituency* di poter utilizzare, in contesti di elevata sensibilità, beni e servizi informatici di cui sono state verificate, prima del loro impiego, affidabilità e robustezza. Nel 2025, le attività di *testing* hanno consentito anche l'individuazione di decine di vulnerabilità *zero-day*.

Per sostenere la ricerca e l'innovazione, altro grande tema a cui è legata l'autonomia tecnologica, si è dato supporto a *startup* innovative, dottorati e progetti di ricerca. Nondimeno, l'impegno dell'Agenzia su questo versante viene anche affrontato contribuendo, con capacità nazionali, alla realizzazione di uno *stack* tecnologico europeo.

È in questa chiave che si pone la realizzazione dell'infrastruttura di *High Performance Computing* (HPC), denominata Megaride, inaugurata a giugno 2025, frutto di una consolidata collaborazione con il consorzio Cineca. Essa si offre, tra le altre cose, come infrastruttura a sostegno del mondo produttivo, della ricerca e della sicurezza nazionale. E il suo inquadramento nel progetto IT4LIA AI Factory esprime il fortissimo legame con l'impresa comune europea per il calcolo ad alte prestazioni.

Il respiro internazionale dell'attività di ACN si coglie anche nel proseguimento del gruppo di cyber esperti nato in seno all'esercizio G7 per iniziativa dell'Italia.

Nel 2025, il Canada ha ospitato gli incontri di questo nuovo formato di collaborazione, impegnato a riflettere sulle più

attuali questioni legate all'armonizzazione degli standard di cybersicurezza, alla protezione dei sistemi e modelli di intelligenza artificiale e delle infrastrutture energetiche.

La Relazione ripercorre, attraverso numeri e narrazioni orientati a illustrarne l'entità, l'attività di un anno, restituendone – si ha motivo di credere – l'importanza che essa ha rivestito per la superficie digitale del Paese.

Chi scrive non può concludere queste righe di presentazione senza rivolgere un sentito plauso, più che doveroso, al personale tutto dell'Agenzia, di cui apprezza l'elevata professionalità e l'alto senso di responsabilità.

Infine, è altrettanto doveroso ricordare come il Governo abbia espresso pieno sostegno all'Agenzia, indirizzandone l'azione. Più di un segno di attenzione ha, poi, dato il Parlamento all'ACN. Ed è per questo che esprimiamo a entrambi il nostro deferente ringraziamento.

Bruno Frattasi

1

Evoluzione della legislazione cyber

Assicurare un adeguato livello di sicurezza e resilienza cibernetica è uno sforzo complesso, in particolare alla luce di un quadro della minaccia sempre più penetrante e di una crescente pervasività e costante evoluzione delle tecnologie.

In tale contesto, un primo e fondamentale ambito di azione dell'Agenzia per la cybersicurezza nazionale attiene alla costruzione e al mantenimento di un quadro giuridico in linea con le sfide che il Paese deve affrontare e aggiornato secondo le più recenti spinte a livello europeo. Riconoscendo che ogni innovazione tecnologica racchiude in sé sia minacce che opportunità, risulta essenziale che la regolazione anticipi, accompagni e favorisca la transizione digitale mettendo al centro la tutela della sicurezza cyber, sempre più cruciale per garantire la resilienza sistemica.

Il legislatore nazionale ha riconosciuto all'ACN un ruolo di primo piano tramite numerosi interventi normativi che incidono sui diversi aspetti della sicurezza digitale. L'esempio più recente è rappresentato dalla legge sull'intelligenza artificiale che, nel disciplinare le applicazioni dell'IA nel nostro Paese, vede nella cybersicurezza un pilastro abilitante per un uso responsabile e sicuro di tale tecnologia. L'Agenzia è stata, inoltre, impegnata nel consolidamento del quadro regolatorio previsto dalla legge n. 90/2024, focalizzandosi sul tema cruciale degli approvvigionamenti di tecnologie digitali che devono rispondere a stringenti requisiti volti a tutelare la sicurezza nazionale e gli interessi strategici del Paese.

Il 2025 è stato, inoltre, un anno chiave per procedere verso la piena attuazione della disciplina nazionale NIS, attività che ha visto un articolato impegno da parte dell'ACN, con la predisposizione di numerosi provvedimenti, di concerto con tutte le altre Amministrazioni competenti e in raccordo con i vari *stakeholder*. Si è trattato di un lavoro complesso, che ha visto l'estensione di nuovi obblighi a migliaia di soggetti, pubblici e privati, chiamati a farsi parte attiva della protezione della cybersicurezza nazionale. In tale processo, l'Agenzia ha improntato la propria azione ai principi di gradualità e proporzionalità, assicurando un costante accompagnamento nei confronti dei soggetti rientranti nella normativa.

Alla luce delle compenetrazioni tra la normativa nazionale e quella dell'Unione europea, l'ACN ha seguito da vicino anche l'evoluzione della legislazione cyber a livello UE, contribuendo non solo all'attuazione nazionale delle normative comunitarie già in vigore, ma anche ai negoziati su quelle in via di definizione. A tale ultimo riguardo, fondamentale è stata la concertazione con le varie Amministrazioni responsabili per la definizione delle posizioni negoziali nazionali in merito alle proposte della Commissione che incidono sul quadro normativo cyber dell'Unione.

1.1 PRINCIPALI NOVITÀ NORMATIVE IN AMBITO NAZIONALE

1.1.1 La legge sull'intelligenza artificiale: nuove competenze ACN

Con la legge n. 132/2025 si è aggiunto un nuovo tassello al percorso di regolamentazione nazionale delle nuove tecnologie. Questa, in linea con gli indirizzi dell'*AI Act* (Regolamento (UE) 2024/1689), introduce nell'ordinamento le prime disposizioni sulle applicazioni di sistemi e modelli di intelligenza artificiale, adottando un'ottica prettamente antropocentrica.

La legge nasce dalla consapevolezza che i sistemi di IA, caratterizzati da abilità di auto-apprendimento e decisione automatizzata, incidono in maniera profonda e strutturale sull'economia, sulla Pubblica Amministrazione e sulla società nel suo complesso. In tale prospettiva, il legislatore ha perseguito un duplice obiettivo: promuovere un impiego trasparente, etico e responsabile dell'IA e, al contempo, assicurare un controllo effettivo sui rischi economici e sociali, nonché sui potenziali effetti lesivi dei diritti fondamentali.

Vengono, quindi, affermati principi generali di trasparenza, sicurezza, affidabilità e non discriminazione, imponendo che le applicazioni di IA rispettino la libertà di informazione, la protezione dei dati personali e la centralità della decisione umana, contribuendo così a rafforzare la fiducia degli utenti e delle istituzioni. La normativa mira a preservare un equilibrio particolarmente delicato: da un lato, valorizzare le numerose e significative opportunità offerte dalle tecnologie emergenti; dall'altro, prevenire e contenere al massimo i rischi legati a un utilizzo improprio e dannoso delle stesse, nonché quelli derivanti da un loro sottoutilizzo che potrebbe tradursi in una perdita di competitività.

La legge, oltre a fissare principi generali e ambiti di applicazione della materia e a definire le linee strategiche per lo sviluppo dell'IA a sostegno dell'innovazione nazionale, delinea anche l'architettura della *governance* italiana, individuando nell'Agenzia per la cybersicurezza nazionale uno dei perni centrali del sistema. All'ACN, quale Autorità di vigilanza del mercato e punto di contatto, sono, infatti, attribuite funzioni di vigilanza e controllo, nonché poteri sanzionatori con riferimento ai sistemi di IA che presentano profili di rischio per la sicurezza della collettività, la resilienza delle infrastrutture digitali e la tutela degli interessi strategici dello Stato.

La *governance* prevede, inoltre, un ruolo prominente in capo all'Agenzia per l'Italia digitale (AgID) a cui è attribuito il ruolo di Autorità di notifica, con compiti di valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale. Tra le altre cose, l'AgID e l'ACN sono chiamate ad assicurare l'istituzione e la gestione congiunta di spazi di sperimentazione normativa (c.d. *sandbox*) ciascuna per gli ambiti di competenza e ferme restando le specifiche attribuzioni di altre Amministrazioni.

All'ACN è attribuito, altresì, il compito di promuovere e sviluppare ogni iniziativa finalizzata a valorizzare l'intelligenza artificiale quale risorsa per il rafforzamento della cybersicurezza nazionale, anche mediante la stipula di accordi di collaborazione con i soggetti privati, nonché tramite strumenti di partenariato pubblico-privato. L'assegnazione di tale ulteriore compito all'Agenzia risulta perfettamente coerente con l'impostazione europea che riconosce la crucialità della cybersicurezza per le varie applicazioni dell'IA. I sistemi di intelligenza artificiale sono, infatti, essi stessi esposti ad attacchi cyber sofisticati che possono alterarne il funzionamento, minarne l'affidabilità e pregiudicarne l'integrità.

La legge sull'IA disciplina, inoltre, l'applicazione dell'intelligenza artificiale in ambiti settoriali di particolare rilevanza strategica e sociale tra i quali figurano la sanità, la ricerca scientifica, il lavoro, la Pubblica Amministrazione e l'attività giudiziaria. Quanto al settore sanitario, ad esempio, è essenziale che le innovazioni che potranno essere garantite dall'utilizzo dei sistemi di IA si muovano all'interno di una cornice regolatoria rigorosa, anche al fine di ridurre l'estensione della superficie esposta ad attacchi cyber. È per questo che l'Agenzia è chiamata, da un lato, a collaborare con le altre Amministrazioni competenti a definire le modalità di trattamento dei dati della piattaforma di intelligenza artificiale in ambito sanitario. In altri casi, l'ACN è, invece, coinvolta all'interno di tavoli specifici per valutare e promuovere un utilizzo etico, responsabile e sicuro dell'IA nei diversi contesti.

La legge si completa, infine, con una visione di politica industriale di ampio respiro. Difatti, prevede che l'ACN faccia parte degli organi di governo dei fondi di *venture capital* destinati al finanziamento, mediante capitale di rischio, di imprese che operano in Italia nei settori dell'intelligenza artificiale, della cybersicurezza, delle tecnologie quantistiche e dei sistemi di telecomunicazioni. Si tratta di un intervento di notevole portata, che prevede investimenti fino a un valore complessivo di un miliardo di euro.

Ulteriori attività in materia di IA

L'Agenzia continua a partecipare alle iniziative di accompagnamento all'attuazione dell'*AI Act* promosse dalla Commissione europea, quali l'elaborazione del Codice di condotta per i sistemi di IA a uso generale e la predisposizione dei documenti di lavoro risultanti dalle riunioni dei sottogruppi dell'*AI Board* (vedasi Capitolo 6).

Sul piano tecnico, l'ACN assicura, altresì, la propria presenza ai lavori dei tavoli di normazione tecnica in materia di IA, funzionali alla definizione degli standard necessari allo svolgimento delle attività di vigilanza del mercato.

Nel loro complesso, le attività di monitoraggio e partecipazione dell'Agenzia contribuiscono a garantire un presidio tecnico-istituzionale costante sulle evoluzioni del quadro normativo europeo in materia di cybersicurezza e di regolazione dell'intelligenza artificiale, nel rispetto delle competenze delle singole Amministrazioni coinvolte.

1.1.2 La legge n. 90/2024: ulteriori passi applicativi per la sicurezza degli approvvigionamenti

Nel quadro delle politiche di rafforzamento della sicurezza nazionale e di tutela degli interessi strategici dello Stato nel dominio cibernetico, si sta progressivamente delineando un sistema organico di misure volte a presidiare l'approvvigionamento di beni e servizi informatici impiegati in contesti sensibili, dal momento che la *supply chain* rappresenta uno dei principali vettori di attacco. Tale approccio ha già trovato espressione in una serie di provvedimenti che, a partire dall'inclusione della cybersicurezza nel Codice dei contratti pubblici (D.Lgs. n. 36/2023), sono finalizzati, tra l'altro, a garantire la sicurezza informatica nell'ambito dell'approvvigionamento di prodotti e servizi tecnologici.

Ciò è stato ulteriormente consolidato con la legge n. 90/2024 che ha previsto l'individuazione di elementi essenziali di cybersicurezza che le Pubbliche Amministrazioni, i gestori di servizi pubblici, le società a controllo pubblico, nonché i soggetti privati inseriti nel Perimetro di sicurezza nazionale cibernetica (PSNC) devono tenere in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici. Inoltre, la legge prevede l'applicazione di criteri di premialità, nei casi connessi alla tutela della sicurezza nazionale, per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea, alla NATO o di Paesi terzi tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

Nel 2025, tale impianto ha trovato concreta applicazione nei decreti del Presidente del Consiglio dei ministri del 30 aprile 2025 e del 2 ottobre 2025, entrambi adottati su proposta dell'ACN, previo parere del Comitato interministeriale per la sicurezza della Repubblica (CISR), chiamato a pronunciarsi in considerazione dei richiamati profili di sicurezza nazionale.

Figura 1 – La cybersicurezza degli approvvigionamenti: principali tappe

In particolare, il DPCM del 30 aprile 2025 definisce, per specifiche categorie tecnologiche impiegate per la tutela degli interessi strategici nazionali, gli elementi essenziali di cybersicurezza che i soggetti interessati sono tenuti a considerare nelle attività di approvvigionamento, al fine di mitigare i rischi cibernetici. Il decreto indica, altresì, i casi in cui, per la tutela della sicurezza nazionale, devono essere applicati i criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza nazionali, dei Paesi UE, NATO, nonché dei Paesi terzi, i quali sono individuati dal DPCM stesso (Australia, Corea del Sud, Giappone, Israele, Nuova Zelanda, Svizzera).

Con il DPCM del 2 ottobre 2025 è stato esteso l'ambito di applicazione delle predette disposizioni ai servizi e sistemi di telefonia mobile 4G e 5G, nonché alle successive evoluzioni tecnologiche. L'inclusione delle reti mobili di nuova generazione riflette la loro crescente rilevanza strategica quali infrastrutture abilitanti per servizi essenziali, funzioni critiche dello Stato e applicazioni ad alto impatto sistemico.

A completamento di tale quadro, l'Agenzia ha adottato nell'ottobre 2025, sentita l'Autorità nazionale anticorruzione (ANAC), le Linee guida per l'applicazione dei criteri di premialità con l'obiettivo di fornire indicazioni operative chiare e uniformi per accompagnare i soggetti chiamati ad applicare tali criteri nell'ambito delle rispettive procedure di approvvigionamento.

FOCUS

Linee guida per l'applicazione dei criteri di premialità

Le stazioni appaltanti e le centrali di committenza potranno procedere con apposite gare o lotti dedicati ai quali applicare i criteri di premialità, al fine di soddisfare il relativo quadro esigenziale e di rispettare le finalità di tutela della sicurezza nazionale: per agevolare l'attività di predisposizione dei bandi di gara, le Linee guida contengono due esempi di clausole-tipo per l'attribuzione della premialità.

L'applicazione della premialità si basa sull'analisi di un inventario di tutti i componenti di fabbricazione del prodotto o delle infrastrutture impiegate per erogare un servizio (Bill of Materials-BOM). Le Linee guida prevedono, da un lato, l'indicazione del bene o del servizio oggetto di descrizione e, dall'altro, un elenco di componenti di cui l'oggetto della fornitura è costituito. A tal proposito, l'ACN ha predisposto e messo a disposizione un tool, strumento operativo dedicato all'analisi del BOM, che consente di esaminare in modo automatizzato la composizione tecnologica delle soluzioni offerte, per attribuire il punteggio premiale e di ridurre il rischio di valutazioni discrezionali o disomogenee. Ai fini dell'attribuzione del criterio di premialità, ciascuno dei componenti elencati nel BOM deve essere riconducibile a uno dei Paesi "trusted" individuati dal DPCM 30 aprile 2025; in tale ottica, viene suggerito di considerare il Paese in cui è localizzato il sito produttivo dei componenti o il luogo di erogazione dei servizi.

1.1.3 La nuova disciplina NIS: stato di attuazione

Nel 2025 l'Agenzia ha proseguito nell'attuazione della nuova disciplina NIS di derivazione europea (D.Lgs. n. 138/2024, c.d. decreto NIS, di recepimento della Direttiva (UE) 2022/2555) che ha innalzato il livello di cybersicurezza in tutta l'Unione, portando avanti la definizione dell'impianto regolatorio. Questo è stato adottato a valle di un'articolata attività di coinvolgimento dei soggetti pubblici e privati a vario titolo interessati, caratterizzata da un approccio sistematico volto a soddisfare le specifiche esigenze nazionali, garantendo il principio di proporzionalità e quello di gradualità.

Ciò ha consentito di delineare un percorso di attuazione graduale degli adempimenti prescritti, scandito temporalmente in fasi attuative definite alla luce dei termini stabiliti per l'adozione della disciplina di rango secondario e per l'adempimento dei relativi obblighi da parte dei soggetti (Figura 2).

Figura 2 – Fasi attuative NIS

L'ACN, in qualità di Autorità nazionale competente NIS, ha continuato a svolgere funzioni di indirizzo e coordinamento, garantendo al contempo continuo supporto ai soggetti NIS, pubblici e privati, anche al fine di favorire l'uniforme applicazione della disciplina e il progressivo innalzamento del livello complessivo di resilienza cibernetica del Paese. In questo contesto, particolarmente importante è stata la collaborazione con le Autorità di settore all'interno del Tavolo per l'attuazione della disciplina NIS (vedasi Capitolo 3), chiamato a contribuire alla definizione delle basi dell'impianto regolamentare, attività che nel 2025 si è caratterizzata per un intenso lavoro di produzione normativa di fonte secondaria (DPCM e Determinazioni del Direttore generale dell'ACN). La collaborazione si è, altresì, estesa anche ai Tavoli settoriali, coordinati e promossi dalle diverse Autorità di settore, che consentono consultazioni mirate volte a realizzare un modello di regolamentazione partecipata.

Il primo obbligo cui i soggetti NIS hanno dovuto adempiere nel 2025 è stata la registrazione sulla piattaforma digitale resa disponibile dall'Agenzia, che ha permesso la costituzione e il progressivo consolidamento dell'elenco dei soggetti, essenziali e importanti. In considerazione dell'elevato numero di autodichiarazioni circa l'appartenenza all'ambito di applicazione ricevute in fase di prima registrazione (oltre 30.000), è stata necessaria un'attività di verifica che ha restituito una platea di soggetti NIS profondamente ampliata rispetto alla precedente disciplina di cui al D.Lgs. n. 65/2018. I soggetti, dunque, si sono attestati per il 2025 in oltre 21.800, ripartiti per settori di attività, come specificato in Figura 3.

Per modulare gli obblighi discendenti dal decreto NIS, i soggetti sono divisi tra essenziali e importanti a seconda del settore nel quale operano e delle loro dimensioni. Nell'ambito della loro individuazione, al fine di garantire la concreta declinazione del principio di proporzionalità è stato adottato il provvedimento che disciplina la c.d. clausola di salvaguardia (DPCM n. 221/2024), che definisce i presupposti e le modalità per richiedere l'applicazione della clausola. In particolare, a fronte del generale criterio dimensionale per l'individuazione dei soggetti NIS, è stata prevista la possibilità per un soggetto di esserne escluso al fine di evitare effetti sproporzionati nel caso in cui sussistano determinate condizioni. In considerazione degli stringenti presupposti e criteri per richiedere e ottenere la concessione della clausola di salvaguardia, essa ha trovato una limitata applicazione: la clausola è stata concessa il 31% delle volte su circa 1.600 richieste.

Allegato I: settori ad alta criticità

Energia
oltre 2.000

Trasporti
oltre 500

Settore bancario
oltre 300

Infrastrutture dei mercati finanziari
meno di 100

Sanitario
oltre 2.000

Acqua potabile
oltre 200

Acque reflue
oltre 200

Infrastrutture digitali
oltre 2.000

Gestione dei servizi TIC
oltre 2.000

Spazio
meno di 100

Allegato II: altri settori critici

Servizi postali e di corriere
oltre 100

Gestione dei rifiuti
oltre 1.000

Fabbricazione, produzione e distribuzione di sostanze chimiche
oltre 1.000

Produzione, trasformazione e distribuzione di alimenti
oltre 3.000

Fabbricazione
oltre 4.000

Fornitori di servizi digitali
oltre 1.000

Ricerca
oltre 100

Allegato III: Amministrazioni centrali, regionali, locali e di altro tipo

oltre 300

Allegato IV: ulteriori tipologie di soggetti

oltre 200

Figura 3 – Soggetti NIS nel 2025

Un ulteriore adempimento portato a compimento nel corso del 2025 ha riguardato l'adozione della Determinazione ACN con cui si stabiliscono le specifiche di base relativamente alle misure di sicurezza da adottare e agli incidenti significativi da notificare. Si tratta, in particolare delle:

- misure di sicurezza di base che i soggetti NIS sono tenuti ad adottare per l'assolvimento degli obblighi in materia di gestione dei rischi per la sicurezza informatica, entro 18 mesi dalla ricezione della comunicazione di inserimento nell'elenco dei soggetti NIS;
- le tipologie di incidenti significativi di base che i soggetti NIS sono tenuti a notificare al CSRIT Italia, entro 9 mesi dalla ricezione della comunicazione di inserimento nell'elenco dei soggetti NIS.

Sempre per rispettare il criterio di proporzionalità, entrambe le specifiche di base sono modulate diversamente a seconda che si applichino a soggetti essenziali o importanti.

La Determinazione detta anche la disciplina transitoria per i soggetti del Perimetro di sicurezza nazionale cibernetica che sono anche soggetti NIS, per gli operatori di servizi essenziali (OSE) precedentemente sottoposti al D.Lgs. n. 65/2018, nonché per gli operatori del settore delle telecomunicazioni (Figura 4).

SOGGETTO	DEFINIZIONE	REGIME TRANSITORIO
PSNC-NIS	Soggetti PSNC che sono anche soggetti NIS	Sui sistemi informativi e di rete diversi da quelli PSNC l'obbligo di notifica degli incidenti significativi di base è anticipato a decorrere dal 30 aprile 2025
OSE **Operatori di servizi essenziali**	Soggetti NIS identificati ai sensi della precedente disciplina NIS (D.Lgs. n. 65/2018)	Sui sistemi informativi e di rete che abilitano i servizi essenziali (ex D.Lgs. n. 65/2018) si applica l'obbligo di mantenimento delle misure tecniche e organizzative già adottate prima del decreto NIS Sui medesimi sistemi l'obbligo di notifica degli incidenti significativi di base è anticipato a decorrere dal 30 aprile 2025
TELCO **Operatori di telecomunicazioni**	Soggetti NIS che forniscono reti o servizi di comunicazione elettronica accessibili al pubblico (ex D.Lgs. n. 259/2003) a ≥ 1% della base utenti nazionale o ≥ 1 milione di utenti	Sulle reti di comunicazione elettronica si applica l'obbligo di mantenimento delle misure di sicurezza e integrità già adottate ai sensi del decreto del Ministero dello sviluppo economico del 12 dicembre 2018 (c.d. decreto TELCO) Sui medesimi sistemi l'obbligo di notifica degli incidenti significativi di base è anticipato a decorrere dal 30 aprile 2025

Figura 4 – Disciplina transitoria

A fine 2025 è stato messo un ulteriore tassello, attraverso la condivisione con il Tavolo NIS, per l'adozione della Determinazione ACN relativa alla politica nazionale di divulgazione coordinata delle vulnerabilità (*Coordinated Vulnerability Disclosure*-CVD). La politica, sulla quale è stata preventivamente acquisita l'intesa del Ministero della giustizia, è volta a disciplinare un processo strutturato attraverso il quale eventuali vulnerabilità nei sistemi informatici e di rete siano segnalate al fabbricante/fornitore dei prodotti o servizi ICT, per consentire a questi ultimi di riconoscerle e risolverle. In tale processo, l'ACN svolge il ruolo di coordinatore, agendo quale intermediario di fiducia (attraverso il CSIRT Italia) tra il segnalante e il fabbricante/fornitore. Un efficace processo di CVD fa sì che le vulnerabilità divengano di dominio pubblico non prima che ne sia stata individuata una soluzione, così da ridurre il rischio che queste vengano sfruttate dagli attaccanti.

FOCUS

La politica nazionale di CVD

Essendo stata elaborata a legislazione vigente, tale politica non reca una disciplina in materia di tutela dei segnalanti delle vulnerabilità sotto i profili della responsabilità civile e penale. In particolare, la politica nazionale di CVD:

- *richiama l'attenzione dei segnalanti sul fatto che le attività di ricerca delle vulnerabilità non devono integrare alcuna fattispecie criminosa (come, a titolo esemplificativo, quella di accesso abusivo a sistema informatico o telematico di cui all'art. 615-ter del Codice penale);*
- *chiarisce che la garanzia dell'anonimato – esperibile su specifica richiesta dal segnalante – non esclude che l'ACN possa trattare informazioni potenzialmente identificative (es. indirizzo IP) e fa salve le ipotesi in cui l'Agenzia sia tenuta a comunicarle alle autorità competenti (es. ipotesi di reato), prevedendo, comunque, l'adozione di specifiche misure a tutela della riservatezza;*
- *fonda una serie di obblighi in capo al segnalante, attraverso la sua adesione alla politica di CVD, nel momento in cui procede alla segnalazione;*
- *invita alla collaborazione con il CSIRT Italia i fabbricanti/fornitori, evidenziando, tuttavia, che tale collaborazione verrebbe considerata obbligatoria nel caso in cui si dovesse trattare di una vulnerabilità attivamente sfruttata.*

Sempre nel corso del 2025 è stata adottata anche la Determinazione ACN recante le modalità con cui i soggetti NIS notificano all'Autorità nazionale competente NIS la loro partecipazione agli accordi di condivisione delle informazioni sulla sicurezza informatica. In particolare, è stato previsto che tale notifica avvenga tramite la piattaforma digitale NIS e, in un'ottica di armonizzazione delle attività, l'adempimento viene ricondotto al più generale aggiornamento delle informazioni che i soggetti NIS devono condividere su base annuale e tempestivamente a seguito di modifiche.

A completamento dell'articolato sforzo di attuazione, l'Agenzia ha fornito un continuo supporto ai soggetti NIS attraverso diverse modalità. Innanzitutto, la piattaforma NIS sul Portale servizi ha subito un'evoluzione significativa passando da alcuni servizi offerti a una platea di centinaia di organizzazioni e utenti, a molteplici servizi offerti a decine di migliaia di organizzazioni e un numero ancora più elevato di utenti (vedasi Capitolo 9). In parallelo, il sito istituzionale è stato arricchito con una sezione dedicata alla nuova disciplina, recante pagine di sintesi sui diversi aspetti del decreto NIS, nonché un ampio catalogo di risposte a domande frequenti. Inoltre, è stato attivato un *service desk* tramite il quale i soggetti possono porre all'ACN quesiti circa i diversi aspetti del decreto NIS, nonché richiedere assistenza per difficoltà di carattere tecnico-procedurale, che ha reso possibili oltre 45.000 interlocuzioni.

Infine, sono state pubblicate le prime 2 Linee guida per accompagnare i soggetti nella realizzazione degli adempimenti previsti dal decreto NIS:

- Specifiche di base – Guida alla lettura: documento volto a facilitare la comprensione e interpretazione del testo delle specifiche di base, evidenziandone e discutendone le caratteristiche peculiari;
- Specifiche di base – Definizione del processo di gestione degli incidenti di sicurezza informatica: documento che suggerisce un modello per il processo di gestione degli incidenti e descrive la relazione tra le fasi del processo e le misure di sicurezza di base.

1.1.4 Ulteriori ambiti di intervento

Nel 2025, il legislatore ha ulteriormente consolidato la presenza dell'ACN in altri ambiti strategici. Ad esempio, con la legge n. 89/2025, l'Agenzia assume un ruolo di supporto qualificato nell'ambito del procedimento autorizzatorio per lo svolgimento di attività spaziali. In particolare, durante l'istruttoria condotta dal Comitato interministeriale per le politiche relative allo spazio e alla ricerca aerospaziale (COMINT), quest'ultimo può avvalersi del contributo di Amministrazioni e organismi non formalmente rappresentati al suo interno. Tra questi rientra espressamente l'ACN, chiamata a intervenire –

attraverso pareri, valutazioni e contributi tecnico-specialistici – ogniqualvolta l'attività spaziale oggetto di autorizzazione presenti aspetti di rilievo sotto il profilo della sicurezza cibernetica. In tal modo, l'ACN si afferma quale interlocutore significativo, contribuendo a garantire che le decisioni autorizzatorie tengano adeguatamente conto anche delle esigenze di cybersicurezza e di protezione degli interessi strategici dello Stato.

Inoltre, nell'ambito del Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026, l'Agenzia ha adottato le Linee guida CAD "Definizione dei processi e delle procedure per la gestione degli incidenti di sicurezza informatica" volte a fornire indicazioni alle Pubbliche Amministrazioni, ai gestori di servizi pubblici e alle società a controllo pubblico su come istituire e strutturare processi e procedure per la gestione degli incidenti cyber. Sempre nel solco del citato Piano triennale, sono stati forniti i contributi di competenza relativi al capitolo sulla sicurezza cibernetica per le Linee guida per l'adozione dell'intelligenza artificiale nella PA. L'Agenzia ha, inoltre, contribuito alle attività di normazione tecnica collaborando con UNINFO.

ACN e UNINFO

All'inizio del 2025 l'Agenzia ha avviato una proficua collaborazione con UNINFO, ente nazionale di normazione tecnica che opera nell'ambito delle tecnologie informatiche e delle loro applicazioni. L'ACN è stata, infatti, inclusa tra i soci di diritto, potendo così contribuire, per i profili di cybersicurezza, alla stesura delle norme tecniche, attraverso cui tradurre i principi della cybersicurezza in criteri operativi e verificabili.

In particolare, l'Agenzia è direttamente coinvolta con propri esperti nelle seguenti Commissioni tecniche e nei relativi gruppi di normazione nazionali e internazionali:

- Commissione UNI/CT 533 Intelligenza Artificiale - AI;
- Commissione UNI/CT 535 *Quantum technologies*;
- Commissione UNI/CT 510 Sicurezza - *Security*;
- Commissione UNI/CT 526 Attività professionali non regolamentate - Figure professionali operanti nel settore ICT.

Nell'ottica di assicurare un quadro giuridico nazionale aggiornato e coerente in materia di cybersicurezza, tenendo anche conto delle evoluzioni normative a livello UE, la legge di delegazione europea 2025 riconosce all'ACN, ancora una volta, un ruolo di primaria importanza rispetto all'attuazione di alcuni specifici regolamenti europei. Tra questi assume rilievo il Regolamento (UE) 2024/2847 *Cyber Resilience Act* (CRA), che introduce requisiti di cybersicurezza per i prodotti con elementi digitali e rispetto al quale la legge designa l'ACN sia come Autorità di notifica, sia come Autorità di vigilanza del mercato, con il compito di garantire che i prodotti con elementi digitali rispettino gli standard di sicurezza previsti a livello europeo. Vi è poi il Regolamento (UE) 2025/37, recante modifiche al *Cybersecurity Act* (CSA), che prevede l'estensione del sistema europeo di certificazione della cybersicurezza anche ai servizi di sicurezza gestiti, ossia quelli relativi alla gestione dei rischi di cybersicurezza (servizi di risposta agli incidenti, test di penetrazione, *audit* di sicurezza e consulenza) o alla fornitura di assistenza per tali attività; ciò si inserisce pienamente nel quadro delle competenze già attribuite all'Agenzia in qualità di Autorità nazionale di certificazione della cybersicurezza. Infine, il Regolamento (UE) 2025/38 *Cyber Solidarity Act* (CSoA) istituisce meccanismi per rafforzare la capacità collettiva dell'Unione in materia di rilevamento delle minacce e degli incidenti informatici, nonché di preparazione e risposta agli stessi; in tale contesto la legge di delegazione individua l'ACN quale polo informatico nazionale e prevede la sua partecipazione ai sistemi europei di allerta, emergenza e riserva per la cybersicurezza.

1.2 PRINCIPALI NOVITÀ NORMATIVE IN AMBITO UE

Nel corso del 2025, l'ACN ha contribuito attivamente ai processi di definizione delle posizioni negoziali nazionali con riguardo a dossier di rilevanza strategica a livello UE, anche in raccordo con le altre Amministrazioni competenti. Questi hanno riguardato, principalmente, le proposte di Regolamento:

- *EU Space Act* (EUSA), per definire una regolamentazione armonizzata delle attività spaziali UE;
- Omnibus Digitale su cybersicurezza, *privacy* e dati, che modifica la Direttiva NIS2 e il Regolamento generale sulla protezione dei dati (GDPR), oltre a razionalizzare l'*acquis* UE in materia di dati;
- Omnibus Digitale sull'IA, il quale prevede, tra le altre cose, il rinvio dell'entrata in vigore di alcuni obblighi dell'*AI Act*;
- istituzione del Fondo europeo per la competitività (ECF), volto a far fronte alle criticità strutturali che ostacolano la capacità dell'UE di competere a livello globale in diversi settori, incluso quello della cybersicurezza.

EU Space Act

L'*EU Space Act*, presentato a giugno, mira a istituire un quadro normativo armonizzato per le attività spaziali all'interno dell'UE, che garantisca sicurezza, resilienza e sostenibilità ambientale, nonché rafforzi la competitività del settore. L'iniziativa nasce dall'esigenza di superare l'attuale frammentazione normativa comunitaria, che genera complessità e costi aggiuntivi per le imprese. Attraverso l'EUSA, infatti, si intende creare un mercato unico delle attività spaziali, facilitando in particolare la crescita e l'operatività transfrontaliera di *startup* e piccole e medie imprese (PMI). La proposta si fonda su tre ambiti principali di intervento: la sicurezza, mediante l'introduzione di regole rigorose per il tracciamento degli oggetti spaziali, al fine di preservare un accesso sicuro e continuo allo spazio; la resilienza, rafforzata attraverso requisiti mirati in materia di cybersicurezza destinati a proteggere le infrastrutture spaziali europee e a garantire la continuità operativa; la sostenibilità, che impone agli operatori di valutare e ridurre l'impatto ambientale delle proprie attività, prevedendo al contempo misure di sostegno all'innovazione in tecnologie emergenti.

Nell'ambito dei negoziati del Regolamento EUSA, l'Agenzia ha contribuito all'azione della *task force*, istituita presso la Segreteria del COMINT, per la definizione di una posizione comune nazionale e per assicurare la coerenza con le normative di settore italiane. In ragione della connotazione dell'EUSA quale *lex specialis* rispetto alla direttiva NIS2, con il potenziale rischio di sovrapposizioni e duplicazioni – sia per quanto riguarda la definizione e l'applicazione degli obblighi, sia con riferimento al regime di vigilanza, monitoraggio, esecuzione, ispettivo e sanzionatorio – l'ACN è intervenuta, in particolare, per circoscrivere gli eventuali oneri aggiuntivi sulle imprese rispetto a quelli derivanti dalla direttiva NIS2.

Omnibus Digitale e Omnibus Digitale sull'IA

Le proposte, presentate a novembre, fanno parte del Pacchetto Digitale, intervento per semplificare la normativa in ambito digitale e rafforzare la competitività dell'Unione, in linea con le priorità politiche della Commissione europea e con le raccomandazioni dei rapporti Draghi e Letta. Queste prevedono, rispettivamente, modifiche alla Direttiva NIS2 e all'*AI Act* per conseguire risparmi significativi per le imprese entro il 2029.

In relazione agli aspetti di cybersicurezza dell'Omnibus Digitale, la proposta introduce un punto di accesso unico (*Single Entry Point*), gestito dall'Agenzia dell'UE per la cybersicurezza (ENISA), per la segnalazione degli incidenti. In tal modo, le imprese assolverebbero contemporaneamente agli obblighi di notifica previsti da 5 discipline europee (NIS2, CER, eIDAS, DORA e GDPR). Tale meccanismo mira a ridurre la duplicazione degli adempimenti, con benefici attesi soprattutto per le piccole e medie imprese, consentendo di assolvere a tutti i regimi di notifica applicabili a un singolo incidente attraverso un'unica comunicazione.

Quanto alla seconda proposta, nell'ambito della progressiva attuazione del Regolamento europeo sull'intelligenza artificiale (*AI Act*), la Commissione europea ha rilevato alcune criticità legate, in particolare, ai ritardi nell'adozione degli standard armonizzati e al livello di

preparazione istituzionale degli Stati membri. In risposta a tali criticità, la proposta di Omnibus Digitale sull'IA mira, tra l'altro, a raccordare la tempistica di applicazione delle disposizioni relative ai sistemi di IA ad alto rischio alla disponibilità effettiva di standard tecnici e di strumenti di supporto, prevedendo una possibile estensione dei termini fino a 16 mesi. In tal modo, il termine per la piena efficacia e operatività dell'intero apparato regolatorio dell'*AI Act* sarebbe posticipato a dicembre 2028.

Nel negoziato dei due Omnibus, l'ACN ha assicurato il proprio contributo nell'ambito del coordinamento, effettuato a livello nazionale dal Dipartimento per gli affari europei della Presidenza del Consiglio dei ministri, ai fini della successiva discussione in seno al Consiglio dell'UE dedicato alla semplificazione (Gruppo Antici).

Regolamento sull'istituzione dell'ECF

La proposta, inserita nel quadro finanziario pluriennale 2028-2034, si ispira alle raccomandazioni dei rapporti Draghi e Letta e alla strategia *Competitiveness Compass* del 2025 della Commissione. La novità principale è la proposta di unificazione di 14 programmi di finanziamento, con regole semplificate e strumenti finanziari diversificati (inclusi *Horizon Europe* e *Digital Europe Programme*, ma anche *European Defence Fund*).

L'ECF avrà una dotazione di circa 409 miliardi di euro, pari al 22% del bilancio complessivo dell'UE per il periodo, con una parte significativa destinata alla ricerca e all'innovazione. Il Fondo si articola in quattro diverse aree tematiche: transizione pulita e decarbonizzazione industriale; resilienza, sicurezza, difesa industriale e spazio; leadership digitale; salute, biotecnologie, agricoltura e bioeconomia. Tra le altre cose, la proposta – oltre a rafforzare la sovranità digitale e la sicurezza delle catene di valore, a investire in tecnologie chiave e a promuovere innovazione e competitività – punta a potenziare la cybersicurezza e ridurre dipendenze da fornitori extra-UE.

Consultazioni pubbliche

L'ACN ha, inoltre, fornito il proprio apporto riguardo a proposte ancora in via di definizione da parte della Commissione europea, nell'ambito delle consultazioni pubbliche relative alla revisione del *Cybersecurity Act*, alla proposta di Regolamento *Cloud and AI Development Act* (CADA) e allo Scudo europeo per la democrazia (*European Democracy Shield*).

Quanto alla revisione del CSA, a 5 anni dall'adozione del Regolamento, la proposta si concentra sul mandato di ENISA, sul quadro europeo di certificazione della sicurezza informatica e sulle sfide legate alla sicurezza della catena di approvvigionamento ICT. Essa rappresenta anche un'opportunità per semplificare le norme sulla sicurezza informatica snellendo gli obblighi di segnalazione degli incidenti, nonché facilitarne l'attuazione riducendo la burocrazia a favore delle imprese.

La proposta di Regolamento CADA mira a colmare il crescente divario tra le esigenze di sviluppo dell'IA e la sua capacità di calcolo, ponendosi tre principali obiettivi: promuovere l'innovazione nel trattamento dei dati e nelle infrastrutture in modo sostenibile ed efficiente nell'uso delle risorse; triplicare la capacità dei *data center* dell'UE in 5-7 anni, allentando le barriere agli investimenti e supportando progetti sostenibili; garantire servizi *cloud* sicuri basati nell'UE per casi d'uso critici, promuovendo la sovranità e la competitività.

Lo *European Democracy Shield* ha l'obiettivo di contrastare attività di interferenza e disinformazione e di rafforzare i valori democratici e i diritti fondamentali all'interno dell'Unione, anche attraverso il sostegno a media liberi e la promozione della partecipazione civica e dell'educazione alla cittadinanza.

2

La minaccia cyber

Nel 2025 si è osservata una crescita importante del numero di eventi malevoli nel cyberspazio, alla quale non ha corrisposto un incremento altrettanto marcato degli incidenti con impatti confermati ai danni di operatori e Pubbliche Amministrazioni.

Tale distinzione tra eventi, incidenti e impatti risulta essenziale per una corretta lettura dei dati, consentendo di separare il volume delle attività osservate dall'Agenzia per la cybersicurezza nazionale dalle conseguenze effettivamente prodotte.

L'aumento di tali indicatori è riconducibile a diversi fattori, tra i quali la sempre crescente capacità del CSIRT Italia di rilevare le attività malevole e la complessità della situazione geopolitica globale, che ha riflessi anche nel dominio cibernetico. In tale quadro, gioca un ruolo significativo il progressivo ampliamento degli obblighi di notifica che consentono una maggiore visibilità sulla minaccia cyber, in particolare la piena applicazione delle previsioni della legge n. 90/2024. D'altro canto, l'aumento degli incidenti in misura minore rispetto a quello degli eventi è attribuibile a una maggiore efficacia delle attività del CSIRT Italia di allertamento generale e puntuale a favore delle potenziali vittime, supportate con l'indicazione di misure di contenimento utili a mitigare le più diffuse minacce. In aggiunta, si registra un progressivo miglioramento della capacità di difesa degli operatori che, essendo maggiormente consapevoli dei rischi, adottano appropriate misure di protezione cibernetica.

L'analisi delle tipologie di minacce cyber rilevate negli eventi evidenzia come l'incremento registrato sia da ricondurre principalmente all'intensificarsi delle campagne di attacchi DDoS condotte nei confronti di soggetti nazionali, nella quasi totalità dei casi prive di effetti significativi. Da segnalare, inoltre, l'aumento degli eventi di esposizione non autorizzata di dati precedentemente esfiltrati e il numero sempre maggiore di campagne di *phishing* e *spearphishing* rilevate, la cui diffusione e qualità risultano amplificate dall'impiego di strumenti basati sull'intelligenza artificiale.

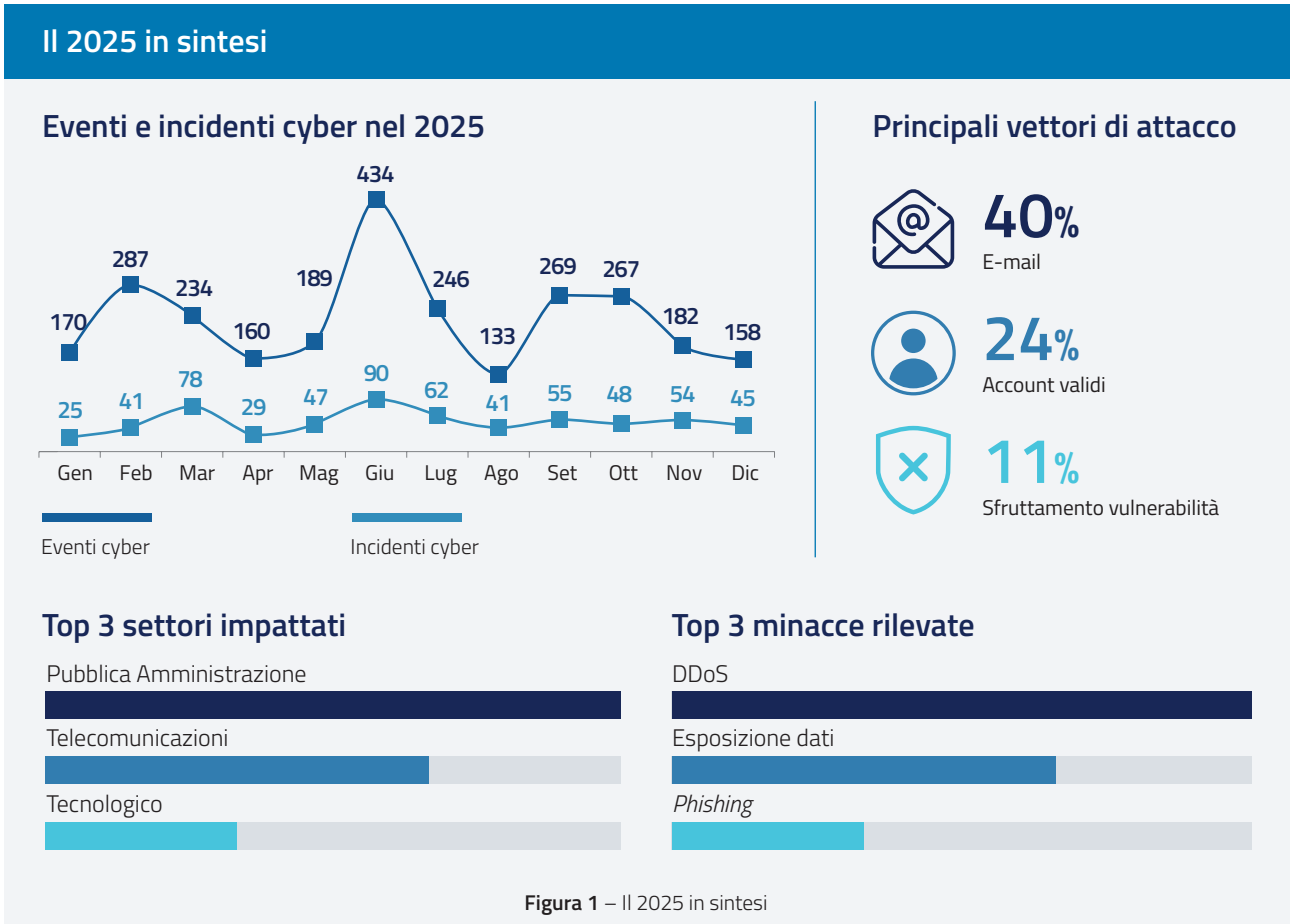


Figura 1 – Il 2025 in sintesi

2.1 I NUMERI DEL CSIRT ITALIA

Il CSIRT Italia ha registrato anche nel 2025 un aumento di tutti gli indicatori riferiti alle attività operative di allertamento e monitoraggio, nonché degli interventi di supporto diretto alle vittime. I dati illustrati nel prosieguo rappresentano le informazioni consolidate all'esito delle numerose attività di approfondimento e analisi che i tecnici del CSIRT Italia effettuano sulle notifiche di incidente e sugli altri avvenimenti di interesse.

Nel dettaglio, l'incremento degli eventi cyber è stato di circa il 38% rispetto al 2024, a fronte di un aumento più contenuto degli incidenti, pari a circa il 7%. Tale andamento conferma una dinamica di crescita del volume complessivo delle attività osservate che, tuttavia, non si è tradotta in un incremento proporzionale degli incidenti. Sono aumentate di oltre il 50% le vittime univoche, ovvero i soggetti che hanno subito almeno un evento cyber gestito dal CSIRT Italia; rileva segnalare che le vittime complessive sono state 3.907, a dimostrazione della frequente reiterazione degli attacchi contro determinati settori o soggetti.

Attività e numeri del CSIRT Italia 2025

Gestione eventi

- **2.729 eventi cyber** (227 al mese)
- **615 incidenti cyber** con impatto confermato (51 al mese)
- **3.907 vittime**, di cui univoche 1.901
- **661 notifiche di incidente**
- **12.202 comunicazioni ricevute**
- **55 interventi a supporto diretto**

Allertamento

- **46.867 comunicazioni** inviate ai soggetti (3.905 al mese)
- **738 *alert* e bollettini** pubblicati sul **portale pubblico**
- **804 *alert* e bollettini** pubblicati sul **Portale servizi**
- **767 stime di impatto di nuove vulnerabilità**
- **5.853 segnalazioni** puntuali **di vulnerabilità** ex legge n. 90/2024
- **800.000+ indicatori di compromissione condivisi**

Monitoraggio sistemi italiani

- **31.050 dispositivi e servizi a rischio** segnalati ai soggetti
- **10.312 dispositivi e servizi potenzialmente compromessi** segnalati ai soggetti
- **2.457 tentativi di *phishing*** segnalati alle vittime

Monitoraggio attori cyber

- **126 attori *ransomware*** monitorati
- **191 attori hacktivisti** monitorati

Analisi minacce

- **25 campagne APT**
- **126 malware analizzati**

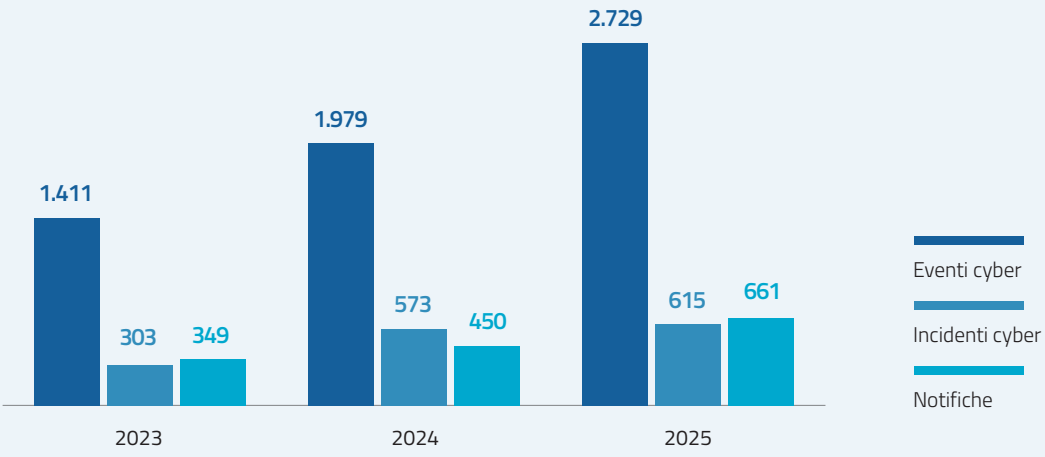


Figura 2 – Attività e numeri del CSIRT Italia 2025

In particolare, il disallineamento tra l'incremento degli eventi e quello degli incidenti è riconducibile all'attività di allertamento preventivo, che ha consentito di mitigare in modo significativo le potenziali conseguenze degli eventi rilevati. Il CSIRT Italia svolge attività di allertamento sia attraverso comunicazioni dirette finalizzate a segnalare potenziali compromissioni o fattori di rischio ai soggetti monitorati, sia tramite i canali di diffusione pubblica. Al riguardo, un incremento rilevante si è registrato per *alert* e bollettini che sono stati diffusi sul portale pubblico (da 587 nel 2024 a 738 nel 2025) e sul Portale servizi ad accesso riservato (passati da 64 a 804). Sono cresciuti notevolmente anche gli indicatori di compromissione che l'ACN ha potuto condividere tramite apposite piattaforme (da oltre 125.000 a più di 800.000).

Rilevante è stato, inoltre, l'impegno per contribuire preventivamente alla mitigazione di vulnerabilità: l'ACN ha condiviso oltre 5.800 segnalazioni puntuali di specifiche vulnerabilità, come previsto dalla legge n. 90/2024, attività con cui i soggetti potenzialmente esposti sono stati informati dei rischi e supportati tramite l'indicazione di interventi risolutivi.

Il forte incremento di tutti gli indicatori relativi al monitoraggio è riconducibile, oltre che all'aumento delle attività di gestione degli eventi e della quantità e qualità delle fonti a disposizione del CSIRT Italia, all'intensificarsi dell'*infosharing* internazionale, che hanno consentito di acquisire e diffondere un volume maggiore di evidenze tecniche rilevanti.

Nell'ambito della risposta agli incidenti cyber, sono cresciute le attività di supporto diretto alle vittime finalizzate al contenimento degli stessi, alla mitigazione degli impatti e al ripristino delle condizioni operative. Tali interventi sono, infatti, passati da 40 nel 2024 a 55 del 2025.

Definizioni

Notifica di incidente
Comunicazione ricevuta dai soggetti che a ciò sono tenuti in osservanza delle disposizioni vigenti.

Comunicazione ricevuta
E-mail ricevuta dal CSIRT Italia relativa a informazioni contenenti profili di natura cyber anche generiche, sottoposte a valutazione preliminare.

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.

Evento cyber
Un avvenimento d'interesse per il CSIRT Italia con potenziale impatto su almeno un soggetto nazionale.

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.

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 ad accesso riservato abilitato allo scambio di informazioni tecniche specifiche con i soggetti della *constituency* del CSIRT Italia.

Portale pubblico
Portale del CSIRT Italia sul sito istituzionale dell'ACN accessibile all'intera comunità.

2.2 ANALISI DEGLI EVENTI CYBER

Operational Summary

L'Agenzia per la cybersicurezza nazionale cura la redazione dell'*Operational Summary*, documento a cadenza mensile, cui si aggiungono due edizioni semestrali, finalizzato alla rilevazione e alla sistematizzazione delle principali fenomenologie cyber rilevate e gestite dal CSIRT Italia. L'*Operational Summary* si configura come un presidio informativo stabile a supporto dell'analisi dell'andamento della minaccia cibernetica. Le informazioni di natura operativa, derivanti dalle attività istituzionali dell'Agenzia, consentono la produzione di dati e indicatori relativi ai settori maggiormente impattati e alle tipologie di minaccia prevalenti.

Il documento è redatto in tre versioni: una a uso interno ACN, una a diffusione limitata, trasmessa ai soggetti più critici della *constituency* del CSIRT Italia, e una versione pubblica scaricabile dal sito web dell'ACN.

Nel corso del 2025, il CSIRT Italia ha trattato un totale di 2.729 eventi cibernetici, con una media mensile di circa 227 eventi (in crescita rispetto ai 165 del 2024) e un picco massimo di 434 nel mese di giugno. Di questi, 615 sono stati classificati come incidenti, con una media mensile di circa 51 incidenti, in crescita rispetto ai 48 dell'anno precedente (Figura 3).

I picchi rilevati nei mesi di febbraio, giugno, settembre e ottobre sono riconducibili a 4 distinte campagne di attacchi DDoS rivendicate da diversi gruppi hacktivisti che si collocano nel contesto del conflitto russo ucraino e, più in generale, nelle dinamiche del quadro geopolitico internazionale. Dalla figura si evince come tali picchi non abbiano comportato un corrispondente incremento degli incidenti.

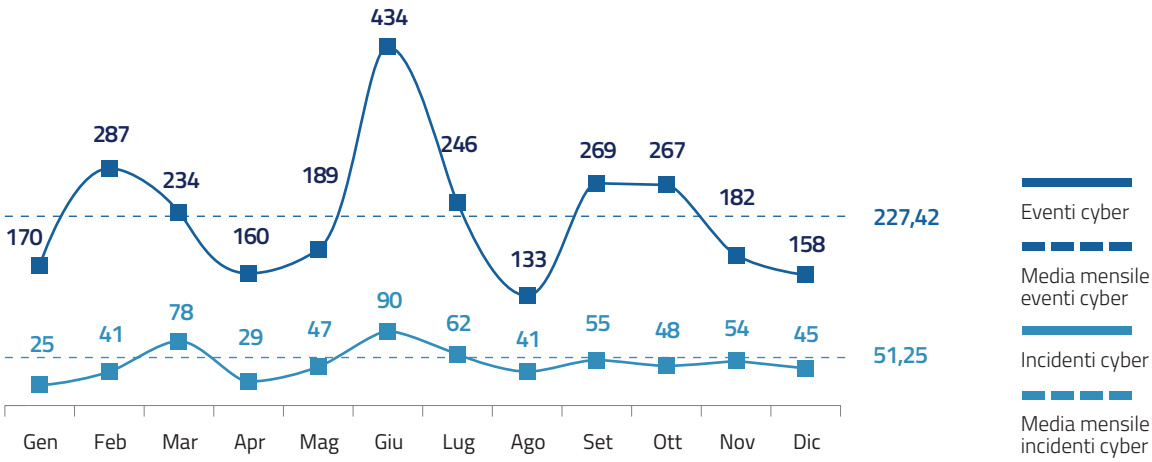


Figura 3 – Distribuzione temporale degli eventi e incidenti cyber nel 2025

A fronte dell'andamento complessivo degli eventi rilevati, l'analisi delle tipologie di impatto consente di qualificare in modo più puntuale le conseguenze effettivamente prodotte dalle attività cibernetiche osservate nel periodo di riferimento. Come rappresentato in Figura 4, gli impatti rilevati hanno interessato prevalentemente la riservatezza e/o l'integrità dei dati e la disponibilità dei dati, che complessivamente rappresentano oltre il 60% del totale.

Accanto a tali dinamiche, assumono rilievo anche le compromissioni di account, che rappresentano una quota significativa degli impatti osservati e costituiscono spesso un fattore abilitante per successive attività malevole. Ulteriori tipologie di impatto includono la compromissione di sistemi e applicazioni, nonché eventi di esposizione, esfiltrazione e manipolazione di dati, con effetti diretti sulla riservatezza, sull'integrità e sulla disponibilità delle informazioni.

Nel complesso, la distribuzione delle tipologie di impatto rilevate nell'ambito degli incidenti restituisce un quadro eterogeneo, caratterizzato sia da effetti immediati sulla disponibilità dei servizi, sia da impatti più strutturali derivanti da accessi non autorizzati a sistemi, account e dati, confermando la varietà delle conseguenze associate agli eventi cibernetici.

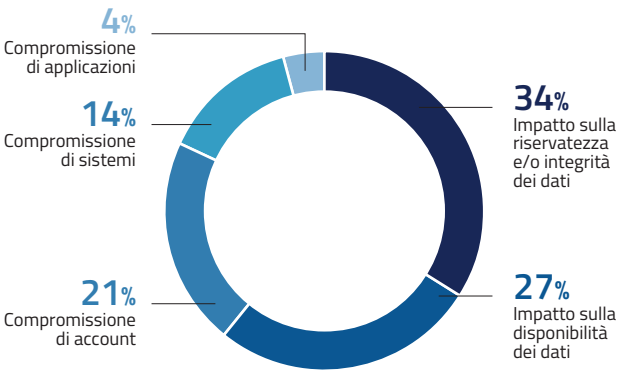


Figura 4 – Tipologia di impatto rilevato negli incidenti

Le tipologie di impatto

Compromissione di sistemi

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.

Compromissione di account

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.

Compromissione di applicazioni

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.

Impatto sui dati

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.

A completamento dell'analisi delle tipologie di impatto, l'esame dei vettori di accesso consente di individuare le modalità attraverso le quali le attività ostili si concretizzano, permettendo agli attori malevoli di ottenere un accesso iniziale a sistemi, account o applicazioni.

Come illustrato in Figura 5, i vettori di attacco rilevati nel periodo di riferimento evidenziano una netta prevalenza di modalità che sfruttano l'interazione con l'utente e l'impiego di account validi, confermando il ruolo centrale del fattore umano e della gestione degli accessi nei processi di compromissione.

Ciò riflette anche il sempre più diffuso impiego di strumenti basati sull'intelligenza artificiale che consentono di generare messaggi di *phishing* altamente credibili, aumentando la probabilità di successo degli attacchi. Rileva come tali tipologie di vettore siano significativamente superiori in numero rispetto allo sfruttamento di vulnerabilità, categoria questa influenzata anche dalla prontezza dei soggetti nel sanare le nuove criticità rilevate e segnalate puntualmente dall'ACN.

Nel complesso, la distribuzione dei vettori di attacco restituisce un quadro in cui le tecniche di intrusione più ricorrenti non si fondano esclusivamente su strumenti sofisticati, ma su combinazioni di ingegneria sociale, abuso di funzionalità legittime e carenze nelle misure di protezione di base. Tale evidenza conferma l'importanza delle attività di prevenzione e mitigazione volte a ridurre l'esposizione ai rischi, prevenire accessi non autorizzati e contenere l'impatto di eventuali intrusioni.

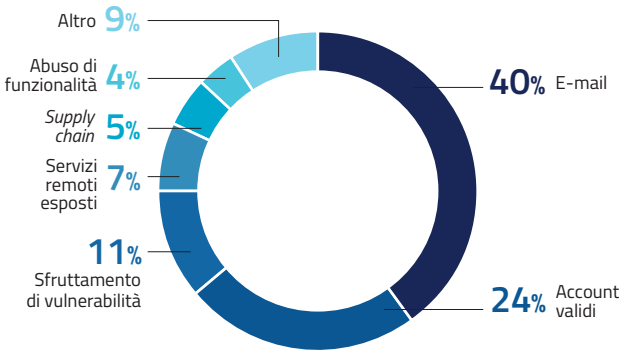


Figura 5 – Distribuzione dei principali vettori di attacco

Principali vettori di attacco

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

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

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.

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

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.

Abuso di funzionalità
Utilizzo improprio di funzionalità applicative legittime, secondo modalità non previste dal loro scopo originario, al fine di ottenere effetti non autorizzati o causare un impatto negativo su dati, sistemi o servizi.

Dall'analisi e dalla successiva classificazione dei 2.729 eventi cibernetici rilevati è stato possibile individuare le principali tipologie di minaccia, come riportato in Figura 6. Dal punto di vista quantitativo, emerge la minaccia DDoS quale tipologia prevalente, seguita dall'esposizione non autorizzata dei dati e dalle campagne di *phishing*.

Si segnala che le tipologie di minaccia non sono da intendersi come categorie rigide e separate, in quanto un singolo evento può essere associato a più minacce. A titolo esemplificativo, un evento categorizzato come *phishing* può essere finalizzato alla diffusione di malware, che a sua volta può evolvere in un incidente di tipo *ransomware*.

Dal confronto tra la distribuzione delle tipologie di eventi e quella delle tipologie di incidenti (Figura 6) emerge in modo chiaro come solo una parte degli eventi rilevati si traduca in incidenti con impatti effettivi. In termini di eventi, risultano preponderanti le attività di tipo DDoS, le esposizioni di dati e le campagne di *phishing*, mentre la distribuzione degli incidenti mostra una configurazione parzialmente diversa, con una maggiore incidenza delle compromissioni da malware, delle esposizioni di dati, del *ransomware* e delle compromissioni di caselle di posta elettronica, tipologie che più frequentemente determinano effetti concreti sui sistemi, sui dati e sulla continuità operativa.

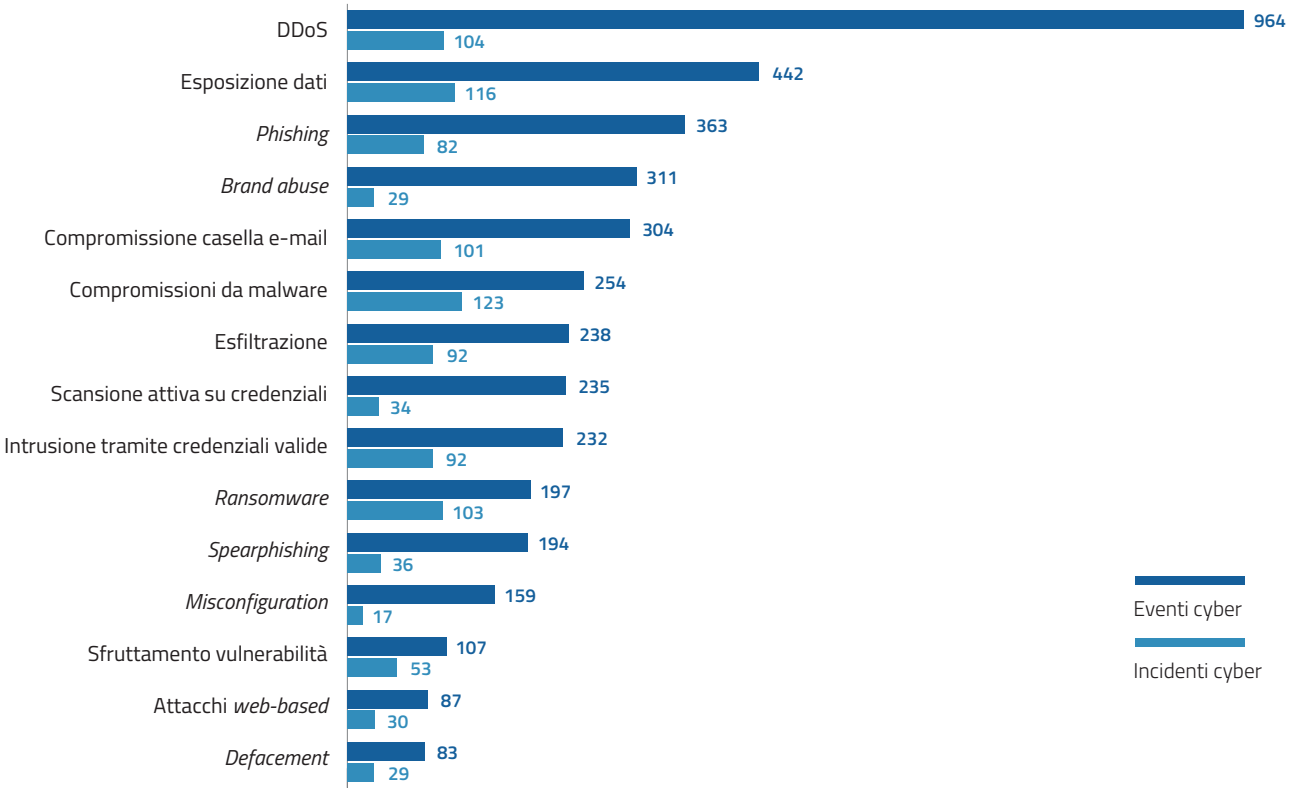


Figura 6 – Minacce rilevate negli eventi e negli incidenti cyber (top 15)

Per quanto attiene ai settori di attività delle vittime, emerge una prevalenza della Pubblica Amministrazione, sia a livello centrale che locale, seguita dal settore delle telecomunicazioni, come illustrato in Figura 7. Nella lettura dei dati deve essere considerato che, alla luce della *mission* istituzionale attribuitale, l'ACN dispone di una maggiore capacità di osservazione nei confronti della Pubblica Amministrazione e dei settori critici individuati dalla normativa vigente.

Ai fini di una corretta interpretazione del dato, è opportuno, altresì, evidenziare che un singolo evento può coinvolgere più vittime, ciascuna delle quali può operare in uno o più settori di attività, con conseguente possibile sovrapposizione nelle classificazioni settoriali.

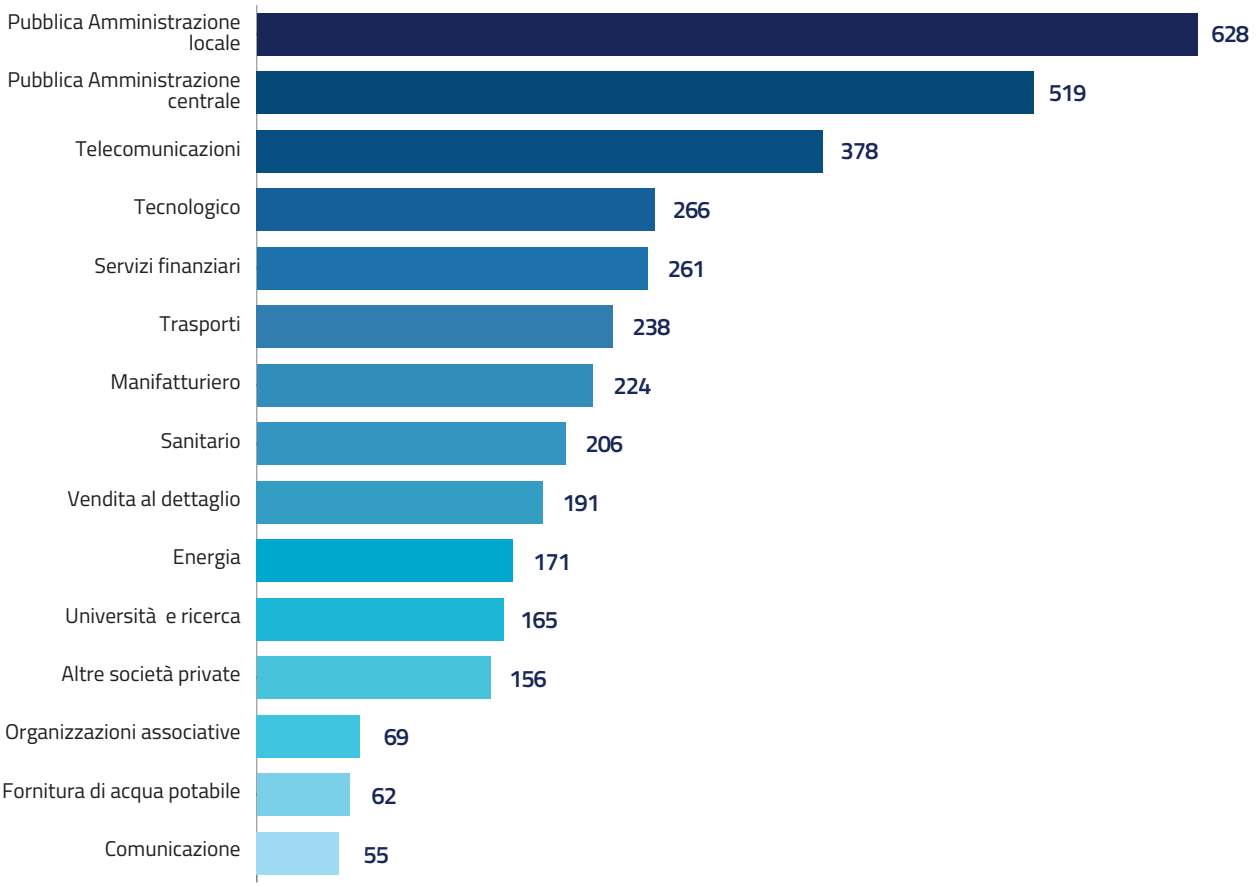


Figura 7 – Vittime di eventi cyber per settore (top 15)

2.3 IL QUADRO DELLA MINACCIA CYBER

Nel corso del 2025, è emerso un quadro complesso delle attività malevole osservate nel dominio cyber nazionale, caratterizzato dalla compresenza di minacce ampiamente diffuse con impatti limitati e di altre meno ricorrenti, ma associate a impatti più rilevanti.

Come già evidenziato, le campagne di attacchi DDoS hanno rappresentato una componente rilevante del quadro della minaccia, incidendo in misura significativa sul volume complessivo delle attività osservate e gestite dagli operatori del CSIRT Italia e dai soggetti interessati. Tali campagne risultano frequentemente riconducibili a dinamiche di hacktivismo, particolarmente quello filorusso molto attivo nell'ambito del conflitto in Ucraina. Le stesse hanno interessato una pluralità di settori (Figura 8), in particolare la Pubblica Amministrazione, i trasporti e le telecomunicazioni, e hanno spesso assunto un'incidenza ciclica e coordinata; nella quasi totalità dei casi, tuttavia, gli impatti sono stati irrilevanti, anche grazie alle azioni di mitigazione adottate dai soggetti colpiti e al coordinamento informativo e operativo attuato con gli stessi dall'Agenzia. In tale contesto, si rileva come la quota di attacchi DDoS che ha prodotto impatti misurabili sia ulteriormente diminuita, passando da circa il 15% nel 2024 a meno dell'11% nel 2025, a conferma di una capacità complessivamente più efficace di contenimento degli effetti sui servizi.

DDoS

Nel 2025 è stato pubblicato il rapporto sulla minaccia DDoS, con l'obiettivo di illustrare le diverse tipologie di attacchi DDoS, le tecniche e le tattiche adottate dagli attaccanti, nonché fornire raccomandazioni e contromisure. Il rapporto presenta, inoltre, un modello semplificato di riferimento, utile per identificare gli *asset* più esposti e orientare, con maggiore precisione, le strategie di mitigazione.
Un attacco DDoS può colpire qualsiasi infrastruttura connessa a Internet, compromettendo la disponibilità dei servizi e causando interruzioni con ripercussioni su utenti e operazioni aziendali. Oltre alle perdite economiche derivanti dall'inaccessibilità a risorse critiche, le vittime possono subire danni reputazionali. L'impatto può estendersi alla produttività e alla continuità operativa, rendendo essenziale l'adozione di strategie di prevenzione e mitigazione per garantire la resilienza dell'infrastruttura.

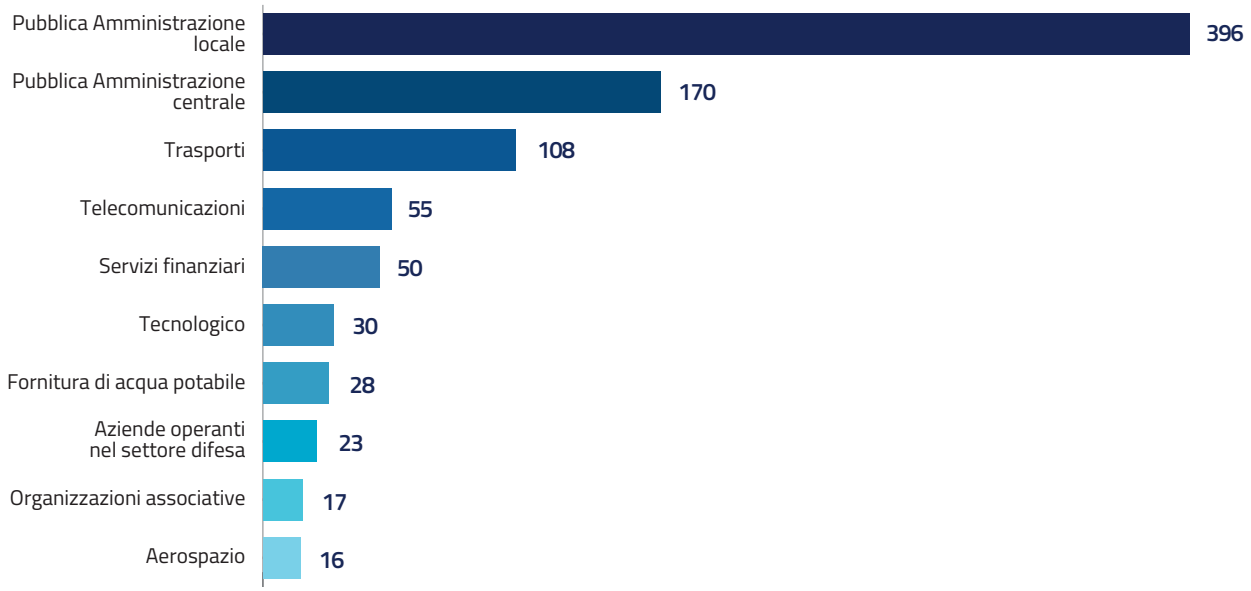


Figura 8 – Numero di eventi DDoS per settore di attività della vittima (top 10)

Parallelamente, i fenomeni di esposizione di dati hanno assunto un peso crescente nel quadro della minaccia. Tali eventi sono stati rilevati nell'ambito di attività di monitoraggio delle principali piattaforme di scambio illecito di dati dove avviene la pubblicazione e la commercializzazione di informazioni e di credenziali compromesse. In più circostanze, le esposizioni di dati hanno rappresentato il primo passo per successive attività malevole, quali, ad esempio, intrusioni, esfiltrazioni e *ransomware*. In altri casi, l'allertamento dell'ACN ha permesso di ridurre il tempo di esposizione alla minaccia attraverso una tempestiva disattivazione delle credenziali compromesse da parte dei soggetti, a detrimento della possibilità degli attaccanti di sfruttarle in tempo utile.

Il *phishing* si è confermato una minaccia ricorrente che abilita in maniera trasversale diverse modalità attacco, dal momento che frequentemente è orientata all'acquisizione non autorizzata di credenziali di accesso come quelle per servizi *cloud* e sistemi informativi. Le campagne osservate hanno interessato in modo particolare settori caratterizzati da un'elevata esposizione digitale e, in numerosi casi, hanno costituito un vettore iniziale per ulteriori compromissioni, inclusa la diffusione di malware e l'accesso non autorizzato a risorse informatiche.

Meno diffusa, ma particolarmente critica sotto il profilo degli impatti, si è confermata la minaccia *ransomware* che comporta la compromissione dell'operatività dei servizi ICT della vittima. Le evidenze indicano come la maggior parte delle vittime sia rappresentata da piccole imprese, in particolare del settore manifatturiero, spesso caratterizzate da livelli di cybersicurezza limitati, mentre il numero di soggetti critici coinvolti risulta complessivamente contenuto (Figura 9). Gli attacchi *ransomware* hanno determinato, in diversi casi, indisponibilità prolungate di dati e servizi, incidendo sulla continuità operativa delle vittime e risultando spesso abilitati dall'utilizzo di credenziali valide precedentemente compromesse, dallo sfruttamento di vulnerabilità non sanate e dall'esposizione di servizi di accesso remoto non adeguatamente protetti.

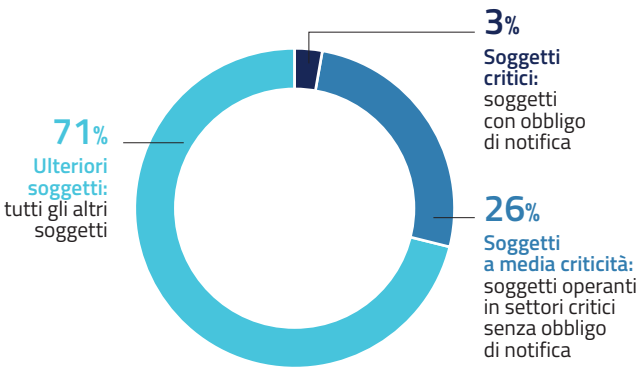


Figura 9 – Distribuzione delle vittime di *ransomware* in base alla loro criticità

In parallelo alle dinamiche riconducibili alle principali tipologie di minaccia fin qui descritte, il quadro osservato include attività che si distinguono non tanto per le modalità di attacco, quanto per il profilo degli attori coinvolti e per le logiche operative adottate. Si tratta di operazioni condotte da soggetti strutturati, caratterizzate da un elevato grado di pianificazione, da una persistenza nel tempo e da una marcata capacità di adattamento al contesto della vittima. Rientrano in questa categoria le minacce avanzate e persistenti (*Advanced Persistent Threat*-APT), che presentano caratteristiche specifiche e richiedono un'analisi dedicata.

Al riguardo, anche nel corso del 2025 sono state riscontrate attività ostili, con buona probabilità ascrivibili ad attori APT. Le analisi di natura tecnica su determinati eventi e incidenti cyber hanno, infatti, portato a evidenziare delle similitudini con attività pubblicamente attribuite da report tecnici a gruppi noti, come APT29, Lazarus Group, LightBasin, Salt Typhoon, Mustang Panda, Antique Typhoon (Storm-0558), UNC5221 e UNC1549. Tali attività hanno interessato, in particolare, diversi soggetti, pubblici e privati, afferenti al settore governativo nazionale e locale, manifatturiero, della sanità, tecnologico, delle telecomunicazioni, dei trasporti, dell'istruzione e aerospaziale.

Si è potuto appurare che tali attori sono riusciti a compromettere reti e sistemi principalmente attraverso lo sfruttamento di vulnerabilità su applicativi pubblicamente esposti, ma anche tramite l'utilizzo di e-mail di *spearphishing* e di account validi. Sono stati, inoltre, rilevati tentativi di infezione non andati a buon fine, condotti tramite campagne di *spearphishing* avanzato e attività di *bruteforcing*.

In alcuni dei casi analizzati sono stati osservati malware non pubblicamente documentati e altamente sofisticati, alcuni dei quali creati appositamente per la realtà *target*, con la finalità di esfiltrazione di informazioni o di controllo remoto. Di particolare rilievo risulta l'impiego di infrastrutture lecite come servizi di archiviazione *cloud,* oltre che 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.

Per aggirare i controlli di sicurezza e nascondere le proprie attività, è emersa una tendenza crescente da parte degli attori ostili a sfruttare piattaforme di condivisione del codice e servizi *cloud* legittimi. Questi strumenti, nati per facilitare la collaborazione, vengono utilizzati per diffondere software malevoli e come canali per impartire comandi o sottrarre informazioni. Parallelamente, l'analisi degli incidenti ha evidenziato come gli attori ostili mirino a mantenere una presenza stabile e duratura all'interno delle reti compromesse. A tal fine adottano molteplici modalità, tra cui l'installazione di servizi di accesso remoto, l'inserimento di componenti nascosti nei portali esposti in rete e l'uso di software obsoleti o non adeguatamente gestiti come punto d'ingresso per controllare nel tempo i sistemi compromessi.

In tutti i casi rilevati, l'ACN ha operato al fine di procedere al ripristino delle condizioni di sicurezza dei soggetti interessati.

2.4 MONITORAGGIO PROATTIVO E ANTICIPAZIONE DELLA MINACCIA

L'Agenzia svolge anche attività di monitoraggio proattivo orientate all'individuazione di vulnerabilità, configurazioni insicure, *asset* esposti e segnali di compromissione, che possono costituire condizioni abilitanti per azioni ostili o risultare già oggetto di sfruttamento. Ciò consente l'adozione di interventi preventivi prima che tali condizioni evolvano in incidenti.

Il monitoraggio proattivo si fonda sull'osservazione sistematica degli *asset* esposti su Internet e sull'analisi integrata di informazioni tecniche provenienti da più fonti. Attraverso tali attività, il CSIRT Italia dispone di una visione sempre aggiornata delle aree di esposizione più rilevanti e dei fattori di vulnerabilità emergenti, con particolare attenzione ai servizi critici e alle tecnologie caratterizzate da una maggiore accessibilità dalla rete pubblica. In tale quadro si inseriscono le attività svolte nell'ambito della cooperazione internazionale, attraverso lo scambio informativo con partner istituzionali esteri anche in relazione all'individuazione di infrastrutture malevole transnazionali.

Nel 2025 particolare attenzione è stata rivolta all'individuazione di dispositivi e servizi potenzialmente compromessi, inclusi sistemi utilizzati come parte di *botnet* o di infrastrutture di supporto ad attività DDoS, nonché apparati di rete e dispositivi *Internet of things* (IoT) esposti e sfruttati da attori malevoli. Tali attività hanno consentito di identificare tempestivamente i soggetti nazionali coinvolti e di attivare azioni di allertamento, contribuendo alla riduzione delle condizioni di esposizione e al contenimento di potenziali effetti a cascata.

FOCUS

Superfice esposta

La superficie esposta su Internet costituisce oggi uno dei principali parametri per la valutazione del rischio cibernetico. Essa comprende l'insieme delle risorse digitali che, essendo esposte in rete, sono più soggette a potenziali tentativi di sfruttamento da parte di attori ostili, nonché i vettori attraverso i quali un sistema può essere compromesso, manipolato o utilizzato come punto di partenza per ulteriori attività malevole. Nelle definizioni più consolidate, la superficie esposta è intesa come un perimetro in costante evoluzione, influenzato dall'introduzione di nuovi servizi digitali, dalla diffusione del cloud computing, dall'interconnessione dei dispositivi IoT e dall'ampliamento delle reti di connettività.

Il monitoraggio di questa superficie esposta rappresenta un processo sistematico e continuo volto a identificare e classificare asset, vulnerabilità e compromissioni, consentendo di adattare rapidamente la postura di sicurezza alle minacce emergenti e di ridurre la finestra di esposizione a vulnerabilità.

Nel corso del 2025 le attività di monitoraggio proattivo ha permesso al CSIRT Italia di segnalare ai soggetti della *constituency*:

- circa 2.457 indirizzi web di *phishing* ovvero pagine web artefatte, contenenti riferimenti espliciti o simili a pagine web di oltre 1.000 soggetti pubblici o privati, prontamente allertati, presumibilmente utilizzate per ingannare gli utenti e carpire credenziali;
- 10.312 dispositivi o servizi IT potenzialmente compromessi, ovvero per i quali è stato rilevato un comportamento associabile ad una attività malevola in corso. Relativamente a tali dispositivi o servizi sono state inviate 486 comunicazioni, di cui il 12% verso soggetti pubblici e l'88% verso soggetti privati;
- 31.050 dispositivi o servizi IT che esponevano potenziali rischi, come ad esempio versioni di software vulnerabili, per i quali sono state inviate 7.545 comunicazioni. Di queste il 28% verso soggetti pubblici e il 72% verso soggetti privati.

La Figura 10 rappresenta la distribuzione delle vulnerabilità identificate da codice CVE (*Common Vulnerabilities and Exposures*) rilevate per settore, articolata per livello di gravità (critica, alta, media) secondo la classificazione *Common Vulnerability Scoring System*-CVSS. Dall'analisi emerge una concentrazione significativa di vulnerabilità nei settori tecnologico e manifatturiero, che presentano non solo i valori assoluti più elevati, ma anche una quota rilevante di vulnerabilità a gravità alta e critica, indicando una superficie di esposizione particolarmente ampia e complessa per l'elevata numerosità di punti potenzialmente sfruttabili da un attore malevolo.

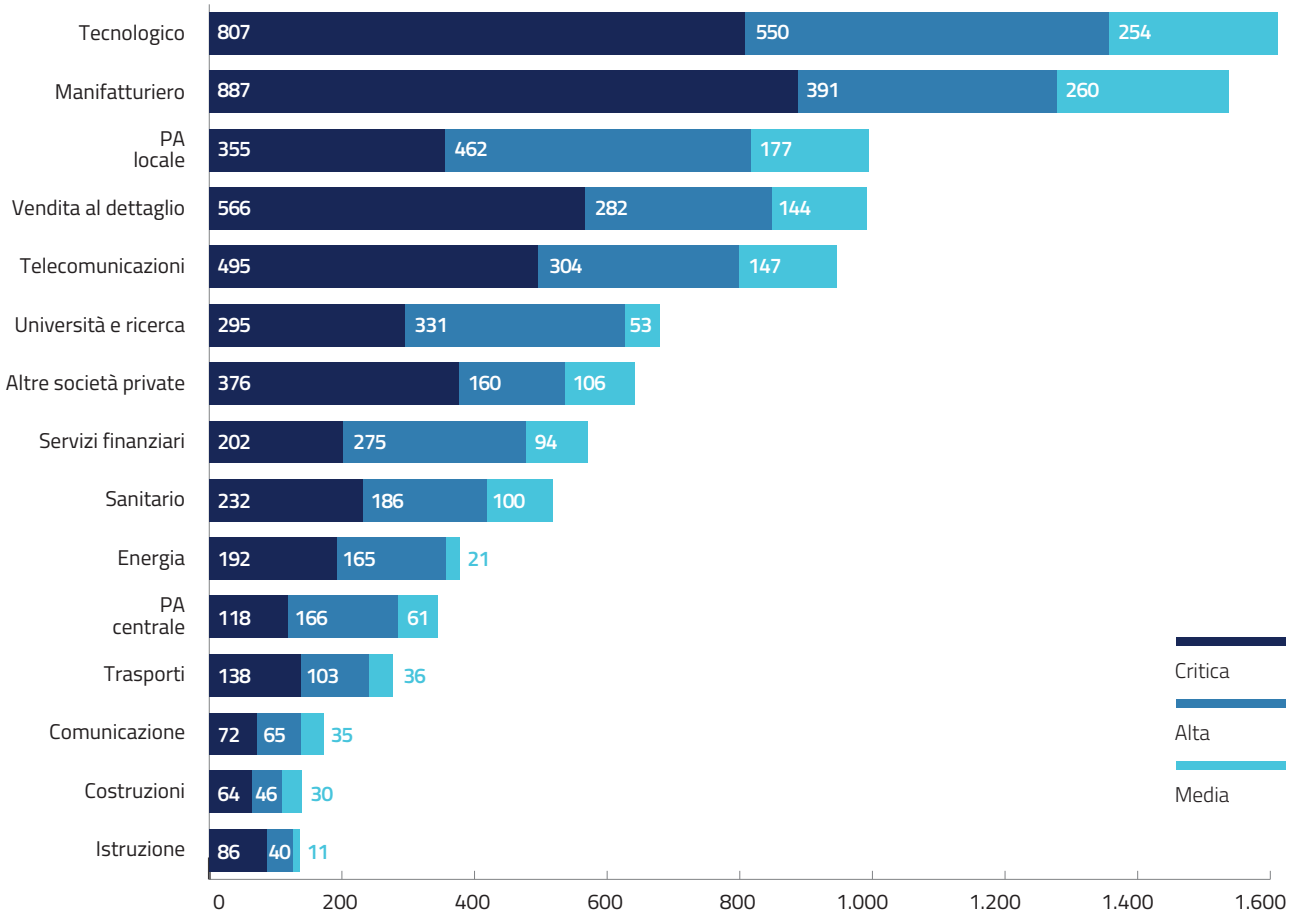


Figura 10 – Distribuzione delle vulnerabilità CVE per settore e livello di gravità (top 15)

Quanto ai servizi e dispositivi a rischio segnalati ai soggetti, la Figura 11 evidenzia la distribuzione delle vulnerabilità rilevate in funzione delle principali categorie tecnologiche interessate. I valori più elevati si riscontrano nei dispositivi di rete e nelle soluzioni di *firewall* e *proxy*, seguiti dai sistemi di *cybersecurity* e *data protection* e dalle tecnologie per il lavoro remoto. Ulteriori concentrazioni di vulnerabilità interessano le piattaforme di collaborazione, i servizi di posta elettronica, i protocolli di *file sharing* e le soluzioni di virtualizzazione.

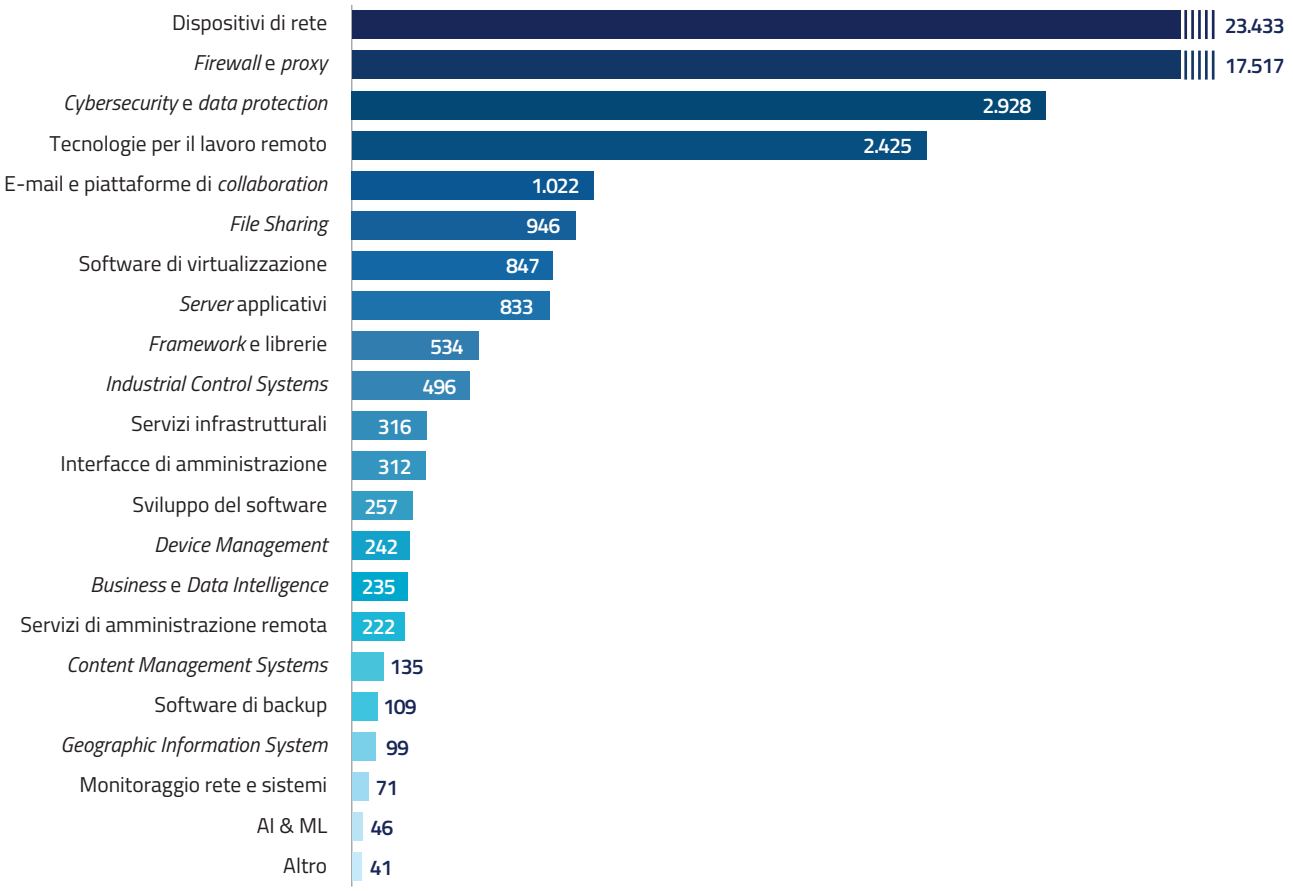


Figura 11 – Numero di dispositivi/servizi a rischio segnalati suddivisi per categoria

La distribuzione osservata riflette il ruolo centrale che tali tecnologie rivestono nell'architettura dei sistemi informativi, nonché la loro necessaria esposizione alla rete pubblica per garantire funzionalità di accesso, interconnessione e gestione dei servizi. In particolare, i dispositivi di rete e le soluzioni di sicurezza perimetrale (*firewall* e *proxy*) costituiscono elementi critici dell'infrastruttura, la cui compromissione può determinare effetti estesi su più sistemi e servizi a valle.

Analogamente, le tecnologie per il lavoro remoto e le piattaforme di collaborazione, ampiamente diffuse a seguito dei processi di digitalizzazione e di riorganizzazione del lavoro, presentano una superficie di esposizione intrinsecamente più ampia, in quanto progettate per essere accessibili dall'esterno. La presenza di vulnerabilità in tali ambiti non implica necessariamente uno sfruttamento in atto, ma individua condizioni strutturali di esposizione che richiedono particolare attenzione in termini di gestione degli aggiornamenti, configurazione sicura e controllo degli accessi.

2.5 INTERVENTI A SUPPORTO DELLE VITTIME DI INCIDENTE

Nei casi più complessi, l'Agenzia fornisce supporto diretto alle vittime di incidenti cibernetici attraverso i team di *Digital Forensic Incident Response* (DFIR) del CSIRT Italia. Tale attività si concretizza nell'affiancamento, anche per periodi prolungati, dei soggetti colpiti per contribuire alla gestione degli incidenti e dei relativi impatti mediante l'individuazione delle misure necessarie al contenimento e al ripristino dell'erogazione dei servizi compromessi.

Gli interventi si fondano sull'integrazione e sull'ottimizzazione delle risorse, in particolare tecnologiche, già presenti nelle infrastrutture coinvolte e seguono un approccio metodologico articolato in più fasi, che prevede una valutazione preliminare delle vulnerabilità, l'acquisizione e l'analisi degli artefatti digitali, la pianificazione delle attività di *remediation* e *recovery* e la verifica dell'attuazione delle misure correttive.

Durante il 2025 il personale tecnico è intervenuto a diretto supporto delle vittime in 55 diverse occasioni, principalmente a beneficio di soggetti della Pubblica Amministrazione centrale e locale, del settore tecnologico e di quello sanitario (Figura 12). L'aumento di tali interventi, che nel 2024 si erano fermati a 40, dimostra una maggiore maturità delle capacità di supporto dell'Agenzia, nonché un numero più elevato di incidenti per i quali si è reso necessario intervenire direttamente.

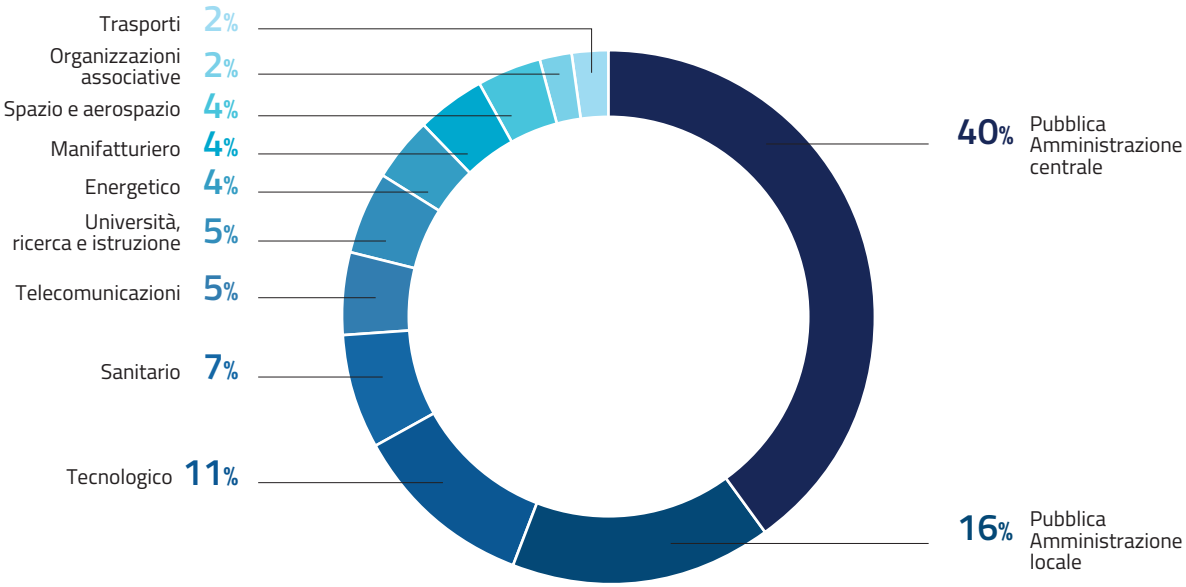


Figura 12 – Interventi a supporto delle vittime per settore

2.6 LA MINACCIA CYBER NELLA PUBBLICA AMMINISTRAZIONE

Nel corso del 2025, l'Agenzia ha rilevato 1.140 eventi cyber riferibili a istituzioni pubbliche nazionali. Di questi, 196 episodi, pari a circa il 17% del totale, sono stati qualificati come incidenti.

Il numero complessivo degli eventi risulta in aumento rispetto ai 756 casi registrati nel 2024 ed è attribuibile principalmente alle già citate campagne DDoS, nonché all'accresciuto cono di visibilità dell'ACN, dovuto anche alla piena applicazione della legge n. 90/2024 che ha esteso a moltissimi soggetti pubblici gli obblighi di notifica.

Come rappresentato in Figura 13, la distribuzione degli eventi cyber che hanno interessato la Pubblica Amministrazione evidenzia come la quota più rilevante abbia riguardato l'Amministrazione dello Stato e gli Organi costituzionali o di rilievo costituzionale. Tale concentrazione riflette il ruolo centrale di questi soggetti nell'assetto istituzionale del Paese e la conseguente ampiezza della loro esposizione digitale in termini di infrastrutture, servizi e visibilità nel dominio cibernetico.

Seguono i Comuni, le Regioni e le Aziende sanitarie, ambiti caratterizzati da un'elevata capillarità territoriale e da una forte interazione digitale con cittadini e imprese. Per tali soggetti, la diffusione di servizi online e la molteplicità degli *asset* IT contribuiscono ad ampliare la superficie di esposizione e, conseguentemente, il volume delle attività cibernetiche rilevate.

Una quota rilevante di eventi ha, inoltre, interessato università e centri di ricerca, nonché enti pubblici non economici, contesti contraddistinti da ecosistemi informativi articolati e da un'ampia interconnessione con reti nazionali e internazionali.

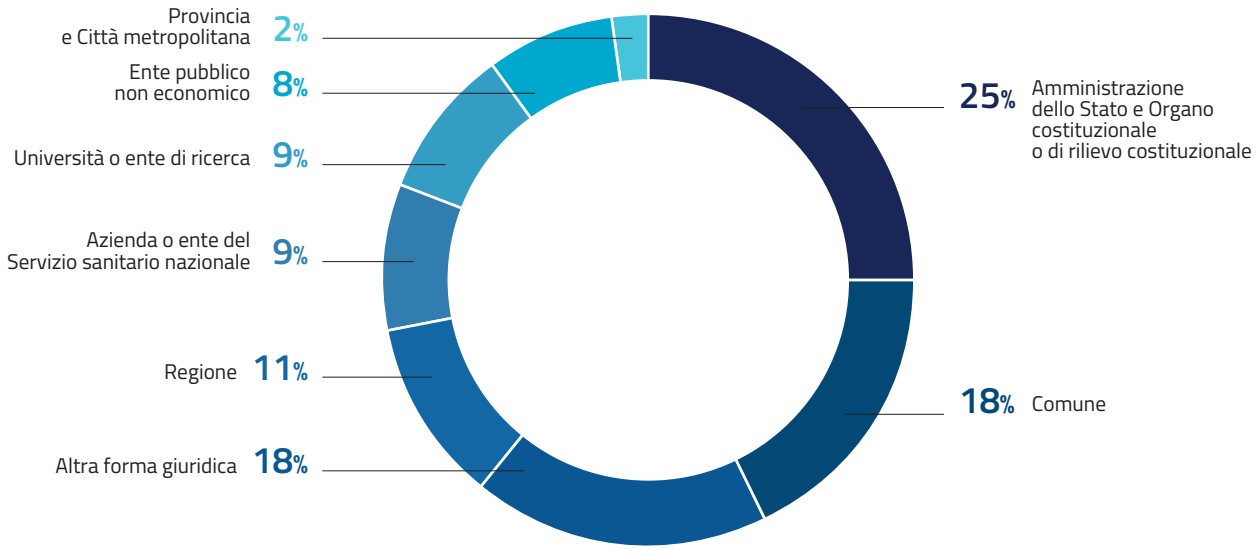


Figura 13 – Distribuzione degli eventi cyber nei settori della Pubblica Amministrazione

L'analisi delle tipologie di minaccia (Figura 14) evidenzia, oltre alla netta prevalenza del DDoS, numeri significativi per le campagne di *phishing* e i fenomeni di *brand abuse*, che confermano il ricorso a tecniche di ingegneria sociale e di sfruttamento dell'identità di soggetti istituzionali per il tentativo di acquisizione indebita di credenziali. Di rilievo risulta anche la presenza di eventi di esposizione dati, di compromissione di caselle di posta elettronica e di scansioni attive su credenziali, riconducibili a attività di ricognizione e preparazione di potenziali attacchi successivi. Queste azioni, infatti, consentono all'attore malevolo di raccogliere informazioni sulla vittima, verificare le credenziali, acquisire accesso a canali di comunicazione interni o predisporre ulteriori azioni di compromissione.

Le restanti tipologie di minaccia, tra cui compromissioni da malware, intrusioni tramite credenziali valide, sfruttamento di vulnerabilità e *ransomware*, presentano una frequenza più contenuta in termini di eventi, ma assumono un peso maggiore laddove evolvono in incidenti con impatto sui sistemi e sull'erogazione dei servizi.

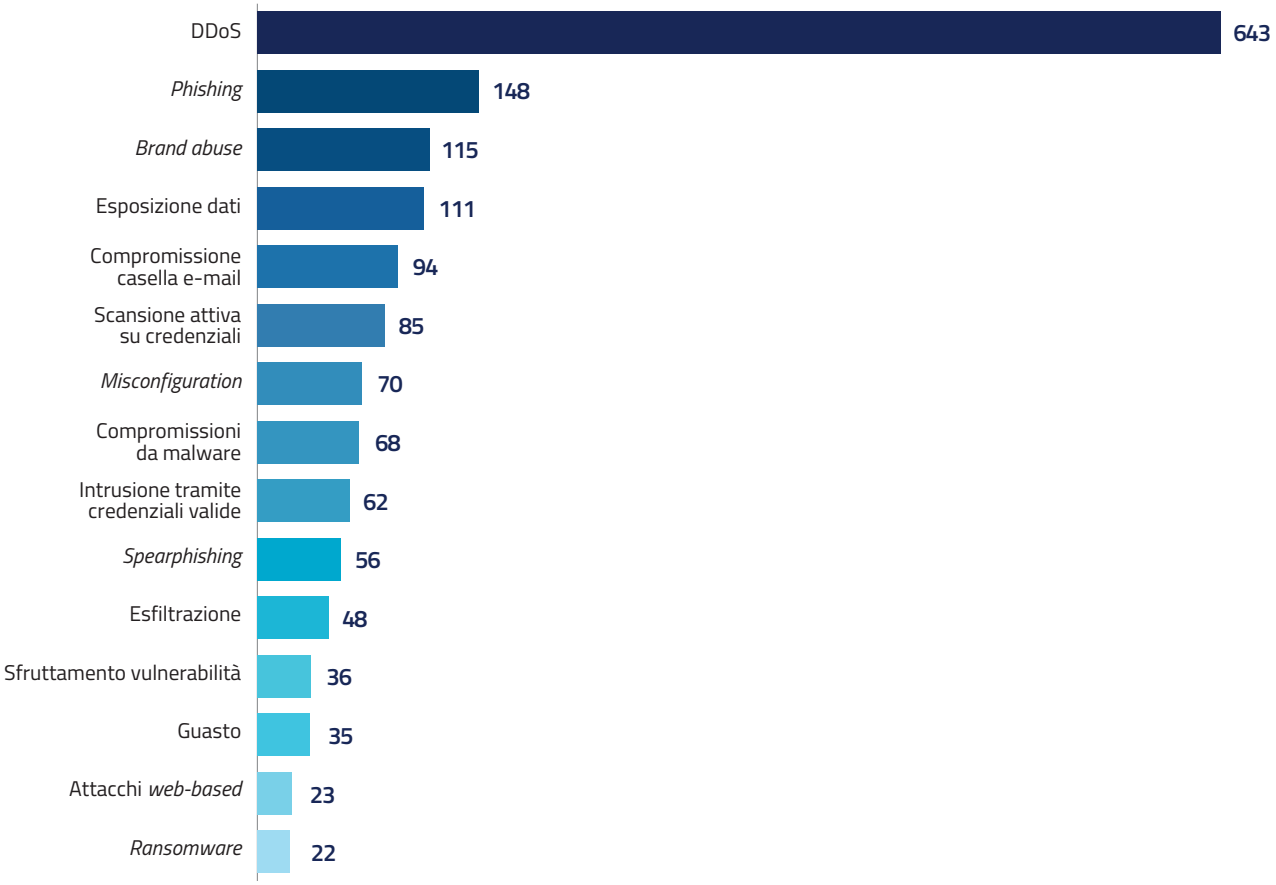


Figura 14 – Tipologie di minacce rilevate negli eventi cyber nella Pubblica Amministrazione (top 15)

3

L'Agenzia nel panorama istituzionale

In un quadro in costante evoluzione sia dal punto di vista normativo che della minaccia, è stato confermato il ruolo centrale dell'Agenzia per la cybersicurezza nazionale nel coordinamento dei molteplici soggetti coinvolti nella sicurezza e resilienza cibernetica del Paese.

Tale funzione si è esplicata attraverso la conduzione e la partecipazione a diversi tavoli interministeriali, volti a favorire una cooperazione strutturata sia a livello politico-strategico che tecnico-operativo. Accanto al Comitato interministeriale per la cybersicurezza (CIC), cruciale nell'indirizzare le politiche nazionali in materia, l'Agenzia promuove il confronto tra rappresentanti dei Ministeri e delle altre Amministrazioni all'interno di organismi quali il Nucleo per la cybersicurezza (NCS), il Tavolo interministeriale per l'attuazione del Perimetro di sicurezza nazionale cibernetica e il Tavolo per l'attuazione della disciplina NIS.

Parimenti significativo si è rivelato il dialogo con il Parlamento, nell'ambito delle funzioni di indirizzo, vigilanza e produzione normativa: l'interlocuzione costante ha, infatti, contribuito all'avanzamento del quadro legislativo in materia di cybersicurezza, di digitalizzazione sicura e nel definire un assetto normativo nazionale in materia di intelligenza artificiale, coerente con quello europeo.

Allo stesso tempo, l'ACN ha mantenuto una presenza costante all'interno del tessuto istituzionale, sociale e produttivo, organizzando e garantendo la propria partecipazione a numerosi eventi di settore. Ha, inoltre, continuato ad ampliare gli spazi di collaborazione tramite la sottoscrizione di accordi con soggetti pubblici e privati per promuovere un ecosistema cyber nazionale sempre più resiliente.

La collaborazione istituzionale si è rafforzata anche attraverso la pianificazione e la partecipazione a momenti esercitativi. In tale quadro, l'Agenzia, sia a livello nazionale che internazionale, ha potuto verificare e affinare i meccanismi di gestione degli incidenti e delle crisi cyber, cooperando con i propri partner a tutti i livelli.

3.1 COORDINAMENTO INTERISTITUZIONALE

L'Agenzia ha consolidato il suo ruolo centrale di coordinamento all'interno dei numerosi consessi interistituzionali che si occupano di cybersicurezza su un piano strategico-politico, tecnico-operativo e normativo-regolamentare. La collaborazione è fondamentale non solo con gli altri soggetti istituzionali, ma anche con quelli della ricerca, dell'università e del mondo privato nell'ottica di individuare sinergie per rafforzare il più ampio ecosistema nazionale della cybersicurezza.

Accanto a queste attività, l'ACN partecipa in maniera attiva anche ad altri contesti di confronto tra Amministrazioni, contribuendo, per quanto di competenza, ai lavori di tavoli tecnici, comitati e gruppi di lavoro trasversali che favoriscono la condivisione di esperienze, lo scambio di informazioni e l'allineamento operativo tra le diverse istituzioni.

Il Comitato interministeriale per la cybersicurezza nel 2025

3.1.1 Comitato interministeriale per la cybersicurezza

Nel 2025 il Comitato interministeriale per la cybersicurezza ha continuato a svolgere il proprio ruolo di indirizzo politico-strategico per la definizione e l'attuazione delle politiche nazionali di cybersicurezza, garantendo il confronto tra i Ministri maggiormente coinvolti dalla materia cyber. Il CIC ha il compito di proporre al Presidente del Consiglio dei ministri, che lo presiede, gli indirizzi delle politiche di cybersicurezza, di verificare l'attuazione della Strategia nazionale in questo ambito, di controllare la gestione economico-finanziaria dell'ACN e di promuovere iniziative volte a potenziare la sicurezza cibernetica.

Nel periodo di riferimento il CIC si è riunito quattro volte, nei mesi di febbraio, aprile, ottobre e dicembre. Il CIC è stato particolarmente impegnato in ambito Perimetro di sicurezza nazionale cibernetica, rendendo il proprio parere in merito a un intervento normativo che ha ampliato la tassonomia degli incidenti per i quali è obbligatoria la notifica da parte dei soggetti inclusi nel PSNC, introducendo la fattispecie relativa all'accesso non autorizzato o con abuso dei privilegi concessi. Ciò si aggiunge alle proposte formulate per l'aggiornamento dei soggetti inclusi nel PSNC, tenendo conto delle indicazioni fornite dal Tavolo interministeriale per l'attuazione del Perimetro di sicurezza nazionale cibernetica.

Il CIC ha altresì fornito il proprio parere sui principali provvedimenti di natura economico-finanziaria relativi all'ACN tra cui il bilancio consuntivo 2024, l'assestamento di bilancio 2025 e il budget economico per l'anno 2026.

FOCUS

La modifica della tassonomia degli incidenti PSNC

La proposta di introdurre una nuova fattispecie di incidente soggetto a notifica per il PSNC ha risposto all'urgente necessità di aggiornare la tassonomia degli incidenti per innalzare il livello di sicurezza nazionale nello spazio cibernetico.
La nuova fattispecie, "Accesso non autorizzato o con abuso dei privilegi concessi", include le attività di accesso ai dati che, sebbene condotte dall'interno delle reti, risultino prive di autorizzazione o comunque abusive, dal momento che eccedono presupposti, limiti, condizioni e finalità dell'autorizzazione e, quindi, illegittime e potenzialmente dannose. La definizione di accesso non autorizzato o con abuso dei privilegi concessi fa riferimento anche a parametri quali-quantitativi per consentire ai soggetti inclusi nel Perimetro di notificare, entro 6 ore dal momento in cui ne vengano a conoscenza, esclusivamente le minacce significative e rilevanti.

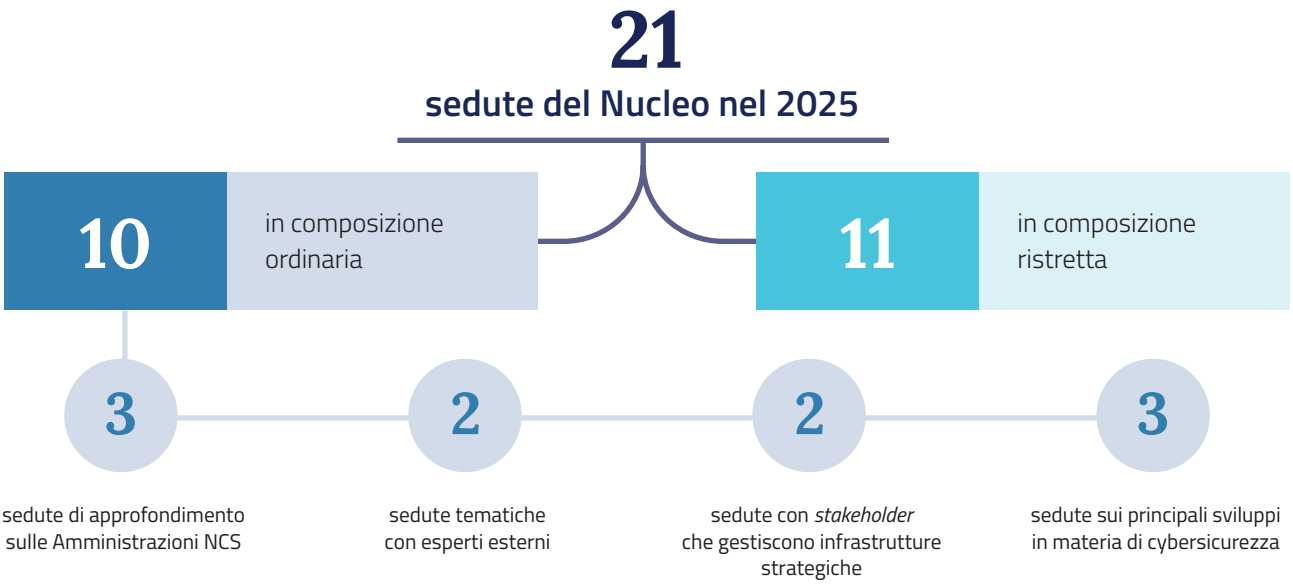
3.1.2 Nucleo per la cybersicurezza

Nel 2025 il Nucleo per la cybersicurezza ha proseguito la propria attività quale sede di coordinamento tecnico-operativo a supporto del Presidente del Consiglio dei ministri, garantendo il raccordo tra le Amministrazioni maggiormente interessate alla materia della cybersicurezza.

In continuità con quanto svolto negli anni precedenti, il Nucleo ha assicurato il supporto alle decisioni del livello politico-strategico, favorendo una valutazione integrata degli scenari di rischio, per un'efficace prevenzione e gestione degli eventi e degli incidenti cibernetici di maggiore rilievo. Con l'entrata in vigore della legge n. 132/2025, la partecipazione al Nucleo per la cybersicurezza è stata allargata anche all'Agenzia per l'Italia digitale. Nel periodo in esame, l'NCS si è riunito complessivamente 21 volte, per 10 sedute in composizione ordinaria e 11 in composizione ristretta.

Il Nucleo per la cybersicurezza nel 2025

Composizione ordinaria



Le sedute in composizione ristretta dell'NCS hanno permesso, sulla base dello scambio informativo tra le Amministrazioni coinvolte, una valutazione di impatto condivisa sulle più urgenti situazioni di rischio cibernetico funzionale alla loro gestione coordinata e all'adeguata informativa al Vertice politico. Nelle sedute in composizione ordinaria, invece, è stato possibile approfondire con tutte le Amministrazioni NCS specifiche questioni, quali l'evoluzione del quadro normativo, lo stato della minaccia e le iniziative nazionali e internazionali messe in atto dall'ACN e dagli altri componenti.

Anche nel 2025 il Nucleo ha continuato ad arricchire le sedute in composizione ordinaria con una programmazione di riunioni specificatamente dedicate alle Amministrazioni NCS, ad approfondimenti tematici e a focus settoriali. In particolare, alcune sessioni hanno riguardato l'illustrazione di assetti organizzativi in materia di cybersicurezza, *best practice* adottate e casi studio di interesse da parte delle diverse Amministrazioni che compongono il Nucleo al fine di favorire la conoscenza reciproca e di condividere le esperienze acquisite. Nel 2025 questa tipologia di riunioni ha consentito di mettere a fattor comune le prospettive in materia cyber del MAECI, del MIT e del Ministero dell'interno.

Il Nucleo si è, altresì, aperto al confronto con autorevoli esperti esterni, organizzando delle sedute di approfondimento su temi di interesse generale. Il Nucleo ha così accolto il Presidente del CENTAI Institute, Mario Rasetti, per discutere dei dilemmi etici e sociali posti dall'intelligenza artificiale e il Presidente dell'Autorità garante per la protezione dei dati personali, Pasquale Stanzione, con un intervento sulle sinergie tra *privacy* e cybersicurezza. Tali sedute hanno consentito di avviare una discussione e una riflessione condivisa a beneficio delle Amministrazioni, rappresentando una *best practice* che vedrà il coinvolgimento in futuro di altri eminenti esperti per allargare il confronto su temi emergenti.

Infine, con l'obiettivo di intensificare il dialogo tra pubblico e privato, sono state organizzate delle sessioni aperte a operatori che gestiscono infrastrutture strategiche nazionali, riunioni che hanno permesso uno scambio sulla minaccia cyber percepita dal rispettivo osservatorio, nonché sulle misure adottate a fronte dello scenario in rapida evoluzione. Tali riunioni hanno coinvolto settori strategici della cybersicurezza, nello specifico il settore energetico e il settore del trasporto aereo, traendo spunto da eventi e incidenti effettivamente avvenuti. Queste sedute hanno anche fatto emergere l'opportunità di organizzare un'esercitazione che potesse coinvolgere il settore energetico e quello delle telecomunicazioni per testare l'ecosistema nazionale di gestione e risposta in caso di crisi cyber, come poi effettivamente avvenuto a dicembre con l'esercitazione nazionale ACN-CyEX25.

FOCUS

Il coordinamento interistituzionale per ACN-CyEX25

In occasione dell'esercitazione ACN-CyEX25 (vedasi paragrafo 3.4) si è resa necessaria l'attivazione del Nucleo per la cybersicurezza. Le due sedute, di cui la prima allargata anche ad alcuni operatori economici coinvolti nell'esercitazione, hanno consentito di testare procedure, flussi informativi e modalità di coordinamento interistituzionale in uno scenario simulato di eventi e incidenti ad alta intensità, rafforzando la capacità di risposta coordinata a livello nazionale e confermando il Nucleo quale consesso fondamentale di raccordo informativo in materia cyber.

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), istituito presso l'ACN e presieduto dal Direttore generale, assicura il coordinamento tra le Amministrazioni coinvolte, a vario titolo, nell'attuazione del PSNC. In particolare, il Tavolo opera a supporto del CIC, specie in relazione all'individuazione dei soggetti che esercitano funzioni essenziali dello Stato o assicurano servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi del Paese attraverso reti, sistemi informativi e servizi informatici il cui malfunzionamento, utilizzo improprio o interruzione potrebbe arrecare pregiudizio alla sicurezza nazionale.

In tale contesto, il Tavolo Perimetro si è riunito due volte nel corso del 2025, nei mesi di marzo e ottobre, deliberando sulle proposte di aggiornamento dei soggetti inclusi nel Perimetro avanzate dalle Amministrazioni competenti per i settori coperti dalla disciplina PSNC. Su proposta del CIC sono stati, quindi, adottati da parte del Presidente del Consiglio dei ministri, i DPCM che recepiscono i citati aggiornamenti, portando a 121 il numero dei soggetti inclusi nel Perimetro a fine 2025.

3.1.4 Tavolo per l'attuazione della disciplina NIS

L'istituzione del Tavolo per l'attuazione della disciplina NIS (c.d. Tavolo NIS), costituito in via permanente presso l'ACN, è composto, oltre che dal Direttore generale dell'Agenzia che lo presiede, da rappresentanti designati dalle Autorità di settore e dalla Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. Il Tavolo ha assicurato la regia della complessa attività di definizione dell'impianto regolatorio previsto dal decreto NIS (vedasi Capitolo 1). Nel 2025, il Tavolo NIS si è riunito 5 volte (gennaio, aprile, luglio, settembre e dicembre) per esaminare e aggiornare diversi provvedimenti attuativi.

Nella seduta di gennaio, il Tavolo NIS è stato sentito per intervenire su termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale, nonché sulle informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e sulla designazione dei loro rappresentanti. Sono state anche definite le modalità di designazione del sostituto punto di contatto, utile a garantire la continuità operativa, e introdotte ulteriori modalità di interazione con la piattaforma NIS per consentire ai soggetti di mantenere aggiornate le informazioni rilevanti.

Nel mese di aprile, il Tavolo NIS si è riunito per esaminare il primo elenco dei soggetti essenziali e dei soggetti importanti, sulla base delle registrazioni effettuate sulla piattaforma entro i termini previsti. Ha, inoltre, preso in considerazione la Determinazione ACN sulle specifiche di base, nonché quella relativa alla partecipazione dei soggetti agli accordi di condivisione delle informazioni sulla sicurezza informatica.

La seduta di luglio ha permesso al Tavolo NIS di regolare il c.d. "aggiornamento continuo" delle informazioni che i soggetti NIS trasmettono tramite piattaforma.

A settembre, il Tavolo NIS ha esaminato l'aggiornamento della disciplina per introdurre, anche sulla base delle indicazioni provenienti dai soggetti NIS, la figura del referente CSIRT, nonché per esonerare i soggetti rientranti nell'ambito di applicazione del Regolamento europeo DORA (*Digital Operational Resilience Act*) dall'obbligo di indicare i componenti degli organi di amministrazione e direttivi.

Nella seduta di dicembre, in vista della riapertura dei termini annuali per la registrazione sulla piattaforma dei soggetti NIS e per l'aggiornamento delle informazioni, sono state meglio specificate alcune modalità per il corretto adempimento di tali obblighi. In tale seduta, infine, il Tavolo NIS è stato sentito per quanto concerne la Determinazione ACN relativa alla politica nazionale di divulgazione coordinata delle vulnerabilità e per consolidare l'elenco dei soggetti NIS nel 2025.

In stretta correlazione con l'attività svolta dal Tavolo per l'attuazione della disciplina NIS, che ha rappresentato la sede nella quale è stato possibile valorizzare le istanze rappresentate dalle Autorità di settore e dai rappresentanti designati dalla Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano, va poi evidenziato il ruolo assunto dai Tavoli settoriali, coordinati e promossi dalle diverse Autorità di settore.

3.1.5 Comitato tecnico-scientifico dell'ACN

Al fine di promuovere la collaborazione con il sistema dell'università e della ricerca, oltre che con il mondo produttivo nazionale, l'ACN si avvale di un Comitato tecnico-scientifico (CTS) con funzioni di consulenza e proposta, che è presieduto dal Direttore generale e composto, oltre che da personale dell'Agenzia, da 4 rappresentanti dell'industria, da 4 rappresentanti degli enti di ricerca e dell'accademia e da un rappresentante delle associazioni del settore della sicurezza delle aziende strategiche del Paese. Nel corso del 2025 si è insediato il nuovo Comitato e, a partire da giugno 2025, si è riunito tre volte. Il CTS si è concentrato sull'aggiornamento dell'Agenda di ricerca e innovazione per la cybersicurezza, sullo sviluppo delle competenze in cybersicurezza predisposta dall'ACN con il MUR (vedasi Capitolo 5) e sul progetto per la valutazione del ritorno degli investimenti in cybersicurezza (*Return on Security Investment*).

Inoltre, il CTS ha approfondito diversi profili legati all'evoluzione delle tecnologie quantistiche, dall'esigenza di divulgazione e consapevolezza, agli impatti per la sicurezza delle infrastrutture digitali nazionali. Infine, il CTS è stato coinvolto in qualità di meccanismo di salvaguardia dell'imparzialità dell'Organismo di certificazione della sicurezza informatica (OCSI). In tale ambito, il Comitato ha contribuito all'aggiornamento delle Linee guida OCSI (vedasi Capitolo 4), rafforzando le misure a tutela dell'imparzialità.

Il Comitato tecnico-scientifico nel 2025

Presidente

Direttore generale ACN

Composizione

4 ACN
- Capo di Gabinetto
- Capo Servizio Operazioni e gestione delle crisi cyber
- Capo Servizio Certificazione e vigilanza
- Capo Servizio Programmi industriali, tecnologici e di ricerca

4 Industria
- Domitilla Benigni
- Andrea Campora
- David Neumarker
- Marco Elio Rottigni

4 Università e ricerca
- Alessandro Armando
- Paola Inverardi
- Antonella Polimeni
- Bruno Siciliano

4 Associazioni del settore della sicurezza informatica
- Yuri Rassega

3.2 RAPPORTI CON IL PARLAMENTO

Come noto, il controllo parlamentare sull'operato dell'Agenzia per la cybersicurezza nazionale è garanzia del rispetto delle funzioni a essa demandate. In questo ambito gioca un ruolo fondamentale la Relazione sull'attività svolta dall'ACN nell'anno precedente presentata dal Presidente del Consiglio dei ministri al Parlamento.

Nel corso del 2025, l'ACN è stata chiamata a fornire il proprio contributo al Parlamento durante la sua attività conoscitiva, legislativa e di vigilanza. Il Direttore generale ha rappresentato l'articolata prospettiva dell'Agenzia nel corso di 5 audizioni, intervenendo in due occasioni nei lavori parlamentari che hanno portato all'adeguamento del quadro normativo nazionale a diversi Regolamenti europei con profili di cybersicurezza, nonché all'approvazione della legge nazionale sull'intelligenza artificiale (legge n. 132/2025). Il Direttore generale è stato chiamato, altresì, a rappresentare il quadro conoscitivo dell'ACN in merito a una serie di altre tematiche, tra cui i profili di cybersicurezza dell'anagrafe tributaria, lo sfruttamento del dominio cibernetico da parte della criminalità organizzata, nonché i collegamenti tra cybersicurezza e violenza di genere online.

Nell'ambito del controllo cui è sottoposta l'Agenzia da parte del Comitato parlamentare per la sicurezza della Repubblica (COPASIR) per quanto concerne le funzioni a tutela della sicurezza nazionale, l'ACN ha – come di consueto – predisposto la Relazione annuale sull'attività svolta nell'anno precedente. In tale Relazione vengono specificati i soli profili relativi alla tutela della sicurezza nazionale nello spazio cibernetico. Ciò, in combinato disposto con la Relazione annuale al Parlamento, consente al COPASIR di ottenere un quadro completo di tutte le attività dell'Agenzia. Infine, il Direttore generale dell'ACN è stato chiamato tre volte in audizione da parte del COPASIR.

Audizioni del Direttore generale dell'ACN

APRILE

Commissione parlamentare di vigilanza sull'anagrafe tributaria

Nell'ambito dell'indagine conoscitiva sulle misure di contrasto all'evasione fiscale, sulla sicurezza delle banche dati dell'anagrafe tributaria e sulla tutela della riservatezza dei dati dei contribuenti, sono stati illustrati i rilevanti risvolti di sicurezza cibernetica e l'approccio olistico dell'ACN, che fornisce risposte multilivello per la prevenzione e la gestione degli incidenti cyber.

MAGGIO

Commissioni riunite IX (Trasporti, poste e telecomunicazioni) e X (Attività produttive, commercio e turismo) della Camera dei deputati nell'ambito dell'esame del disegno di legge recante disposizioni e deleghe al Governo in materia di intelligenza artificiale

L'intervento ha riguardato la necessità di raccordare la normativa nazionale con quella europea e la definizione dell'architettura della *governance* nazionale in materia di intelligenza artificiale.

GIUGNO

Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali

Il contributo ha riguardato l'uso del dominio cibernetico da parte della criminalità organizzata, incluse le piattaforme di comunicazione criptata e le valute virtuali, con un focus sulla minaccia *ransomware*. Sebbene il contrasto al crimine non rientri nel mandato istituzionale dell'ACN, questa svolge un ruolo fondamentale nel prevenirlo attraverso le azioni volte a rafforzare la resilienza sistemica nazionale.

OTTOBRE

XIV Commissione (Politiche dell'Unione europea) della Camera dei deputati nell'ambito dell'esame del disegno di legge di delegazione europea 2025

È stato illustrato l'impegno dell'Agenzia volto ad assicurare l'adeguamento dell'ordinamento interno alle disposizioni contenute nel *Cyber Resilience Act*, alla revisione del *Cybersecurity Act* e alle misure previste dal *Cyber Solidarity Act*.

NOVEMBRE

Commissione parlamentare di inchiesta sul femminicidio, nonché su ogni forma di violenza di genere

L'intervento, afferente al filone di inchiesta sulla violenza online, si è incentrato sull'utilizzo consapevole delle tecnologie digitali, sui profili di connessione tra cybersicurezza e protezione dei dati e sull'utilizzo dell'intelligenza artificiale per produrre *deep fake*.

3.3 PARTECIPAZIONE A EVENTI E ACCORDI DI COLLABORAZIONE

Un importante ruolo nell'azione ad ampio spettro dell'Agenzia è stato svolto, anche nel corso dell'anno in esame, dalle numerose iniziative di collaborazione attraverso la partecipazione a eventi e la stipula di accordi. In un contesto caratterizzato da minacce informatiche in costante evoluzione e da una crescente interdipendenza digitale, l'innalzamento della postura nazionale di cybersicurezza, anche nel 2025, ha rappresentato una priorità strategica per la tutela degli interessi del Paese. La complessità e la pervasività dei rischi cyber richiedono, infatti, un approccio sistemico, fondato sulla sinergia tra istituzioni, imprese, organismi di ricerca e tutti gli attori coinvolti nel funzionamento delle infrastrutture digitali e dei servizi essenziali.

FOCUS

Il supporto dell'ACN ai grandi eventi: Olimpiadi Milano Cortina 2026

A gennaio 2025, l'Agenzia e la Fondazione Milano Cortina 2026 hanno sottoscritto un protocollo per contribuire alla cybersicurezza dei Giochi olimpici e paralimpici invernali di Milano Cortina 2026 per monitorare e analizzare le minacce, scambiare informazioni critiche e supportare la gestione delle eventuali crisi.
*Data la rilevanza strategica dell'evento e l'elevata complessità di assicurarne la sicurezza cibernetica, sono state destinate risorse ad hoc (D.L. n. 96/2025) in favore dell'*ACN*. Ciò rimarca l'importanza della cybersicurezza in occasione di grandi eventi internazionali e conferma la fiducia riposta nell'Agenzia quale presidio operativo essenziale per la tutela della superficie digitale del Paese, chiamata a garantire la protezione delle reti, dei dati e dei servizi critici in contesti caratterizzati da una particolare esposizione al rischio.*

In tale quadro, il rafforzamento e il consolidamento dei rapporti con *stakeholder* pubblici e privati ha spinto l'Agenzia ad assicurare la propria presenza ai principali eventi nazionali in materia di cybersicurezza fornendo il proprio contributo sulle principali tematiche di attualità e sulle attività da essa svolte. Attraverso la predisposizione di stand dedicati ACN, è stato, inoltre, instaurato un costante dialogo e confronto con i partecipanti e i visitatori dei grandi eventi di cybersicurezza e dei maggiori eventi dedicati alla Pubblica Amministrazione (Cyber 4.0., *Rome future week*, ForumPA, assemblea nazionale ANCI).

Inoltre, l'Agenzia è stata protagonista di circa 60 eventi divulgativi, informativi e di supporto per avviare un proficuo dialogo con i soggetti che operano nei diversi settori cui si applica la disciplina NIS ed evidenziare come questa costituisca un elemento cardine della resilienza cyber del Paese.

Oltre a ciò, l'Agenzia ha dato il proprio apporto a numerosi eventi organizzati da associazioni, università e aziende, garantendo il contributo di propri qualificati rappresentanti. Tale sforzo, ha permesso all'Agenzia di aumentare la capillarità della propria presenza su tutto il territorio nazionale, nonché di fornire un apporto anche di tipo tecnico, come con l'evento "Cybersecurity nella PA".

FOCUS

L'evento "Cybersecurity nella PA"

Nel mese di ottobre, l'ACN ha collaborato all'evento "Cybersecurity nella PA", iniziativa organizzata da Cerchio ICT, consorzio di 4 società in house ICT operanti in Trentino-Alto Adige, Emilia-Romagna e Veneto (Informatica Alto Adige, Trentino Digitale, Lepida e Pasubio Tecnologia). L'evento, della durata di 3 giorni e distribuito su 2 sedi (Bologna e Trento), ha approfondito le strategie e le azioni che gli enti locali stanno mettendo in campo in tema di cybersecurity. L'Agenzia ha contribuito all'iniziativa con un aggiornamento sull'attuazione della Direttiva NIS2, nonché sulle opportunità di finanziamento provenienti dalla Strategia nazionale di cybersicurezza 2022-2026 e dal PNRR al fine di rafforzare i livelli di cybersicurezza delle PA locali. Infine, esperti del CSIRT Italia, rappresentanti delle Forze dell'ordine e dei CSIRT territoriali hanno esaminato scenari operativi per affrontare le crescenti minacce cyber, con particolare riguardo alla minaccia ransomware. L'evento si è concluso con una simulazione table-top che ha coinvolto attivamente i partecipanti nella gestione di un incidente ransomware.

Sempre nell'ottica di ampliare gli spazi di collaborazione istituzionale, nel 2025 l'Agenzia ha stipulato oltre 20 accordi con soggetti pubblici e privati, intercettando il comune obiettivo di rafforzare la resilienza sistemica, facilitare la condivisione tempestiva delle informazioni e favorire la prevenzione, la mitigazione e la risposta a incidenti cyber. Attraverso un impegno congiunto e condiviso è stato possibile consolidare ulteriormente un ecosistema cyber nazionale capace di sostenere la trasformazione digitale del Paese in condizioni di sicurezza, perseguendo tre direttrici principali: promuovere la cultura, la formazione e la ricerca sulla cybersicurezza, innalzare il livello di sicurezza cibernetica dei dati e delle infrastrutture nazionali, collaborare con le istituzioni per consolidare sinergie nel settore della cybersicurezza.

3.4 ESERCITAZIONI NAZIONALI E INTERNAZIONALI

Nel corso del 2025, l'Agenzia ha realizzato e partecipato a diverse esercitazioni, nazionali e internazionali, testando le capacità di gestione e risposta agli incidenti e alle crisi cibernetiche, permettendo di verificare la prontezza di reazione e di aggiornare procedure e meccanismi dell'intero ecosistema nazionale. L'impegno dell'Agenzia mira a promuovere una preparazione cyber strutturata e continuativa, in linea con il quadro normativo europeo e con le crescenti sfide del contesto geopolitico e tecnologico.

A livello nazionale, nel 2025 è proseguito il programma di esercitazioni ACN-CyEX, promosso e coordinato dall'Agenzia per rafforzare la preparazione complessiva degli attori coinvolti nella gestione della cybersicurezza e di migliorare le capacità di prevenzione, risposta e coordinamento in caso di incidenti e crisi cyber del Paese. Rispetto all'anno precedente, la seconda edizione ha raggiunto un ulteriore livello di maturità, caratterizzato da un aumento della complessità e del realismo degli scenari, nonché dal coinvolgimento di un numero crescente di attori istituzionali e operatori privati, sia nella fase di pianificazione che di esecuzione.

ACN-CyEX25, culminata con la fase di gioco il 10 e 11 dicembre, online e in presenza, ha visto coinvolti 19 operatori del settore energetico e delle telecomunicazioni e diverse Amministrazioni, per un totale di 506 partecipanti. La simulazione ha previsto scenari multipli di crescente complessità, caratterizzati da incidenti cibernetici concomitanti (*phishing*, *smishing*, uso sospetto di credenziali, *ransomware*, attacchi DDoS, compromissioni della *supply chain* ed esfiltrazioni di dati), mettendo in evidenza le interdipendenze tra domini IT e OT e l'evoluzione verso dinamiche di *escalation* sistemica a livello nazionale. Le ripercussioni hanno riguardato anche aspetti reputazionali, comunicativi e di coordinamento intersettoriale e interistituzionale.

L'esercitazione ha consentito, inoltre, di simulare e testare i meccanismi di notifica di incidente al CSIRT Italia, il quale ha ricevuto 126 segnalazioni in 2 giorni, nonché il meccanismo di coordinamento tecnico, mediante una *war room*, e interistituzionale con l'attivazione dell'NCS. Ciò ha favorito una maggiore integrazione tra i livelli di governo degli operatori privati e una più stretta connessione tra dimensione tecnica, operativa e decisionale.

ACN CYEX 25

I numeri di ACN-CyEX25

19
Organizzazioni partecipanti

+500
Persone coinvolte

+1.250
Inject inviati

+45.000
E-mail inviate

+120
Segnalazioni ricevute dal CSIRT Italia

In ambito Unione europea, l'Agenzia ha partecipato alle esercitazioni della rete EU-CyCLONe e del gruppo del Consiglio dell'UE sulle questioni cyber (HWPCI). Nel mese di ottobre, l'ACN ha partecipato all'esercitazione della rete EU-CyCLONe denominata CySOPEx25, finalizzata a identificare miglioramenti e potenziali lacune nelle procedure standardizzate di risposta a incidenti e crisi (ovvero le nuove *standard operating procedures* sviluppate in ambito ENISA), nonché ad addestrarsi sulla consapevolezza situazionale e sui processi di condivisione delle informazioni.

A questa ha fatto seguito l'esercitazione BlueOLEx25, appuntamento annuale di riferimento della rete EU-CyCLONe, che vede l'ACN in primo piano nell'organizzazione e pianificazione detenendo la *lead* del relativo gruppo di lavoro (vedasi Capitolo 6). L'esercitazione ha consentito di testare, in un contesto realistico e intersettoriale, i processi di cooperazione operativa tra gli Stati membri, il raccordo con il livello politico europeo e l'efficacia delle procedure di scambio informativo, rafforzando la capacità collettiva di risposta a crisi cyber complesse e ad alto impatto

sistemico. Inoltre, l'Agenzia ha contribuito attivamente all'esercitazione di tipo *table-top* Cyber Blutprint TTX promossa dall'HWPCI che, sulla base del medesimo scenario, ha permesso di testare l'applicazione del nuovo *Cyber Blueprint* a livello strategico-politico. Nel loro insieme, le attività esercitative sono state orientate alla verifica delle modalità di interazione interna alle reti, al rafforzamento della fiducia reciproca e della collaborazione tra i partecipanti, con l'obiettivo di favorire una risposta coordinata ed efficace in caso di crisi cibernetica su vasta scala.

Nel corso del 2025 l'Agenzia è stata impegnata per pianificare e preparare Cyber Europe 2026, ottava edizione della principale esercitazione europea di gestione delle crisi cibernetiche, organizzata con cadenza biennale sotto l'egida di ENISA. In tale contesto, l'Agenzia coordina la partecipazione dei soggetti nazionali, favorendo l'allineamento tra livello italiano ed europeo e la preparazione congiunta agli scenari esercitativi. L'edizione 2026 sarà focalizzata su scenari di crisi cyber ad alto impatto nei settori ferroviario e marittimo e prevederà il coinvolgimento degli Stati membri, delle istituzioni e delle agenzie dell'Unione, nonché delle principali reti europee di cooperazione, tra cui EU-CyCLONe e *CSIRTs Network*.

Nel 2025 sono state avviate, inoltre, le attività preliminari dell'esercitazione EU Integrated Resolve 2026, promossa dal Consiglio dell'Unione europea, dalla Commissione europea e dal Servizio europeo per l'azione esterna, finalizzata a rafforzare la capacità dell'UE di affrontare crisi complesse e ibride. In questa fase iniziale, l'ACN ha partecipato alle attività di coordinamento a supporto dell'Ufficio del Consigliere militare del Presidente del Consiglio dei ministri, contribuendo al raccordo tra Stati membri e istituzioni europee in vista delle successive fasi di pianificazione previste per il 2026.

In ambito NATO, l'ACN ha garantito il proprio contributo alle attività connesse alla pianificazione e allo svolgimento della Crisis Management Exercise (CMX25), esercitazione strategico-procedurale di riferimento dell'Alleanza che si tiene con cadenza biennale. Anche in tale contesto, l'Agenzia ha fornito il supporto di competenza all'Ufficio del Consigliere militare del Presidente del Consiglio dei ministri, che coordina la partecipazione nazionale all'iniziativa, assicurata tramite il Nucleo interministeriale situazione e pianificazione (NISP). Nel corso dell'anno, l'ACN ha inoltre partecipato alle attività esercitative correlate, Short Notice Exercise, contribuendo a testare i meccanismi nazionali di risposta e coordinamento in scenari di crisi caratterizzati da elevata complessità e ridotti tempi di preavviso, in coerenza con il quadro di cooperazione internazionale e con le esigenze di integrazione tra dimensione civile e militare della gestione delle crisi.

Nel 2025, di concerto con il Ministero della difesa, il personale dell'Agenzia ha partecipato alle esercitazioni Locked Shields e Crossed Swords organizzate dal NATO *Cooperative Cyber Defence Centre of Excellence* di Tallinn, ricoprendo ruoli qualificati di natura valutativa e operativa. Le esercitazioni hanno consentito di testare in condizioni realistiche le capacità di analisi, risposta e coordinamento, con particolare riferimento alla *cyber threat intelligence*, alla *situational awareness* e al *threat hunting*.

Nel corso del 2025 L'Agenzia ha, inoltre, partecipato all'esercitazione internazionale di gestione delle crisi cibernetiche AI & Cyber – Crisis Management Exercise, organizzata dell'omologa agenzia cyber francese, ANSSI, nell'ambito dell'*AI Action Summit* ospitato a Parigi nel mese di febbraio. L'esercitazione, di tipo *table-top*, ha coinvolto rappresentanti istituzionali, esperti

di cybersicurezza e attori del settore dell'intelligenza artificiale provenienti da numerosi Paesi ed è stata finalizzata a stimolare il confronto strategico su scenari di crisi cyber che interessano sistemi basati sull'IA.

Infine, nell'ambito della *Counter Ransomware Initiative* (vedasi Capitolo 6), l'Agenzia ha partecipato a un'esercitazione di tipo *table-top* in cui è stato simulato un attacco *ransomware* su larga scala al settore sanitario. L'iniziativa ha coinvolto oltre 30 Paesi, consentendo di valutare i processi decisionali e i meccanismi di coordinamento e cooperazione internazionale nella risposta a questa insidiosa minaccia cyber.

4

La sicurezza tecnologica

La sicurezza tecnologica rappresenta un elemento essenziale per la resilienza sistemica del Paese sia per la protezione delle infrastrutture critiche, sia per garantire un diffuso utilizzo di soluzioni affidabili. In uno scenario in cui il rischio zero non esiste, è essenziale avere a disposizione sistemi e servizi che rispondano a specifici requisiti di sicurezza cibernetica.

In questo contesto, l'Agenzia per la cybersicurezza nazionale svolge un ruolo centrale su più piani, garantendo le attività di scrutinio tecnologico negli ambiti più critici per la sicurezza nazionale, nonché quelle di certificazione e conformità rispetto a standard internazionali. A ciò si affiancano le attività di accompagnamento alla digitalizzazione sicura della Pubblica Amministrazione, basata, in particolare, sulla transizione alle tecnologie *cloud*. Per tutti questi aspetti si rivela indispensabile un'attenta azione di verifica e di ispezione, funzionale a una più completa valutazione dei profili di rischio.

L'Agenzia è attiva, inoltre, sul fronte dei poteri speciali esercitabili dal Governo, nel cui ambito fornisce analisi degli aspetti tecnici di cybersicurezza sia per quanto riguarda i casi di sua più diretta competenza come le tecnologie 5G, sia per gli altri casi che dovessero rilevare nei settori della difesa e sicurezza nazionale, nonché negli altri ambiti ritenuti strategici. L'ACN è chiamata, infine, a sostenere il rafforzamento delle capacità crittografiche del Paese, anche alla luce delle imminenti rivoluzioni derivanti dalla transizione al quantum, che rischiano di rendere insicure le attuali soluzioni in uso.

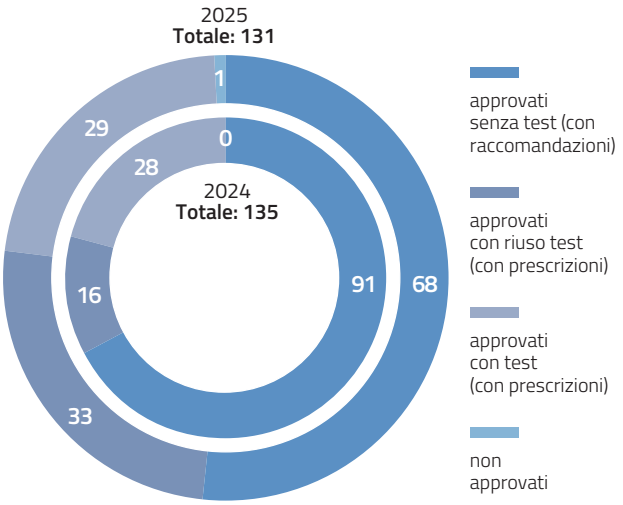
4.1 SCRUTINIO TECNOLOGICO PER IL PSNC

Nell'ambito dell'attuazione del PSNC, il Centro di valutazione e certificazione nazionale (CVCN) effettua i controlli necessari allo scrutinio tecnologico sugli *asset* rilevanti per il Perimetro di sicurezza nazionale cibernetica. A seguito di comunicazione da parte del soggetto sull'intenzione di acquisire un determinato bene ICT da impiegare all'interno del Perimetro, il CVCN attiva un procedimento amministrativo, che può concludersi con l'approvazione all'impiego, oppure con la non approvazione. L'approvazione all'impiego del bene ICT oggetto di comunicazione può essere soggetta a specifiche raccomandazioni o prescrizioni.

Nel 2025, il numero totale di procedimenti amministrativi avviati è rimasto sostanzialmente invariato rispetto all'anno precedente (165 procedimenti nel 2025, 171 nel 2024) così come allineato è risultato il numero dei procedimenti conclusi (131 nel 2025, mentre nel 2024 erano stati 135, come riportato in Figura 1), alcuni dei quali intrapresi nell'anno precedente. Da osservare che, non essendo ammessa la ripetizione di test già eseguiti, è notevolmente aumentato il numero di procedimenti approvati con riuso di test (33 nel 2025 a fronte dei 16 dell'anno precedente) in quanto è stato possibile trarre vantaggio da risultati già collezionati negli anni passati.

I procedimenti attivi, ossia in corso, a fine 2025 sono risultati più numerosi rispetto al passato, soprattutto per un incremento delle comunicazioni depositate nell'ultimo periodo dell'anno. Si riporta, pertanto, un incremento del numero di procedimenti in tutte e tre le fasi (Figura 1).

Procedimenti CVCN conclusi



Procedimenti CVCN attivi

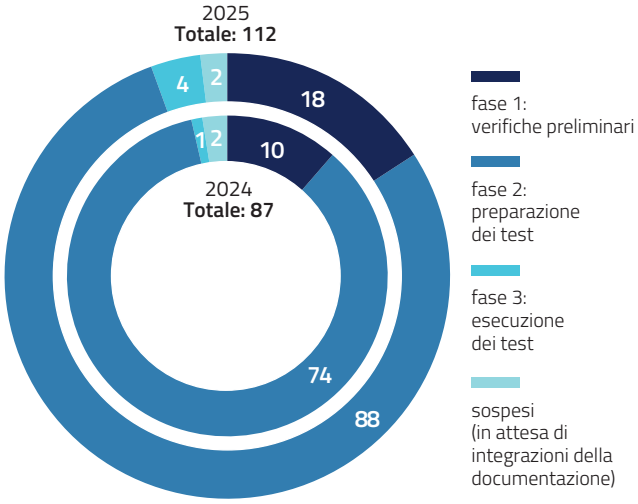


Figura 1 – Procedimenti CVCN conclusi e attivi al 31 dicembre: 2025 e 2024 a confronto

Al netto di volumi totali coerenti con il 2024, le attività del CVCN hanno registrato un generale incremento, riconducibile, essenzialmente, al maggior numero di procedimenti relativi a comunicazioni di affidamento per l'acquisizione di "Componenti hardware e software per acquisizione dati, monitoraggio, supervisione, controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali". Tali componenti, principalmente destinati ai sistemi di controllo industriale (ICS/SCADA ovvero *Industrial Control Systems* e *Supervisory Control And Data Acquisition*) nelle infrastrutture critiche, sono parti di sistemi complessi. Inoltre, ciascuna comunicazione comprende diversi elementi contemporaneamente e, in generale, l'attività del CVCN non può prescindere dal considerare l'ambiente di esercizio nella sua interezza. Tutto ciò si traduce in una maggiore complessità e durata dell'attività di analisi, valutazione e test, ossia, in definitiva, in tempistiche di preparazione dell'ambiente di test più lunghe, che richiedono numerose interazioni con i soggetti del Perimetro e i loro fornitori.

Le comunicazioni al CVCN afferenti a componenti ICS/SCADA sono passate da 23 nel 2024 a 37 nel 2025 (+60%), rappresentando la tipologia più consistente sul totale delle comunicazioni (Figura 2). Tra le altre componenti più frequenti, meritano menzione gli apparati di rete che, rispetto all'anno precedente hanno registrato un calo relativo (*switch*, *firewall* e *router*).

Tecnologie operative e sistemi industriali

OT (*Operational Technology*)
Insieme di tecnologie hardware e software utilizzate per monitorare e controllare processi fisici, anche in ambito industriale. Comprendono sensori, attuatori, macchinari e reti dedicate che operano in tempo reale.

ICS (*Industrial Control Systems*)
Categoria di sistemi che gestiscono il controllo industriale nelle infrastrutture critiche e negli impianti produttivi. Gli ICS includono varie architetture (inclusi i sistemi SCADA), coordinando automazione e sicurezza dei processi.

SCADA (*Supervisory Control And Data Acquisition*)
Sottotipo di ICS progettato per monitorare e controllare impianti distribuiti geograficamente. Utilizza unità remote per raccogliere dati, nonché un sistema centrale che supervisiona, registra e permette interventi in tempo reale.

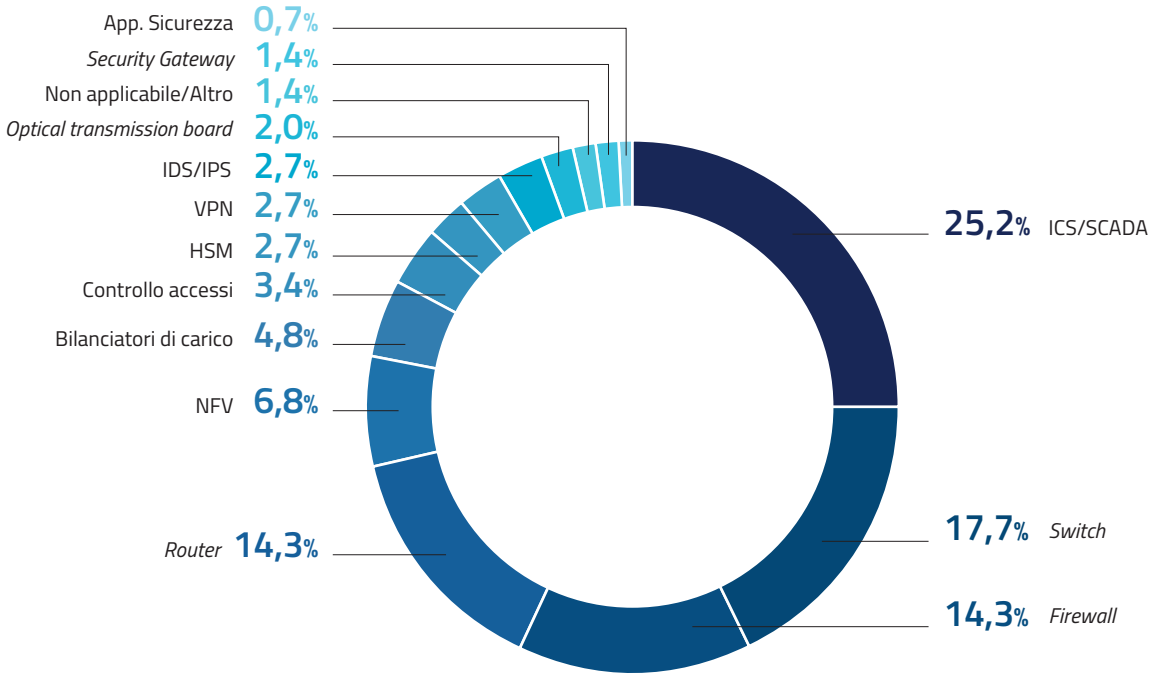


Figura 2 – Suddivisione dei procedimenti CVCN del 2025 per tipologia di componente

Nel corso dell'anno, particolare attenzione è stata posta al miglioramento dell'efficienza del CVCN soprattutto nella fase di preparazione all'esecuzione dei test (fase 2). La fase 2, diversamente dalla fase delle verifiche preliminari (fase 1) e da quella di esecuzione dei test (fase 3), non ha una durata predeterminata e risulta statisticamente quella che si protrae maggiormente. Basti pensare che, nel 2025, la fase 2 ha avuto mediamente una durata pari a 123 giorni, contro una media di 39 giorni per la fase 1 e di 51 giorni per la fase 3.

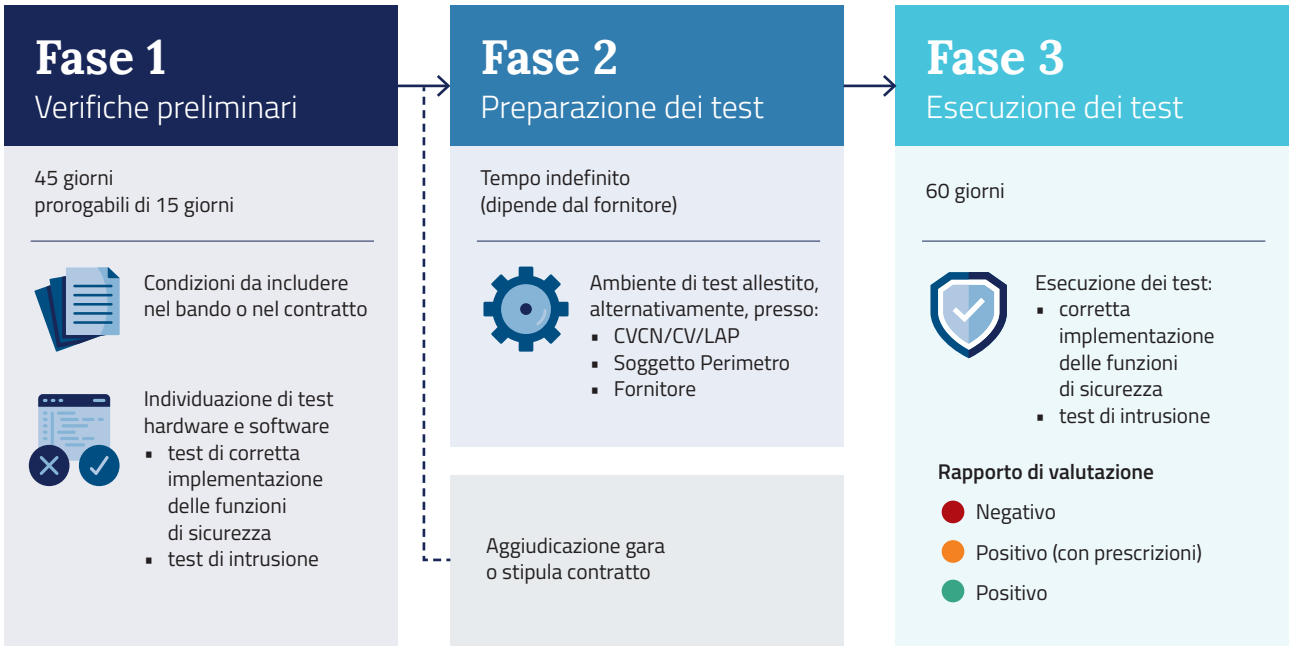


Figura 3 – Fasi della procedura di valutazione CVCN

Al fine di ridurre i tempi connessi alla fase 2, il CVCN ha intrapreso diverse iniziative. In particolare, per agevolare i fornitori nella preparazione della documentazione di progetto è stato migliorato il modello riportante i requisiti per la predisposizione dell'ambiente di test. Tale attività, infatti, è onere dei fornitori, i quali sono tenuti a garantire la dovuta collaborazione con il CVCN al fine di allestire un ambiente di test adeguatamente rappresentativo della realtà di esercizio. Inoltre, sono state incrementate le occasioni di interazione con i soggetti e con i fornitori, prevedendo una riunione di avvio lavori che consente di chiarire a tutti gli *stakeholder* le caratteristiche e i requisiti operativi della piattaforma per il test. Tutto ciò ha consentito una compressione dei tempi medi per la preparazione all'esecuzione dei test di circa 1/3 rispetto al 2024.

FOCUS

Ambiente di test

Le attività di valutazione degli oggetti della fornitura vengono eseguite in un ambiente di test che deve essere rappresentativo dell'ambiente di esercizio del soggetto, ma separato da quest'ultimo: tale requisito è stato imposto per evitare il rischio di inserire nell'ambiente di esercizio un oggetto non ancora sottoposto a test di sicurezza e, quindi, con potenziali vulnerabilità o configurazioni carenti, oltre che per evitare che le attività di test possano interferire con la normale erogazione dei servizi del soggetto.

Il compito dell'allestimento dell'ambiente di test spetta al fornitore, ma – a seconda del luogo in cui l'ambiente è ubicato – tale attività viene svolta in modalità differenti. L'ambiente di test viene, infatti, preferibilmente allestito presso i laboratori del CVCN, dove i valutatori hanno il grado massimo di libertà di accesso all'oggetto e la completa disponibilità della strumentazione. In alcune circostanze, però, l'ambiente di test può essere allestito presso il fornitore, il soggetto o il produttore stesso, principalmente in relazione alla tipologia dell'oggetto della fornitura (dimensioni, caratteristiche fisiche, eccessive dipendenze da altri servizi/prodotti non replicabili, erogazione in cloud in modalità PaaS o SaaS, ecc.). Similmente, quando le attività di test vengono affidate a un laboratorio accreditato di prova (LAP), l'ambiente viene preferibilmente allestito presso il LAP stesso.

Per quanto riguarda l'attività di esecuzione dei test (fase 3), il CVCN ha effettuato 29 test di componenti, identificando un totale di 38 vulnerabilità di tipo *zero-day*, di cui 28 con gravità alta o critica, secondo la classificazione internazionale di riferimento CVSS. Come mostrato in Figura 4, a seguito della comunicazione del CVCN al produttore, per 21 vulnerabilità sono in corso le interlocuzioni con il produttore, 11 sono state prese in carico ai fini della risoluzione, mentre 6 sono già state corrette e, conseguentemente, pubblicate come CVE (ossia il codice univoco assegnato a ciascuna specifica vulnerabilità).

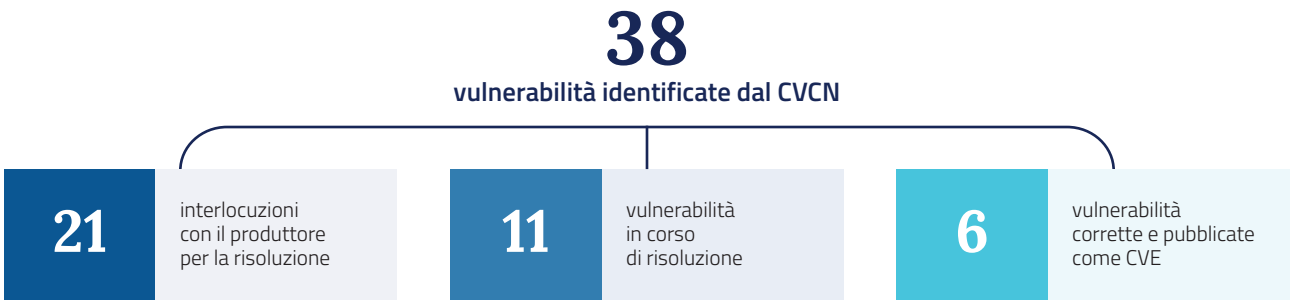


Figura 4 – Stato di risoluzione delle vulnerabilità *zero-day* identificate dal CVCN

4.1.1 La rete dei laboratori a sostegno del PSNC

Il 2025 ha visto il consolidamento della rete dei Laboratori di prova grazie alla conclusione di 9 procedimenti di accreditamento di cui 1 di livello medio-alto, 2 medio-basso e 6 basso. Complessivamente ciò porta il totale dei LAP che possono supportare il CVCN nelle proprie attività di scrutinio tecnologico a 14, distribuiti su tutti i livelli di severità dei test che possono eseguire. Inoltre, a fine 2025 erano attivi ulteriori 7 procedimenti di accreditamento.

Figura 5 – LAP accreditati: una panoramica

Per quanto riguarda gli esami del personale dei LAP, nel 2025 sono state condotte 20 sessioni, che hanno permesso di qualificare un totale di 36 nuovi valutatori (VLAP), distribuiti tra i vari livelli (Figura 6).

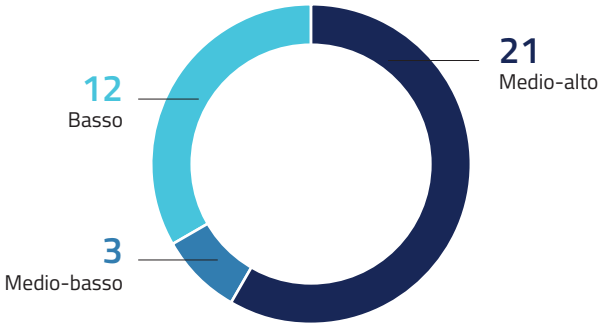


Figura 6 – VLAP valutati idonei nel 2025

Quanto alla collaborazione con i Centri di valutazione (CV) dei Ministeri dell'interno e della difesa, nel mese di gennaio il CVCN ha organizzato una sessione formativa pratica della durata di 5 giorni. Il personale di entrambi i CV si è potuto confrontare con processi di valutazione presentati dal CVCN, ispirati a scenari reali. Ciò ha consentito di stimolare il coordinamento e lo scambio di esperienze tra i due CV e il CVCN al fine di rendere le rispettive modalità di valutazione sempre più omogenee.

A fine anno si è tenuto un seminario dedicato principalmente ai LAP, nel corso del quale sono state illustrate le prospettive di sviluppo anche in aggiunta delle attività delegate dal CVCN. Il processo di accreditamento condotto dal CVCN, unitamente al raccordo tra l'ACN e l'Ente italiano di accreditamento Accredia, rende, infatti, i LAP soggetti naturalmente predisposti a operare in contesti che prevedono l'esecuzione di test di sicurezza (inclusi quelli previsti da *Cybersecurity Act*, *Cyber Resilience Act* ed eIDAS). L'evento ha riscosso un buon interesse da parte dei diversi *stakeholder*, provenienti sia dai LAP che dai CV. Questo, oltre a iniziative del CVCN orientate a un più frequente e strutturato ingaggio dei LAP, dovrebbe consentire ai laboratori di adottare piani di business sostenibili.

4.2 EVOLUZIONE E ATTIVITÀ DELL'OCSI

Per garantire uno spazio digitale più sicuro, uno strumento cruciale è rappresentato dalle certificazioni di sicurezza informatica che, in Italia, vengono rilasciate dall'OCSI sulla base di un accurato processo di valutazione.

Il 2025 è stato un anno di passaggio dallo Schema nazionale di certificazione (ex DPCM 30 ottobre 2003) alla piena operatività del sistema europeo EUCC che, adottando i *Common Criteria*, consente una certificazione uniforme a livello UE per i prodotti ICT. L'EUCC, l'unico schema ad oggi adottato ai sensi del *Cybersecurity Act*, è entrato, infatti, in vigore il 27 febbraio 2025 e, a partire dalla stessa data del 2026, è possibile emettere solo tali certificati. In questo intervallo vengono portate a termine le certificazioni già precedentemente avviate ai sensi dello Schema nazionale. I certificati emessi dall'OCSI nell'ambito dell'EUCC, oltre a essere riconosciuti in tutta l'Unione europea, sono mutuamente riconosciuti a livello internazionale in base ai termini dell'accordo CCRA (*Common Criteria Recognition Arrangement*) dai Paesi aderenti.

L'EUCC ridefinisce il ruolo dell'OCSI, prevedendo compiti anche per Accredia, in quanto ente nazionale di accreditamento e per l'ACN quale Autorità nazionale di certificazione della cybersicurezza. Il nuovo sistema si articola su più adempimenti: Accredia è responsabile per l'accreditamento dei laboratori di prova e degli organismi di certificazione (in Italia solo l'OCSI), l'ACN per l'autorizzazione degli stessi, mentre l'OCSI abilita i laboratori a operare come Laboratori per la valutazione della sicurezza (LVS). Per chiarire i relativi ruoli e processi, a febbraio sono state adottate specifiche Linee guida, con cui l'Agenzia ha definito il quadro di riferimento per le attività dell'Autorità nazionale di certificazione della cybersicurezza, dell'OCSI e degli LVS.

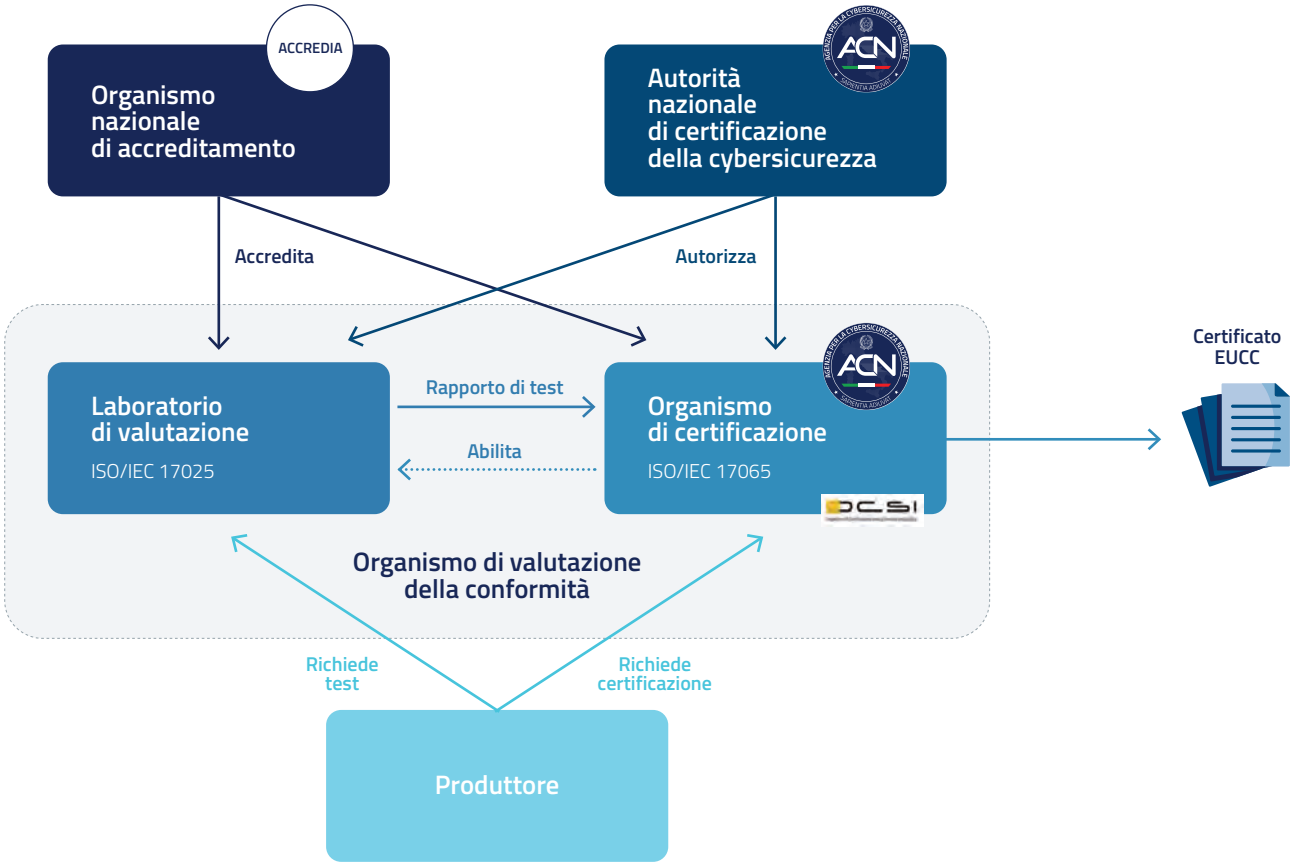


Figura 7 – Soggetti e ruoli in ambito EUCC

Un primo passo per mettere a terra il nuovo impianto è stato fatto a luglio quando l'OCSI ha ottenuto l'accreditamento da parte di Accredia quale organismo di certificazione rispetto alla norma internazionale ISO/IEC 17065. Questo consente all'Organismo nazionale di rilasciare certificati EUCC. L'accreditamento dell'OCSI è stato notificato alla Commissione europea dalla stessa ACN, alla luce del suo ruolo di Autorità nazionale di certificazione della cybersicurezza. Inoltre, a dicembre è stato abilitato dall'OCSI anche il primo LVS, preventivamente accreditato da Accredia come laboratorio di prova ai sensi della norma ISO/IEC 17025. Ciò permetterà all'OCSI di emettere i primi certificati EUCC già dall'inizio del 2026, in concomitanza con la dismissione del previgente Schema di certificazione nazionale dal 27 febbraio 2026.

FOCUS

Attività internazionali dell'OCSI

In linea con gli anni precedenti, l'OCSI ha continuato a portare avanti le attività di cooperazione in ambito europeo in quanto parte della National Cybersecurity Certification Authority (NCCA) italiana nei comitati e gruppi di lavoro della Commissione europea, tra cui lo European Cybersecurity Certification Group (ECCG) e lo European Cybersecurity Certification Committee. In particolare, è stato impegnato nella revisione dell'EUCC e nella definizione delle politiche per la certificazione della cybersicurezza europee.
Inoltre, in ambito internazionale, in seno all'accordo di mutuo riconoscimento CCRA, che comprende 36 agenzie governative di Paesi di tutto il mondo, l'OCSI ha partecipato agli incontri periodici, fornendo contributi tecnico-scientifici alla realizzazione della conferenza internazionale annuale Common Criteria, nonché annunciando che l'edizione del settembre 2026 sarà ospitata a Roma con il supporto dell'ACN. La conferenza rappresenta l'evento di maggior rilievo nel campo della certificazione della cybersicurezza, raccogliendo i massimi esperti a livello internazionale del settore provenienti da laboratori, aziende produttrici che ricorrono alla certificazione e agenzie governative con il ruolo di autorità di vigilanza e di organismi di certificazione.

L'OCSI ha avviato nel 2025 gli ultimi 16 processi di certificazione basati su tale Schema ed emesso 10 certificati di cybersicurezza riferiti a varie categorie di apparati: dispositivi di rete, dispositivi di creazione di firma, applicativi per la gestione di dati, sistemi operativi. I rimanenti processi di certificazione in corso a fine 2025 si trovavano nelle fasi conclusive. È stata, inoltre, avviata l'attività di certificazione per un primo prodotto ICT basata sull'EUCC. Per alcuni processi di certificazione avviati in base allo Schema nazionale è ipotizzabile la riconversione in nuovi processi EUCC nel corso del 2026.

Si evidenzia che circa il 50% delle richieste di certificazione di prodotti ricevute dall'OCSI provengono da aziende produttrici di apparati ICT che hanno sede principale negli Stati Uniti, quali IBM e HP, mentre il restante 50% proviene da Stati membri dell'UE e da altri Paesi. Ciò attesta il riconoscimento dell'OCSI quale organismo operativo a livello internazionale non solo dalle altre agenzie governative aderenti al CCRA, ma anche dal mercato dei principali soggetti economici del settore.

Con riferimento al compito assegnato all'OCSI di organismo notificato per l'accertamento di conformità di dispositivi di creazione di firma/sigillo qualificata rispetto ai requisiti del Regolamento eIDAS, sono stati emessi 4 accertamenti di tali dispositivi.

L'OCSI opererà, in prospettiva, anche come organismo di certificazione rispetto alle soluzioni di portafoglio digitale. Nel corso del 2025 sono proseguite le attività normative dedicate alla creazione del portafoglio europeo di identità digitale (*European Digital Identity Wallet*-EUDI Wallet) istituito dal Regolamento eIDAS2. Entro la fine del 2026, ciascuno Stato membro dovrà rendere disponibile una soluzione nazionale di portafoglio, uno strumento che metterà l'identità digitale del cittadino sotto il proprio controllo esclusivo. Ogni versione del portafoglio, in conformità con i requisiti europei, sarà interoperabile con i servizi offerti da tutti gli Stati membri dell'Unione europea.

Dall'entrata in vigore di eIDAS2, l'ACN ha contribuito, in coordinamento con il Dipartimento per la trasformazione digitale (DTD) della Presidenza del Consiglio dei mi-

nistri e con tutti gli altri attori coinvolti nel progetto, alla revisione dei nuovi atti di esecuzione della Commissione europea in attuazione del citato Regolamento. Ha fornito, in particolare, il proprio apporto ai lavori per definire un sistema nazionale di certificazione per EUDI Wallet, dal momento che ogni soluzione di portafoglio dovrà essere obbligatoriamente certificata a un livello di garanzia "elevato", come definito da eIDAS2.

4.3 LE ATTIVITÀ DI VERIFICA E ISPEZIONE

L'Agenzia svolge attività di verifica e ispezione per gli adempimenti di cybersicurezza attribuiti dalla normativa vigente. Si tratta di processi strutturati tesi a valutare, testare e garantire la sicurezza delle infrastrutture ICT, dei dati e dei sistemi informatici di soggetti, pubblici e privati, sottoposti a vigilanza, identificando vulnerabilità, misurando il grado di rischio cyber e constatandone la conformità alle normative di riferimento.

Ciascun procedimento parte da una fase di verifica documentale, ivi incluso l'eventuale controllo delle evidenze preliminari; a ciò fa seguito l'attività ispettiva volta sia a riscontrare le evidenze acquisite in sede di verifica, sia a effettuare analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto e di diritto ritenuti comunque necessari.

In tale contesto, l'attività dei gruppi ispettivi ha rivestito un ruolo cruciale per assicurare efficacia alla vigilanza che l'Agenzia è chiamata a operare al fine di accertare il livello di conformità alle diverse disposizioni. In particolare, le ispezioni vengono effettuate in tre ambiti principali: la rispondenza ai requisiti per l'accreditamento dei laboratori di prova, le misure di sicurezza richieste per la qualificazione dei servizi *cloud* per la PA, nonché il corretto impiego dei beni ICT da parte dei soggetti del Perimetro.

Al fine di stabilire una struttura logica e coerente per tutte le procedure, di consentire una gestione – documentale e operativa – efficace ed efficiente, nonché di offrire garanzie di imparzialità, indipendenza e riservatezza rispetto alle attività ispettive, l'ACN ha continuato a sviluppare un sistema di gestione della qualità in conformità a quanto previsto per gli organismi di ispezione (UNI CEI EN ISO/IEC 17020). In tali attività è stato, inoltre, indispensabile tenere in debita considerazione la complessità delle componenti ICT della specifica infrastruttura in esame, così come la sensibilità dei dati e delle informazioni oggetto di trattamento e la criticità dei processi di sicurezza gestiti.

Nel corso del 2025 si segnala un sostanziale incremento delle attività di verifica e ispezione nei confronti dei LAP, propedeutiche al loro accreditamento: sono state, infatti, esaminate le documentazioni presentate da 15 laboratori e condotte 15 attività ispettive. Inoltre, sono state avviate 2 attività ispettive nei confronti di soggetti appartenenti al PSNC e 1 su un *cloud service provider* nell'ambito della qualificazione dei servizi *cloud* per la PA.

Le ispezioni svolte in ambito PSNC e *cloud* si sono focalizzate sulla gestione degli accessi e delle identità, sulla sicurezza dell'infrastruttura e delle sue componenti software, sull'analisi delle vulnerabilità, sul livello di aggiornamento delle configurazioni, sulle caratteristiche dei sistemi di cifratura, nonché sui processi che garantiscono la continuità operativa e un livello di resilienza adeguato al rischio.

Un ulteriore focus in tale ambito è stato anche determinato dall'incremento dei compiti in capo all'ACN a seguito dell'entrata in vigore dello schema di certificazione europeo EUCC, che richiede l'espletamento di nuove attività come l'autorizzazione degli organismi di valutazione della conformità.

4.4 *CLOUD* PER LA PA

L'Agenzia è impegnata nel supportare il più ampio processo di digitalizzazione della Pubblica Amministrazione basata sulla transizione alle tecnologie *cloud*, definendo regole e meccanismi per guidare i relativi aspetti di cybersicurezza, cristallizzati nel Regolamento *cloud* adottato dall'ACN nel 2024. Partendo dalla classificazione del dato o del servizio supportato, operata dall'Amministrazione in quanto proprietaria del dato e del relativo processo, è oggi possibile graduare gli oneri e le garanzie rispetto all'effettivo rischio, permettendo altresì di bilanciare opportunamente i requisiti in tema di sovranità, di presidio tecnologico e operativo, oltre agli aspetti di sicurezza informatica e resilienza, rispetto a quelli di economicità ed efficienza.

Il 2025 ha rappresentato l'anno di piena maturità del Regolamento *cloud* e un banco di prova per confermarne l'effettivo allineamento con l'attuale scenario tecnologico. Difatti, nell'anno trascorso, sono divenute efficaci alcune misure, tra cui:

- il censimento continuativo dei servizi *cloud* e delle infrastrutture digitali (su cui questi si basano) di cui fanno uso le PA; il censimento permette di avere una mappa dinamica dei servizi *cloud* fruiti a livello nazionale, consentendo di intercettare i profili di rischio per le PA che li utilizzano e di orientare le azioni correttive;
- l'obbligo di adeguamento anche per le infrastrutture di *housing*, ossia quelle strutture che ospitano fisicamente i *server* destinati all'erogazione dei servizi *cloud*; si tratta dell'ultimo tassello per il presidio dell'intera filiera di fornitura del servizio *cloud* (la c.d. catena di qualificazione) che include ora anche le infrastrutture utilizzate quale fondamenta base dei *data center*, che contribuiscono a garantire almeno i requisiti relativi alla sicurezza fisica e agli aspetti ambientali ed energetici, tutti ambiti che ricadono sotto il Regolamento;
- i requisiti relativi principalmente agli aspetti di sicurezza informatica, la cui applicazione era stata differita per garantire il necessario allineamento dei sistemi; si tratta, ad esempio, della previsione di misure di contrasto ad attacchi come quelli di tipo DDoS, sia a livello di infrastrutture di rete, sia sul piano applicativo.

In tale contesto, l'Agenzia è stata impegnata a portare avanti le varie attività richieste per i procedimenti di qualificazione dei servizi *cloud* e di adeguamento delle infrastrutture digitali che consentono l'erogazione di tali servizi. Ciò è funzionale a garantire che tutte le PA possano effettuare la transizione al *cloud* su soluzioni sicure e affidabili. Nel corso dell'anno, a partire dalle istanze dei soggetti privati interessati, l'ACN ha qualificato oltre 1.700 servizi *cloud* (tra quelli di base, ovvero *Infrastructure-as-a-Service* o IaaS, piattaforme *Platform-as-a-Service* o PaaS, e quelli direttamente applicativi *Software-as-a-Service* o SaaS) e adeguato più di 130 infrastrutture digitali (Figura 8). Così facendo, il Catalogo delle infrastrutture digitali e dei servizi *cloud* è stato popolato con i principali applicativi, consentendo una più ampia copertura delle esigenze del mercato pubblico, nonché abilitando le PA a effettuare una migliore selezione del fornitore.

Inoltre, l'ACN ha supportato le PA per l'adeguamento ai livelli minimi di oltre 50 nuove piattaforme gestite direttamente da soggetti di diritto pubblico (c.d. *on premises*), tra servizi *cloud* e infrastrutture digitali. Per la maggior parte di tali piattaforme, in virtù degli specifici profili di rischio, sono state altresì eseguite onerose attività di monitoraggio ex post, concluse con specifiche prescrizioni e indicazioni per il necessario incremento di maturità.

Infine, tra le attività svolte anche in relazione alla sempre maggiore convergenza tecnologica tra sistemi di intelligenza artificiale e tecnologie *cloud*, l'Agenzia è impegnata nella valutazione dei servizi di IA erogati in *cloud* per la Pubblica Amministrazione (nell'ambito del paradigma *AI-as-a-Service*) al fine di valutare la conformità di tali servizi alle prescrizioni del Regolamento *cloud*.

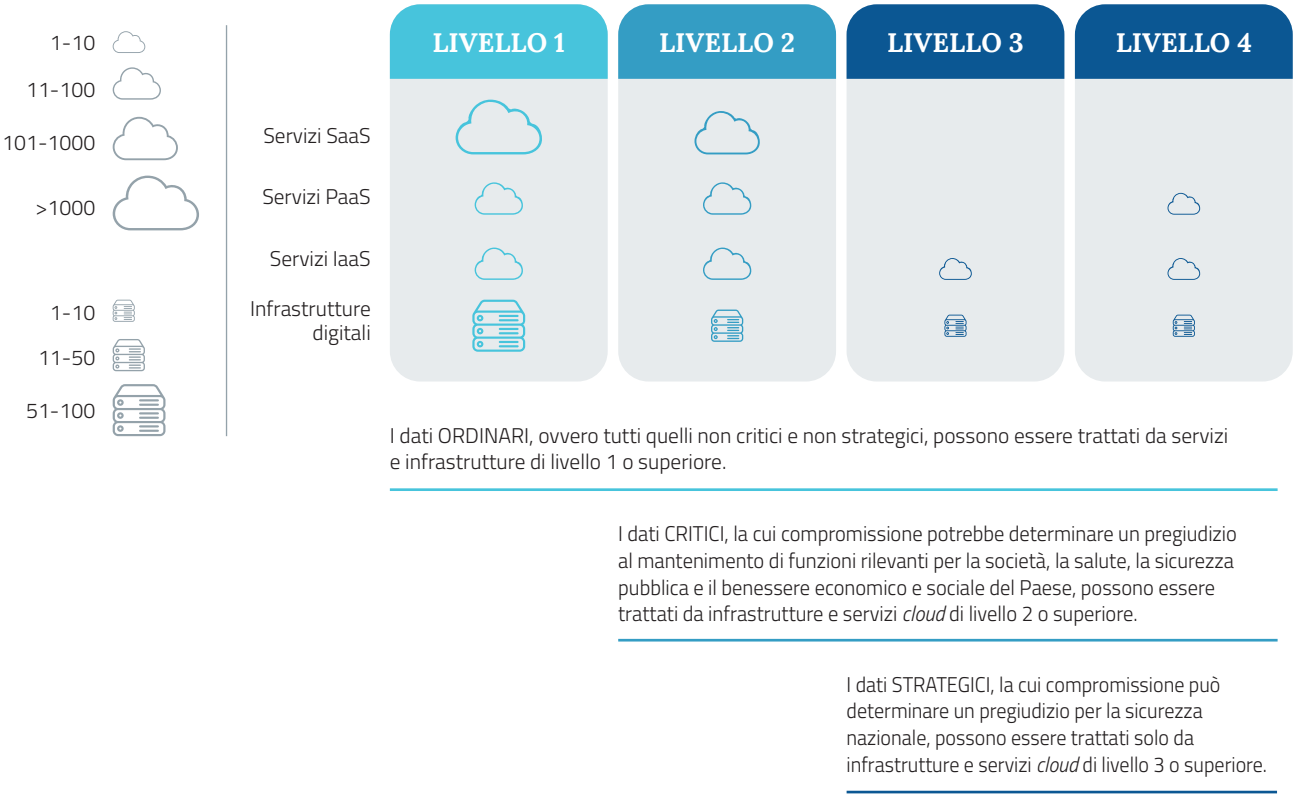


Figura 8 – Servizi *cloud* qualificati e infrastrutture digitali adeguate nel 2025

Cloud e innovazione digitale del Paese

Gli sforzi profusi dall'ACN nel mettere in sicurezza le infrastrutture e i servizi *cloud* per la PA contribuiscono a gettare le basi per supportare il Paese nel processo di trasformazione digitale. L'Agenzia sta, infatti, contribuendo attivamente a specifiche progettualità di digitalizzazione a livello nazionale, in particolare:

- al progetto relativo all'Ecosistema dei dati sanitari, il cui avvio è previsto nel 2026. In tale ambito, l'ACN sta contribuendo alla definizione delle misure di sicurezza della piattaforma, anche in relazione alla possibilità di realizzare un'architettura federata a livello regionale;
- alle piattaforme digitali utilizzate per l'approvvigionamento pubblico (c.d. Piattaforma di approvvigionamento digitale), che permetteranno a ciascuna PA la gestione digitale di tutte le fasi di un appalto, garantendo anche l'interoperabilità con le infrastrutture nazionali centralizzate. A tal fine, l'Agenzia ha curato la definizione delle regole di cybersicurezza delle piattaforme;
- alle iniziative volte all'erogazione dei finanziamenti (previsti dal Decreto ministeriale MIMIT del 18 luglio 2025) a sostegno delle PMI italiane per dotarle di soluzioni tecnologiche di *cybersecurity* e *cloud computing*, al fine di promuoverne la digitalizzazione sicura. Per accedere a tale finanziamento è possibile, tra le altre cose, avvalersi di una soluzione *cloud* qualificata dall'ACN.

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

Al fine di salvaguardare gli assetti delle imprese operanti in ambiti ritenuti strategici e di interesse nazionale, sono attribuiti al Governo poteri speciali, esercitabili previe approfondite procedure di verifica e valutazione che includono diversi soggetti istituzionali. Tra questi rientra anche l'ACN, chiamata a fornire il proprio contributo tecnico per tutte le procedure relative alle tecnologie 5G (ex art. 1-bis del D.L. n. 21/2012) e, di volta in volta, per quelle riguardanti i settori della difesa e della sicurezza nazionale e gli ambiti ritenuti di rilevanza strategica nei settori dell'energia, dei trasporti, delle comunicazioni (artt. 1 e 2 del medesimo decreto-legge).

Nel 2025 si è registrato un sensibile incremento nel numero di notifiche presentate ai sensi degli artt. 1 e 2 rispetto alle quali l'ACN ha fornito un contributo (370 delle 877 notifiche totali), marcando un aumento, rispetto all'anno precedente, del 25%.

Il contributo apportato dall'ACN è consistito nella predisposizione sia di approfondimenti istruttori, che hanno riguardato all'incirca il 30% delle notifiche analizzate, sia di pareri, contribuendo anche alla definizione di prescrizioni nel 4% circa dei casi trattati, nonché di motivazioni a supporto dei provvedimenti di veto, che hanno interessato 2 operazioni. Con riferimento alle prenotifiche, l'ACN ha fornito un contributo sul 40% delle 178 prenotifiche presentate.

Relativamente alle notifiche artt. 1 e 2 per cui l'ACN ha fornito supporto, l'esito del procedimento è quello sintetizzato in Figura 9.

Si segnalano 52 notifiche che hanno interessato profili di cybersicurezza nei settori compresi dagli artt. 1 e 2. Queste si sono concluse, in 19 casi, con la non applicabilità del *Golden Power* e, in 32 casi, con il non esercizio dei poteri speciali, mentre un procedimento si è concluso con l'esercizio dei poteri speciali attraverso l'imposizione di prescrizioni. In tale ambito, 12 casi hanno richiesto un approfondimento istruttorio attraverso quesiti a risposta scritta e/o audizioni delle società coinvolte e di soggetti terzi.

Il 2025 ha registrato anche un incremento delle notifiche che hanno interessato il settore dell'intelligenza artificiale; in valore assoluto il numero di notifiche si è attestato su 85, e in 2 circostanze il relativo procedimento si è concluso con l'esercizio dei poteri speciali attraverso l'imposizione di prescrizioni.

Il settore delle comunicazioni elettroniche si è attestato in valore assoluto a 56 notifiche, e in un caso sono stati esercitati i poteri speciali attraverso l'imposizione di prescrizioni.

Per quanto riguarda le attività svolte nel contesto dell'art. 1-bis del D.L. n. 21/2012, concernenti le valutazioni dei piani di approvvigionamento di sistemi e apparati in tecnologia 5G, l'ACN ha effettuato l'analisi delle 25 notifiche pervenute nel corso del 2025, che comprendevano sia le notifiche dei piani annuali (18) che i loro aggiornamenti (7). Infine, con riferimento alle attività di monitoraggio previste per la verifica dell'ottemperanza alle prescrizioni imposte in sede di approvazione dei piani annuali, l'ACN, quale membro del Comitato preposto, ha ricevuto e analizzato 39 relazioni di ottemperanza.

Le due attività, di analisi dei piani annuali e di monitoraggio delle prescrizioni, sono state condotte in modo

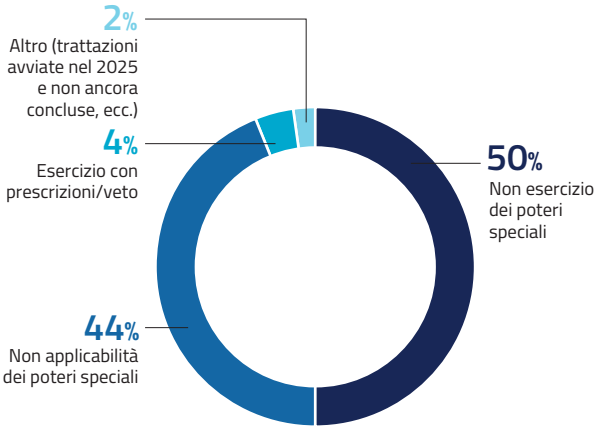


Figura 9 – Esito dei procedimenti *Golden Power* (artt. 1 e 2) cui l'ACN ha contribuito nel 2025

coordinato, secondo un approccio che ha permesso di verificare, attraverso l'analisi dei piani afferenti al periodo 2025-2026, il rispetto delle prescrizioni riferite allo sviluppo della rete che erano state adottate in occasione dell'approvazione dei piani per il periodo 2024-2025, permettendo altresì di avere una visione unitaria dell'evoluzione della rete.

Con riferimento a quest'ultimo aspetto, l'attività di monitoraggio si è concentrata, in particolare, su valutazioni che afferiscono alle misure strategiche del *Toolbox* europeo sul 5G, al quale si sono ispirati i decreti di approvazione dei piani, soprattutto con riferimento alle misure sulla diversificazione dei fornitori nella componente di accesso radio.

L'attività di monitoraggio ha avuto anche un carattere più tecnico, avente ad oggetto la valutazione degli aspetti di sicurezza dei componenti installati nelle reti 5G, sulla base sia dell'impiego di componenti certificati, sia dell'analisi dei report dei test di sicurezza svolti dagli operatori su specifici sistemi critici.

4.6 LA CRITTOGRAFIA

Nel corso del 2025 l'Agenzia, anche in relazione alla previsione della legge n. 90/2024 sull'istituzione del Centro nazionale di crittografia, ha continuato a orientare la propria azione in materia di crittografia secondo le linee descritte nel box.

Attività ACN in ambito crittografia

Elaborazione di linee guida contenenti informazioni descrittive sugli standard crittografici e raccomandazioni tecniche su quali schemi adottare con i rispettivi parametri di sicurezza.

Supporto nelle attività di valutazione di sicurezza, scrutinio tecnologico e certificazione, in ambito crittografico, di sistemi e prodotti e che fanno uso di soluzioni crittografiche.

Valutazione della sicurezza dei sistemi crittografici di nuova concezione, ovvero analisi di cifrari non standardizzati e nuove minacce e studio di soluzioni derivanti da progetti universitari, centri di ricerca e soggetti privati.

Transizione alla crittografia post-quantum tramite analisi di sicurezza dei nuovi schemi resistenti ai computer quantistici e sviluppo di una strategia nazionale per la transizione.

Collaborazioni nazionali e internazionali per la definizione di standard, attività di regolazione, valutazione della sicurezza e certificazione dei sistemi crittografici.

Promozione di attività per la valorizzazione della ricerca inerente a nuove tecnologie crittografiche nazionali, anche attraverso la collaborazione col mondo accademico.

Rafforzamento dell'utilizzo consapevole della crittografia come strumento di cybersicurezza, anche tramite eventi di formazione e divulgazione.

La promozione dell'uso della crittografia come strumento di cybersicurezza rientra tra i compiti chiave dell'Agenzia in ambito nazionale, che porta avanti in collaborazione con enti universitari e di ricerca, con altre istituzioni interessate e con il mondo industriale. Rilevante la collaborazione con l'associazione di promozione sociale De Componendis Cifris e con l'Università degli studi Roma Tre per l'organizzazione dell'evento CIFRIS25, annuale conferenza nazionale di crittografia svoltasi a settembre, con l'intento di divulgare la cultura crittografica e il suo utilizzo corretto riunendo, nella stessa sede, esperti del mondo accademico, istituzionale e industriale.

L'ACN nel 2025 ha continuato, inoltre, ad arricchire la serie "Linee guida funzioni crittografiche", ideata per fornire dettagli tecnici e raccomandazioni sugli schemi crittografici e i relativi parametri, da adottare fin dalle fasi di progettazione di reti, applicazioni e servizi. Questa tipologia di iniziative testimonia l'impegno costante dell'Agenzia nel rafforzare la cultura crittografica a livello nazionale, favorendo la diffusione di competenze specialistiche e consolidando un ecosistema di interlocutori qualificati in grado di supportare le esigenze di sicurezza del Paese.

In particolare, sono state pubblicate 2 nuove Linee guida, a copertura di ulteriori aspetti della crittografia:

- Cifratura Autenticata: una tecnica crittografica che combina in un unico meccanismo la cifratura e l'autenticazione del messaggio, garantendo sia la confidenzialità che l'integrità e l'autenticità dei dati trasmessi;
- *Transport Layer Security* (TLS): un protocollo crittografico che sta alla base della sicurezza della rete Internet moderna, in quanto ideato per assicurare la sicurezza di tutte le comunicazioni di rete, siano esse usate da infrastrutture critiche, istituzioni finanziarie o dai cittadini, fornendo confidenzialità, integrità e autenticazione.

L'ACN è attiva, infine, sul fronte delle tecnologie quantistiche. Queste, infatti, rappresentano un cambiamento di paradigma fondamentale per l'informatica, la crittografia e i modelli scientifici, che hanno visto un'importante accelerazione negli ultimi anni e, nei decenni a venire, avranno notevoli ripercussioni in tutti i settori. I computer quantistici consentono, oggi solo a livello teorico, di eseguire calcoli complessi che sono in grado di compromettere la crittografia moderna, in particolar modo i sistemi crittografici a chiave pubblica, largamente utilizzati nella sicurezza delle comunicazioni, nelle transazioni finanziarie, per gli scambi di chiavi segrete oltre alla creazione e verifica di firme digitali. Sebbene i computer quantistici attuali non siano ancora una minaccia concreta, la comunità internazionale della cybersicurezza è concorde nel valutare che lo possano diventare entro 10-15 anni. La preparazione alla minaccia quantistica è, quindi, da considerarsi come un aspetto integrante della gestione del rischio delle minacce cyber a lungo termine.

Per arginare tale minaccia, la comunità scientifica ha elaborato delle soluzioni alternative ai moderni sistemi crittografici a chiave pubblica: la distribuzione quantistica delle chiavi (QKD) e la crittografia post-quantum (PQC).

La QKD sfrutta direttamente le proprietà della meccanica quantistica per stabilire comunicazioni sicure indipendentemente dalla potenza di calcolo dell'avversario. Tali soluzioni, tuttavia, presentano numerose limitazioni d'uso e non sostituiscono diverse funzioni di crittografia a chiave pubblica, come la firma digitale.

La PQC è una branca della crittografia che prevede l'impiego di schemi crittografici progettati per resistere ad attacchi quantistici, ma implementabili sui sistemi attuali.

Considerate le gravi conseguenze che lo sviluppo del calcolo quantistico avrebbe sulla crittografia moderna e a causa della minaccia concreta di scenari come lo "*store now, decrypt later*", anche in considerazione dei lunghi periodi necessari per convertire sistemi complessi, effettuare una rapida transizione ai nuovi sistemi di crittografia è una priorità a livello mondiale.

A tal fine, in ambito UE si sta lavorando a una tabella di marcia coordinata per la transizione alla crittografia post-quantum. L'ACN contribuisce al *Work Stream on Post-Quantum Cryptography* del Gruppo di cooperazione NIS (vedasi Capitolo 6), che nel 2025 ha pubblicato un primo documento contenente un calendario per la migrazione e un elenco delle misure da includere nelle tabelle di marcia nazionali PQC di ciascuno Stato membro (Figura 10).

Figura 10 – Tappe della tabella di marcia per la transizione alla PQC concordata dal Gruppo di cooperazione NIS

Questo tipo di iniziative permetteranno all'Italia di definire un Piano di transizione nazionale, garantendo un processo che rispetti i tempi prestabiliti e che avvenga in modo efficace e coordinato.

In tale contesto, rileva la redazione della Strategia italiana per le tecnologie quantistiche, pubblicata a settembre 2025. La Strategia è il frutto di un lavoro condiviso coordinato dal MUR con il contributo del MIMIT, del Ministero della difesa, del MAECI, del DTD e dell'Agenzia. Il documento inquadra l'attuale panorama italiano e internazionale e identifica le sfide e gli obiettivi del nostro Paese, definendo azioni mirate a potenziare la ricerca e l'innovazione, migliorare l'accesso alle infrastrutture e stimolare gli investimenti privati.

5

Programmi di investimento a sostegno della cybersicurezza

Nel contesto attuale, caratterizzato da una progressiva digitalizzazione dei servizi e da una crescente interconnessione delle infrastrutture informative, la cybersicurezza conferma la sua valenza strategica per l'azione della Pubblica Amministrazione e del settore privato.

L'evoluzione – qualitativa e quantitativa – delle minacce cibernetiche, unitamente all'ampliamento della superficie di attacco derivante dall'adozione di piattaforme digitali, impone un adeguamento strutturale delle politiche di protezione di *asset* informativi e dei servizi erogati nei confronti di cittadini e imprese.

In tale quadro, la definizione di programmi di investimento a sostegno della cybersicurezza non può essere limitata a interventi contingenti o esclusivamente tecnologici, bensì deve configurarsi come un processo organico, programmato e coerente, di pianificazione strategica, finalizzato alla gestione sistemica del rischio cyber, in modo da consentire il rafforzamento delle capacità di prevenzione, rilevazione e risposta agli incidenti, nonché la continuità operativa delle funzioni fondamentali del sistema Paese.

L'obiettivo di rendere l'Italia più sicura sotto il profilo cyber è stato portato avanti dall'Agenzia per la cybersicurezza nazionale anche nel 2025 attraverso programmi di investimento che hanno seguito quattro principali direttrici: consolidare le capacità cyber della Pubblica Amministrazione, sostenere l'ecosistema della ricerca e dell'innovazione anche per favorire il trasferimento tecnologico, assicurare il continuo miglioramento dei servizi cyber nazionali e gettare le basi per il miglior utilizzo delle tecnologie, anche emergenti, grazie alla gestione di finanziamenti europei.

5.1 PROGRAMMI PER LA PUBBLICA AMMINISTRAZIONE

L'Agenzia è particolarmente impegnata, fin dalla sua istituzione, per sostenere le capacità di cybersicurezza della PA, al fine di rafforzarne la postura cyber e renderla sempre più in grado di gestire le minacce cibernetiche. Si tratta di un obiettivo cruciale considerando la rilevanza nell'ecosistema cyber nazionale della Pubblica Amministrazione, che gestisce servizi di pubblica utilità, spesso essenziali, e che tratta informazioni appartenenti a tutti i cittadini.

Come riportato nelle precedenti Relazioni al Parlamento, l'Investimento 1.5 "Cybersecurity" della Missione 1 – Componente 1 – Asse 1 del PNRR è stato lo strumento per una crescita strutturata della resilienza cyber del Paese, con interventi strategici e mirati, in particolare a sostegno della Pubblica Amministrazione. L'efficace azione dell'ACN, in qualità di soggetto attuatore dell'Investimento, ha permesso, entro il 2024, di conseguire tutti gli obiettivi (3 *milestone* e 1 *target*) e di impegnare quasi per intero i fondi disponibili.

A dicembre 2025 risultavano liquidati dall'Agenzia circa 254 milioni di euro sui 623 milioni di euro disponibili (circa il 41%) corrisposti sia per l'attuazione diretta di interventi volti alla costruzione ed evoluzione delle capacità dell'ACN e per la realizzazione dei servizi cyber nazionali (interventi c.d. a titolarità, per un totale di circa 125 milioni di euro), sia per il ristoro delle attività finanziate a favore di soggetti terzi (interventi c.d. a regia, per un totale di circa 129 milioni di euro). Tale avanzamento risulta coerente con le previsioni di spesa per il 2026 e, in particolare, in linea con l'estensione, dal 31 dicembre 2025 al 31 marzo 2026, dei termini di conclusione dei progetti in corso nell'ambito di interventi a regia, in modo da fornire a tutti i soggetti finanziati la più ampia possibilità di portare a conclusione e rendicontare le attività effettuate.

L'obiettivo di potenziare le capacità cyber della PA è stato, a partire dal 2022, uno dei principali perseguiti dall'Agenzia nell'ambito del PNRR attraverso una serie di attività di cui le Amministrazioni hanno beneficiato per realizzare progetti legati al miglioramento della loro

postura di sicurezza cibernetica, al fine di aumentare il loro livello di maturità cyber, ridurre le vulnerabilità e rendere le organizzazioni più resilienti, pronte a prevenire, rilevare e gestire le minacce in modo efficace.

In particolare, nel 2025 sono state portate avanti le progettualità finanziate attraverso gli Avvisi pubblici 7/2023 e 8/2024, indirizzati al potenziamento della resilienza cyber, rispettivamente di Amministrazioni centrali (Organi costituzionali o di rilievo costituzionale, Ministeri, Agenzie fiscali, Enti di regolazione dell'attività economica, Autorità amministrative indipendenti ed Enti a struttura associativa) e di Amministrazioni locali (Comuni con una popolazione superiore a 100.000 abitanti, 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).

Avviso 7/2023

L'Avviso 7/2023 ha garantito il potenziamento di processi e procedure di risposta agli incidenti cyber, di *security by design*, di supporto alla continuità operativa a seguito di incidenti informatici, di gestione delle vulnerabilità, di gestione accessi e identità digitali, nonché l'implementazione di piani di reingegnerizzazione delle reti, di CSIRT e SOC delle singole Amministrazioni, di modelli organizzativi. Tutte queste attività hanno permesso di migliorare significativamente il livello di postura cyber delle Amministrazioni centrali coinvolte, garantendo il rafforzamento delle difese di cybersicurezza, l'adeguamento dei sistemi critici di risposta agli attacchi, l'aumento della consapevolezza dei rischi cibernetici, il potenziamento delle strutture di gestione del rischio cyber, il miglioramento e l'adeguamento dei processi interni.

Nel corso del 2025 sono stati completati gli interventi per il 75% delle Amministrazioni aderenti, per un totale di 116 attività progettuali completate; le ultime 19 saranno completate nei primi mesi del 2026.

Avviso 8/2024

L'Avviso 8/2024 ha permesso il finanziamento di progetti finalizzati a proteggere dati, sistemi e utenti dalle minacce informatiche, assicurando al contempo la continuità dei servizi essenziali delle singole PA locali. Tali progetti hanno previsto un approccio multidimensionale che ha combinato l'*assessment* tecnologico, il miglioramento dei processi organizzativi e la formazione del personale. Dal punto di vista tecnologico, sono stati potenziati i sistemi di protezione degli *endpoint* e perimetrali, implementati controlli avanzati sugli accessi ed è stata rafforzata la sicurezza delle reti e delle applicazioni. Sono state, inoltre, attivate iniziative per rafforzare la *governance* della sicurezza e la gestione del rischio, anche attraverso l'adozione di standard nazionali e internazionali per la continuità operativa e di strumenti di monitoraggio avanzato. Particolare rilievo è stato dato, infine, alla formazione e alla consapevolezza del personale, mediante percorsi formativi specifici e programmi di *security awareness*, includendo simulazioni di *phishing*.

Degli 87 progetti finanziati, nel corso del 2025, sono state portate avanti le attività tecniche, la cui finalizzazione è prevista entro il primo trimestre del 2026, in coerenza con le tempistiche di chiusura dell'Avviso.

Attraverso tali procedure, con i progetti conclusi e in via di conclusione, si è confermata la capacità del PNRR di fungere da traino sia per lo sviluppo nell'immediato di capacità di cybersicurezza per l'intero ecosistema digitale nazionale, sia per alimentare il percorso di crescita ed evoluzione di lungo termine di tali capacità, attraverso un approccio programmatico improntato al rafforzamento dell'autonomia e della resilienza cyber complessiva.

Il percorso di supporto alle PA, avviato attraverso i finanziamenti PNRR, è corroborato e continuerà a essere sostenuto dai fondi messi a disposizione per l'attuazione della Strategia nazionale di cybersicurezza (vedasi Capitolo 8). In particolare, le Misure #55 e #33, volte rispettivamente alla digitalizzazione della PA e alla creazione di CSIRT regionali, costituiscono naturale prosecuzione e valorizzazione di iniziative precedentemente avviate attraverso i finanziamenti erogati dal PNRR, nell'attuazione degli Avvisi pubblici 1/2022, 3/2022 e 6/2023, e stanno consentendo di capitalizzare investimenti, competenze e risultati conseguiti. In particolare, nel 2025 si è registrato un avanzamento degli indicatori legati all'adozione di modelli condivisi, al potenziamento delle capacità operative e alla diffusione di strumenti comuni orientati al potenziamento dei CSIRT regionali e alla costituzione di una rete nazionale di CSIRT.

Sempre a sostegno della protezione cyber della PA, l'Agenzia ha avviato, nel corso del 2025, un progetto in collaborazione con l'Istituto poligrafico e zecca dello Stato (IPZS) per contrastare il fenomeno del *phishing* nella Pubblica Amministrazione. Il progetto prevede l'attivazione di un servizio di segnalazione, attraverso il quale i dipendenti della PA, centrale e locale, potranno far valutare e-mail sospette al fine di ricevere un riscontro sull'eventuale natura malevola di quanto segnalato. Nella seconda metà del 2025 è stata avviata una fase pilota per la sperimentazione del servizio, che ha visto il coinvolgimento di alcune Amministrazioni in vista della successiva apertura del servizio alle PA interessate. Con l'iniziativa si intende tutelare il patrimonio informativo delle Pubbliche Amministrazioni, proteggendole da campagne di *phishing* e aumentando la consapevolezza dei dipendenti rispetto ai rischi legati al *social engineering* e agli attacchi informatici.

Un'ulteriore iniziativa, avviata sempre nel 2025 e in collaborazione con IPZS, risponde all'esigenza di garantire una comunicazione sicura e affidabile tra i dipendenti della Pubblica Amministrazione. A tal fine, l'Agenzia e l'Istituto sono impegnati in un progetto per lo studio e la realizzazione di una piattaforma nazionale per la gestione sicura della messaggistica istantanea dei dipendenti della PA, che dovrà assicurare riservatezza, disponibilità e integrità del dato a tutela delle informazioni scambiate. Nel corso del 2025 si è conclusa la prima fase progettuale, che ha riguardato principalmente la raccolta dei requisiti, l'analisi di soluzioni disponibili sul mercato o adottate da altri Stati membri dell'UE, la valutazione di alcuni prototipi e il completamento di uno studio di fattibilità.

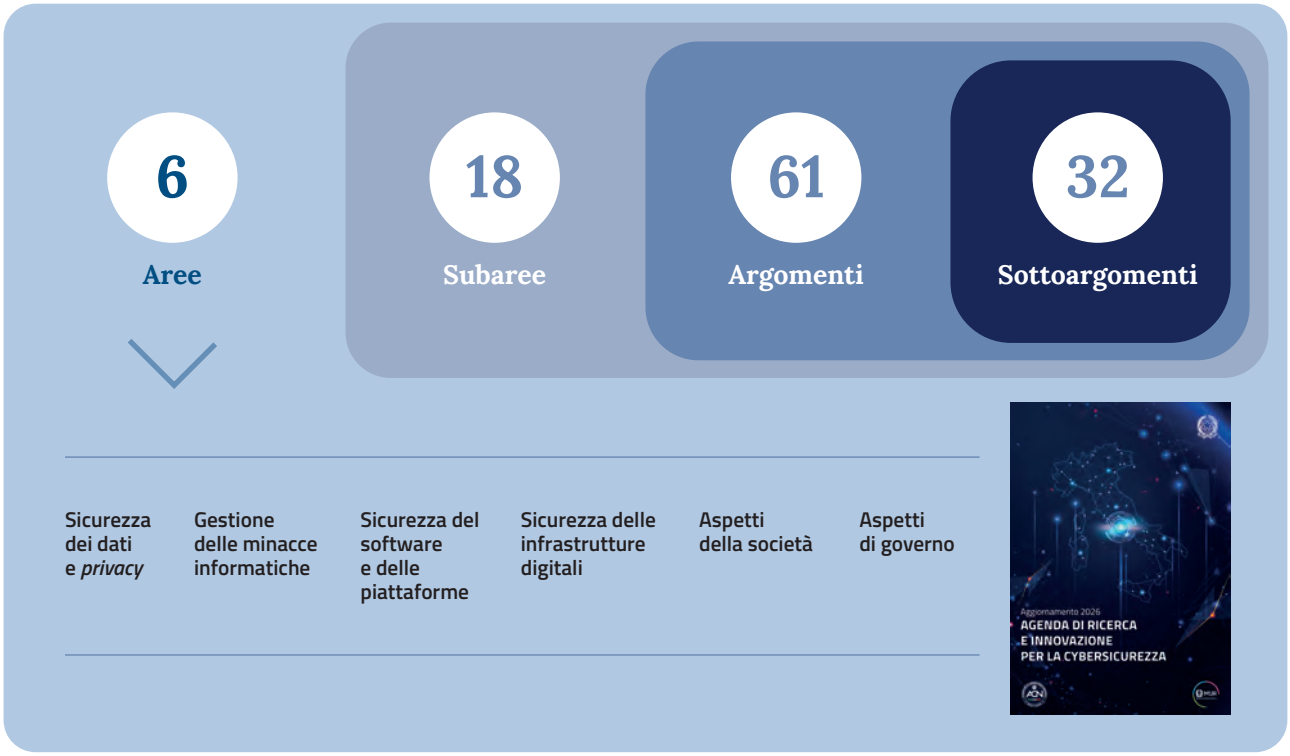
5.2 PROGRAMMI PER LA RICERCA E L'INNOVAZIONE

Nel corso del 2025, l'ACN ha proseguito l'attuazione del percorso strategico in materia di ricerca e innovazione, improntato, da un lato, a un aggiornamento continuo dei temi e delle aree di intervento, anche in funzione dell'emergere e del consolidarsi di nuove tecnologie e, dall'altro, alla costruzione e al rafforzamento di una rete di soggetti della ricerca con cui sviluppare progetti e collaborazioni sinergiche per il conseguimento degli obiettivi strategici.

5.2.1 Sostegno alla ricerca

Nel corso dell'anno è stata sviluppata la versione aggiornata dell'Agenda di ricerca e innovazione per la cybersicurezza, il documento strategico frutto di un'attività congiunta, avviata nel 2023, tra l'ACN e il MUR con l'obiettivo di supportare e orientare le scelte di ricerca e innovazione, favorendo la collaborazione pubblico-privato e contribuendo al rafforzamento delle capacità cyber nazionali. Il documento recepisce i principali indirizzi strategici di ricerca e innovazione italiani ed europei, inclusi quelli derivanti dalle più recenti evoluzioni dei quadri normativi in materia di cybersicurezza che prevedono requisiti concreti destinati a influenzare la gestione del ciclo di vita delle tecnologie digitali.

L'Agenda si rinnova e si espande, rafforzando l'impianto trasversale, strutturato in 6 aree, 18 subaree e 61 argomenti prioritari, con ulteriori approfondimenti mirati sulle principali *Emerging Disruptive Technologies* (EDT) che stanno modificando lo scenario del rischio cyber: intelligenza artificiale *general-purpose* (GPAI), tecnologie quantistiche e OT. In particolare, l'aggiornamento introduce 32 sottoargomenti pensati per mettere a fuoco le sfide aperte relative a queste tecnologie e offrire specifiche direzioni di approfondimento. Tra questi, numerosi temi chiave hanno ricadute progressive nel tempo: dalla gestione del bilanciamento tra sicurezza e prestazioni dei modelli GPAI al miglioramento della percezione del rischio da parte degli utenti, dal necessario rafforzamento della resilienza dei sistemi cyber-fisici in ambito OT, all'evoluzione sicura delle infrastrutture di comunicazione quantistica verso l'Internet quantistico.



L'Agenda si propone di fornire una base di conoscenza condivisa da utilizzare per indirizzare le attività di ricerca portate avanti dall'intero ecosistema cyber nazionale. Rappresenta, inoltre, un fondamento per tutte le iniziative volte a promuovere e valorizzare i risultati della ricerca sulla cybersicurezza condotte dall'Agenzia, nonché per lo sviluppo di politiche di ricerca e innovazione in materia di cybersicurezza a favore sia del settore pubblico, sia di quello privato.

Un altro importante filone di attività per far avanzare la ricerca è rappresentato dal programma di promozione dei dottorati di ricerca in cybersicurezza. Giunto nel 2025 alla seconda edizione, il programma consente di erogare finanziamenti triennali per progetti di dottorato su tematiche inerenti agli argomenti delineati nell'Agenda di ricerca e innovazione, rappresentando un esempio concreto di sostegno alla ricerca su priorità di interesse nazionale. Nel 2025, l'Agenzia ha pubblicato il secondo bando di selezione, con un budget da 3 milioni di euro, e assegnato 30 borse per il XLI ciclo di dottorato.

L'ultima edizione del bando, che ha visto una partecipazione ancora più ampia dell'anno precedente con 221 progetti presentati da 54 università distribuite su tutto il territorio nazionale, ha portato alla selezione di 30 progetti. Questi affrontano temi di ricerca che spaziano su tutte e 6 le aree dell'Agenda, coprendo 10 delle 18 subaree e 9 delle 19 EDT (Figura 1). Con la seconda edizione del bando, sale a 60 il numero complessivo di progetti di ricerca ammessi a finanziamento, a copertura del 93% delle subaree dell'Agenda.

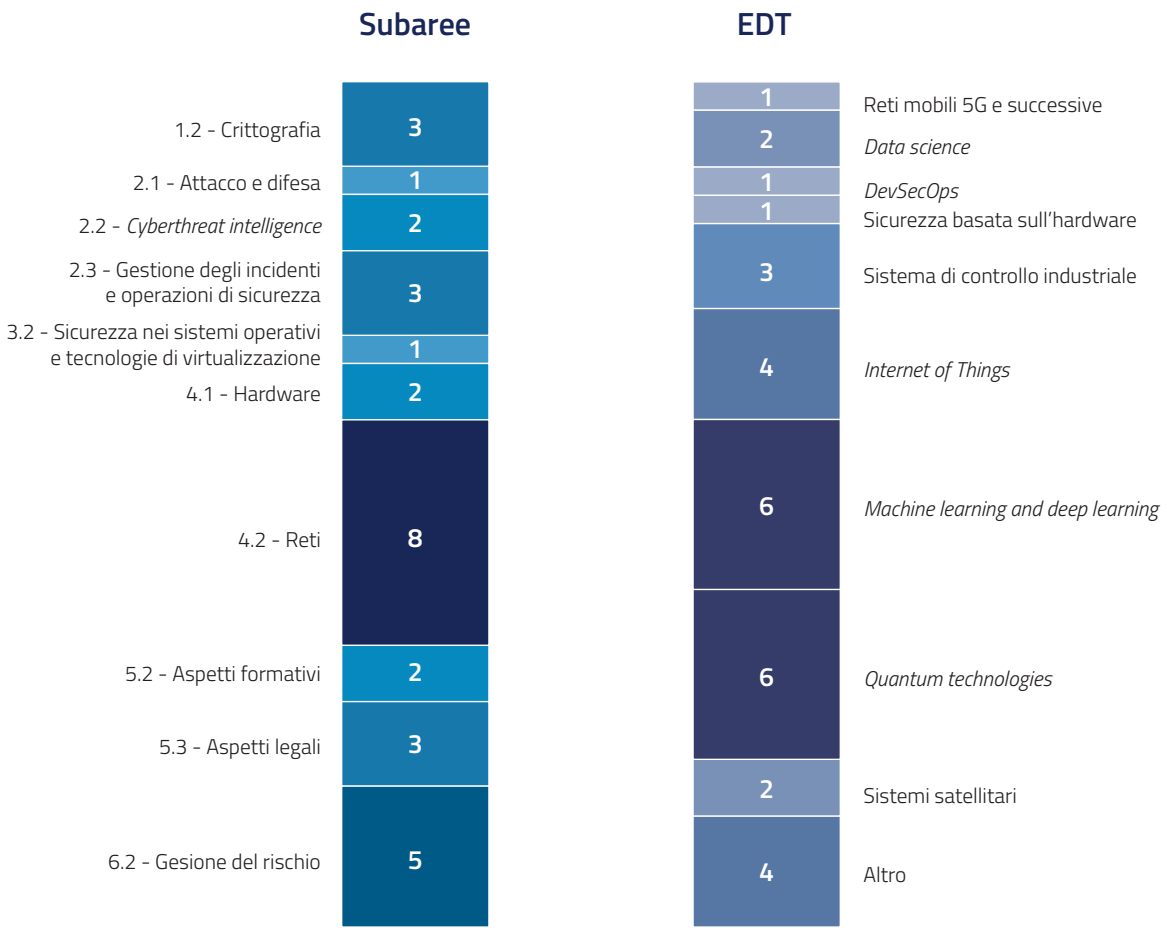


Figura 1 – Ripartizione dei progetti ammessi a finanziamento nel XLI ciclo di dottorato per subarea e per EDT dell'Agenda di ricerca e innovazione 2023-2026

Il programma dedicato ai dottorati, oltre a fornire un sostegno concreto a giovani ricercatori, funge da leva strategica per alimentare una catena virtuosa di collaborazione con le istituzioni di ricerca italiane, anche al fine di intercettare innovazioni promettenti in termini di trasferimento tecnologico. In quest'ottica, la collaborazione che l'Agenzia instaura con i dottorandi e con i relativi supervisori scientifici per lo svolgimento dei progetti finanziati consolida sinergie che mirano a massimizzare la produzione e valorizzazione di ricerca applicata, favorendo il trasferimento dei risultati della ricerca verso il mondo produttivo.

Quale ulteriore tassello di supporto alla ricerca, nel 2025 è stata condotta, in attuazione del protocollo d'intesa con l'Agenzia nazionale di valutazione del sistema universitario e della ricerca (ANVUR), un'analisi sullo stato della ricerca italiana in ambito cybersicurezza. Sulla base delle tematiche individuate dall'Agenda di ricerca e innovazione è stata effettuata una mappatura delle istituzioni di ricerca, pubbliche e private, e dei ricercatori attivi sul territorio. In particolare, si è lavorato per identificare le tematiche inerenti alla cybersicurezza maggiormente trattate nelle pubblicazioni scientifiche, nonché oggetto di corsi di dottorato; l'analisi ha riguardato, inoltre, le principali iniziative di trasferimento tecnologico in materia di cybersicurezza effettuate dagli atenei e dagli enti di ricerca. Tale analisi consentirà all'ACN e all'ANVUR di stilare un rapporto congiunto che descriverà lo stato della ricerca nazionale in materia, per orientare sempre più efficacemente i programmi di supporto alla ricerca in cybersicurezza.

Un ultimo filone di attività dell'Agenzia a sostegno della ricerca nazionale in cybersicurezza riguarda la partecipazione diretta nella redazione di proposte per progetti di ricerca, con il coinvolgimento di attori pubblici e privati lungo l'intera filiera della ricerca e dell'innovazione. Le iniziative proposte si concentrano principalmente su ambiti prioritari quali la valutazione e la messa in sicurezza dei sistemi di IA generativa, in particolare le applicazioni ad alto rischio, e l'impiego dell'IA per l'automazione di processi di cybersicurezza.

Tutte queste iniziative hanno un significativo potenziale impatto in termini di trasferimento tecnologico verso l'industria, nonché – in prospettiva – di rafforzamento della sovranità tecnologica europea nel dominio della *cybersecurity*. Le soluzioni previste potranno essere validate in contesti applicativi reali ad alta criticità, grazie al coinvolgimento di utenti finali appartenenti a rilevanti realtà industriali europee.

Analisi dei programmi europei di ricerca e sviluppo

Nel corso dell'anno, è stata condotta un'analisi dei principali programmi europei dedicati alla ricerca e allo sviluppo, ovvero *Horizon Europe*, *Digital Europe Programme* e *European Defence Fund*, con riferimento agli argomenti prioritari e alle EDT individuati nell'ambito dell'Agenda di ricerca e innovazione 2023-2026. L'approccio adottato ha previsto la ricerca di *keyword* associate a ciascun ambito ed EDT all'interno dei testi delle *call* e delle descrizioni dei progetti finanziati negli ultimi 2 anni, così da ricostruire la presenza di temi cyber nei programmi di finanziamento europei. Inoltre, è stata valutata la presenza di partner e coordinatori italiani nei consorzi dei progetti finanziati.

In particolare, sono state analizzate 601 *call*, per un totale di oltre 14.000 progetti finanziati e un contributo complessivo pari a 4,1 miliardi di euro. Sono state così individuate 360 *call* riconducibili ai temi cyber individuati dall'Agenda per un totale di 4.314 progetti finanziati, di cui 1.361 con partner italiani e 476 di questi coordinati da partner italiani.

4,1 Mld €
Contributo UE

+14.000
Progetti finanziati

+4.300
Progetti cyber finanziati

+1.300
Progetti cyber con partner italiani

+470
Progetti cyber
con coordinatori italiani

5.2.2 Sostegno all'innovazione e al trasferimento tecnologico

A supporto della catena nazionale dell'innovazione, prosegue l'impegno dell'Agenzia nell'ambito del Cyber Innovation Network (CIN), programma avviato nel 2023 per sostenere le capacità industriali, tecnologiche e scientifiche in cybersicurezza. Attraverso la costituzione di una rete di collaborazioni, il CIN coinvolge operatori qualificati dell'ecosistema dell'innovazione, quali incubatori universitari, *startup studio*, fondi di investimento e acceleratori di *startup*, nella progettazione e implementazione di programmi di supporto alle *startup* innovative.

Giunto al terzo anno di programmazione, il Cyber Innovation Network ha visto tra i principali risultati nel 2025 l'ampliamento della rete e la nascita di nuovi programmi congiunti di sostegno all'imprenditorialità innovativa, contribuendo così al rafforzamento del sistema Paese e al consolidamento della filiera industriale nel settore della cybersicurezza. Gli operatori, selezionati dall'ACN tramite avvisi a evidenza pubblica, riportano annualmente informazioni sulle proprie *Call4Startup*, iniziative definite in collaborazione con l'Agenzia per lo *scouting* e la selezione delle *startup* di maggiore interesse strategico e con elevato potenziale di crescita nell'ambito della nuova imprenditorialità innovativa in materia cyber. Queste vengono selezionate per ricevere un supporto sotto forma di contributi a fondo perduto, opportunità di *networking* e percorsi di accompagnamento imprenditoriale.

Nel corso del 2025, oltre ai 5 accordi di collaborazione precedentemente finalizzati (con CDP Venture Capital,

I3P Incubatore del Politecnico di Torino, Scientifica, Nana Bianca e Zest), è stato formalizzato un sesto accordo con Alan Advantage, consolidando ulteriormente la rete di *partnership* strategiche del CIN.

Dall'avvio del CIN, l'Agenzia ha lanciato complessivamente 6 *Call4startup* (Figura 2) con 5 operatori, 3 delle quali, lanciate nel 2024, si sono concluse nel 2025 e hanno coinvolto I3P, Scientifica e Nana Bianca. Nel 2025, inoltre, sono state lanciate altre 3 *Call4startup*, 2 delle quali hanno permesso di avviare la collaborazione con Zest e Alan Advantage, alle quali si aggiunge la seconda edizione del programma congiunto con Scientifica. È, inoltre, in fase di lancio la seconda edizione del programma con I3P.

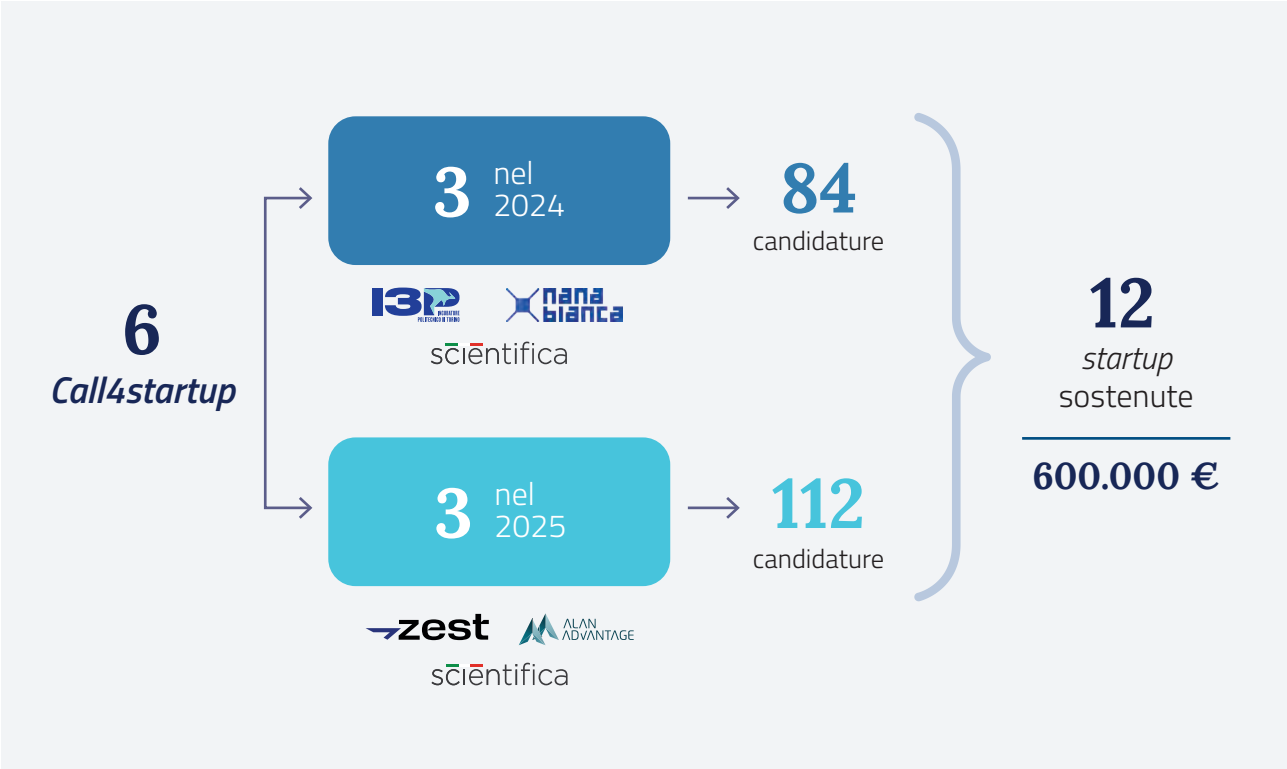


Figura 2 – Il Cyber Innovation Network nel 2025

L'interesse suscitato da queste iniziative è risultato notevole, come dimostrano le 196 candidature totali ricevute per le prime *call*. Alle 84 candidature ricevute nel 2024, seguono le 112 *startup* candidate alle 3 iniziative lanciate nel 2025. Ciò ha permesso, complessivamente, di sostenere direttamente 12 *startup*, alle quali sono stati già riconosciuti un totale di 600.000 euro di contributi a fondo perduto (Figura 2).

L'analisi delle *startup* candidate al CIN dimostra un elevato grado di maturità tecnologica, con numerose *startup* piuttosto avanzate nel processo volto a lanciare sul mercato i loro prodotti e servizi. Relativamente agli ambiti tecnologici di attività, oltre il 50% delle *startup* che hanno partecipato alle 6 *call* dell'Agenzia sviluppa soluzioni in settori strategici come l'IA, la crittografia e l'IoT (Figura 3).

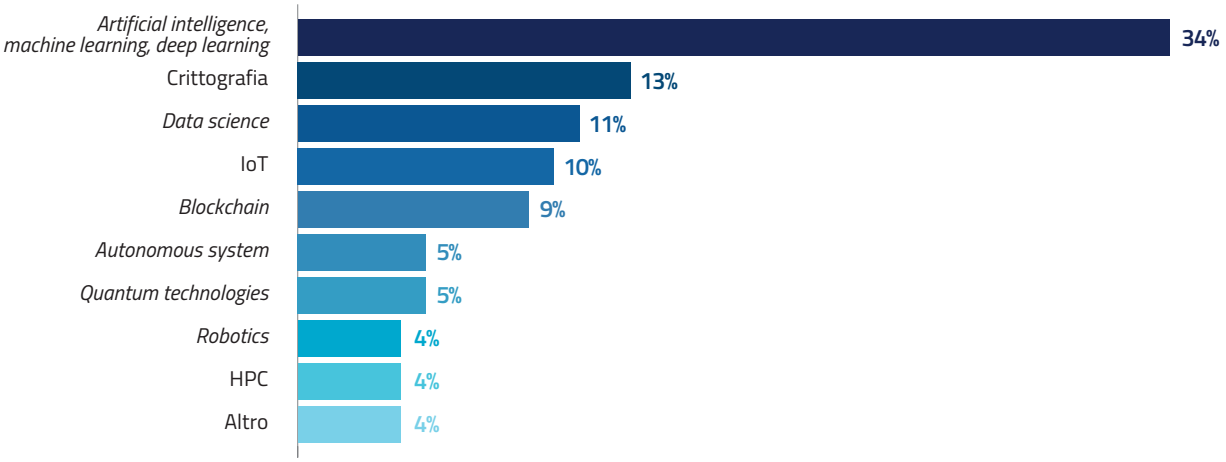


Figura 3 – Distribuzione delle *startup* candidate per principale ambito tecnologico

L'ACN sostiene le attività di accelerazione e incubazione degli operatori del CIN anche per quanto riguarda l'internazionalizzazione delle *startup*, attraverso iniziative realizzate in collaborazione con il MAECI e con l'ICE (Agenzia per la promozione all'estero e l'internazionalizzazione delle imprese italiane). Nello specifico, nel 2025 l'Agenzia ha promosso, insieme alle stesse, la partecipazione della prima delegazione italiana alla *RSAC Conference*, organizzando anche uno stand italiano incentrato sull'innovazione tecnologica in ambito cyber. Ciò costituisce uno sviluppo del Tavolo di coordinamento per l'internazionalizzazione delle imprese cyber avviato nel 2024. Alla *RSAC Conference* hanno preso parte 16 *startup* specializzate in *cybersecurity*, rappresentative dell'intera filiera della sicurezza informatica nazionale, appositamente selezionate dall'ICE. Rileva segnalare che, di queste, ben 5 ricevono il sostegno degli operatori del CIN.

Sempre nel campo dell'internazionalizzazione, l'ACN – anche alla luce della collaborazione con l'omologa agenzia spagnola INCIBE – ha promosso la partecipazione di aziende italiane (incluse alcune *startup* della rete CIN) al Foro Italia-Spagna sulla cybersicurezza, seminario internazionale mirato allo sviluppo di progetti congiunti tra realtà italiane e spagnole.

Parco nazionale della cybersicurezza

Misura #49

Sempre nel corso del 2025 l'Agenzia ha avviato – in linea con il Piano di implementazione della Strategia nazionale di cybersicurezza 2022-2026 – le attività propedeutiche per la creazione del Parco nazionale della cybersicurezza (Misura #49), una struttura diffusa per ricerca, sviluppo e sperimentazione in ambito *cybersecurity* e tecnologie digitali, che consentirà l'adesione di *stakeholder* nazionali, pubblici e privati. L'obiettivo di tale misura, in continuità con le precedenti iniziative del CIN, è promuovere l'autonomia strategica nazionale. Il progetto è sostenuto dall'Agenzia, in collaborazione con le altre Amministrazioni responsabili della misura (DTD, MEF, MIMIT e Ministero della difesa). Nel 2025 sono state avviate le interlocuzioni con le altre Amministrazioni coinvolte e ulteriori attori istituzionali che hanno confermato i principi dell'iniziativa, relativi in particolare al modello *hub & spoke*: un *hub* centrale per ospitare le funzioni istituzionali, di coordinamento e di indirizzo strategico ed eventuali spazi e infrastrutture, accompagnato da *spoke* distribuiti sul territorio nazionale, che potranno offrire servizi specializzati con il coinvolgimento di *stakeholder* e soggetti industriali, ai quali sarà aperta la possibilità di collaborazione nel Parco.

5.3 PROGRAMMI A SUPPORTO DEI SERVIZI CYBER NAZIONALI

L'Investimento 1.5 "Cybersecurity" del PNRR, oltre a quanto già richiamato sull'innalzamento della postura cyber delle PA, ha permesso all'Agenzia di sviluppare e consolidare diversi servizi cyber nazionali, al fine di rendere disponibili strumenti avanzati per la prevenzione, la gestione e la mitigazione del rischio cibernetico, anche attraverso forme strutturate di cooperazione con la Pubblica Amministrazione e con il settore privato.

Sulla base dei risultati raggiunti nel 2024, con il progressivo dispiegamento di HyperSOC, della rete di CSIRT e di ISAC Italia, l'Agenzia, nel 2025, ha potuto completare la messa a regime dei servizi e lavorare per il loro ulteriore potenziamento e per la loro piena integrazione all'interno dell'ecosistema nazionale di cybersicurezza. Tali sforzi rispondono all'esigenza di assicurare continuità, scalabilità ed efficacia nel tempo delle capacità di risposta e resilienza.

L'HyperSOC è un sistema integrato per la protezione degli *asset* strategici nazionali, finalizzato a rafforzare le capacità di monitoraggio e analisi degli eventi di sicurezza dei soggetti aderenti, sia pubblici che privati. Attraverso HyperSOC, l'ACN comunica alle organizzazioni partecipanti criticità quali vulnerabilità, configurazioni non corrette e software obsoleti, fornendo indicazioni operative e supporto per la loro mitigazione.

Nel corso del 2025, il progetto ha consolidato e ampliato ulteriormente la propria capacità operativa, registrando un ampliamento dei soggetti aderenti, arrivati a 37 tra entità private e pubbliche anche di livello locale. Sono, inoltre, cresciuti gli *asset* monitorati e i servizi erogati. In particolare, sono state potenziate le capacità di monitoraggio sul piano tecnologico, attivando due nuovi servizi dedicati, rispettivamente, alla condivisione di regole di rilevamento (*Advanced Threat Detection*) e all'individuazione di eventi cyber rilevanti, come attacchi DDoS e campagne di *phishing* (*Notable Security Events*). I soggetti aderenti possono integrare tali regole e scenari nei propri sistemi di sicurezza per identificare minacce ed eventi di interesse per l'Agenzia, comunicando in maniera automatizzata alla stessa gli eventuali riscontri. Ciò mira a rafforzare ulteriormente la capillarità, l'efficacia e la resilienza di HyperSOC, rendendolo un elemento centrale del sistema nazionale di cybersicurezza e un punto di riferimento stabile per la protezione degli *asset* strategici del Paese.

Inoltre, il servizio di *Attack Surface Monitoring*, già operativo, ha consentito il rilevamento proattivo delle criticità sul perimetro esterno dei soggetti partecipanti; il potenziamento del servizio *Golden Set of IoC* ha permesso il monitoraggio di indicatori di compromissione su scala nazionale e settoriale, garantendo una condivisione bidirezionale e in tempo reale tra le piattaforme dei soggetti aderenti e quelle dell'Agenzia.

Allo stato attuale risultano oltre 300 utenti abilitati all'utilizzo della piattaforma, per un totale di oltre 10.500 *asset* inseriti sotto monitoraggio, per i quali sono state prodotte diverse centinaia di migliaia di segnalazioni di vulnerabilità, per oltre quasi 4.000 indicatori di compromissione riscontrati dai soggetti.

FOCUS

High Performance Computing

Nel 2025, sotto la spinta propulsiva dei finanziamenti del PNRR, sono proseguite le attività propedeutiche alla realizzazione dell'infrastruttura di High Performance Computing (HPC) dedicata alla cybersecurity nazionale, frutto della collaborazione tra l'Agenzia e il consorzio Cineca. In particolare, a giugno è stata inaugurata a Napoli l'infrastruttura HPC Megaride, presso l'Università degli studi di Napoli Federico II nel polo di San Giovanni a Teduccio. Mettendo a disposizione un'elevata potenza di calcolo, l'obiettivo dell'HPC è quello di supportare e promuovere, da un lato, la ricerca scientifica, sia in ambito accademico che industriale e, dall'altro, la cybersicurezza del Paese attraverso lo sviluppo di strumenti di simulazione, basati su intelligenza artificiale e machine learning, per potenziare l'HyperSOC nella prevenzione, scoperta, risposta e predizione degli impatti di attacchi cyber. L'infrastruttura, inoltre, per garantire lo sviluppo consapevole e sicuro di tecnologie digitali e favorire l'autonomia strategica nazionale ed europea, sarà messa a disposizione anche del Cyber Innovation Network dell'Agenzia e, più in generale, del mondo produttivo anche nell'ambito del progetto IT4LIA AI Factory (vedasi paragrafo 5.4).
Nel 2025 sono state portate avanti diverse attività propedeutiche alla messa in produzione del sistema HPC per la valutazione delle infrastrutture disponibili e la definizione del modello di erogazione dei servizi, in coordinamento tra i diversi attori tecnici e istituzionali, con l'obiettivo di predisporre l'infrastruttura all'utilizzo operativo di casi d'uso avanzati.

Rete CSIRT

La rete nazionale di CSIRT, coordinata dal CSIRT Italia, costituisce il sistema per la gestione e la risposta a minacce, incidenti e crisi cibernetiche, supportando la *constituency* nazionale nella gestione di eventi cyber, che possono avere un impatto negativo su servizi critici o generare situazioni di crisi a livello nazionale. La rete si fonda su una stretta collaborazione tra il CSIRT Italia e i vari CSIRT regionali e delle PA centrali.

Nel corso del 2025, sono state potenziate le piattaforme a supporto del CSIRT Italia ed è stata abilitata l'interconnessione con i CSIRT regionali, istituiti presso Regioni e Province autonome, al fine di garantire una maggiore copertura informativa sul territorio. Si è, inoltre, puntato a un'estensione ulteriore della rete nazionale, avviando la progressiva inclusione dei CSIRT delle Pubbliche Amministrazioni centrali.

Sono state portate avanti attività per rafforzare ulteriormente le piattaforme e gli strumenti di coordinamento e comunicazione, migliorando l'analisi e la gestione degli incidenti, la condivisione in tempo reale delle informazioni e l'integrazione con i sistemi di *cyber threat intelligence* nazionali ed europei. Si è lavorato, inoltre, per sviluppare procedure standardizzate e capacità operative condivise, al fine di garantire uniformità nella risposta agli incidenti e facilitare la cooperazione tra tutti i livelli della rete.

Tali interventi intendono garantire che la rete CSIRT nazionale diventi un punto di riferimento stabile, capillare e partecipato, in grado di assicurare la protezione continua degli *asset* critici del Paese e di coordinare efficacemente la risposta agli eventi cyber su scala nazionale e internazionale.

ISAC Italia

ISAC Italia è l'*Information Sharing and Analysis Center* nazionale istituito presso l'Agenzia, con l'obiettivo di riunire in una rete gli ISAC settoriali e conseguentemente raccogliere, analizzare e condividere, in maniera bidirezionale e multisettoriale, le informazioni, operazionali e strategiche, a maggior valor aggiunto. Nel corso del 2025 è proseguita l'attività dell'ISAC Italia volta ad agevolare sempre di più lo scambio di informazioni a livello nazionale attraverso l'adozione di un lessico comune, provvedendo ad aggiornare la tassonomia sugli eventi cyber, oltre che proseguendo l'attività di informazione sulle principali minacce cyber, attraverso la pubblicazione di specifici report.

La tassonomia cyber dell'ACN

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

Nel 2025, la tassonomia è stata arricchita con ulteriori informazioni utili per meglio caratterizzare gli eventi cyber e realizzata anche in versione *machine-readable* per massimizzarne la diffusione e facilitarne l'integrazione nelle piattaforme utilizzate dai soggetti della *constituency*, tra cui quelle che impiegano strumenti di raccolta, analisi e correlazione di eventi di sicurezza.

Nel suo ruolo di facilitatore per la costruzione della rete nazionale degli ISAC, nel corso del 2025 l'ACN ha proseguito la collaborazione con l'ISAC del comparto autostradale (AISCAT-Associazione italiana società concessionarie autostrade e trafori), che ha consentito di sviluppare specifici scenari di rischio cyber, strumenti fondamentali per simulare attacchi, valutare la robustezza delle misure di protezione esistenti e orientare la pianificazione degli investimenti in cybersicurezza.

Tramite la rete nazionale degli ISAC, l'Agenzia persegue l'obiettivo di rafforzare la resilienza cibernetica nazionale attraverso il superamento delle logiche frammentarie dei singoli, costruendo un ecosistema capace di garantire risposte tempestive, coordinate ed efficaci alle minacce, a tutela dei settori strategici e della continuità operativa del Paese.

5.4 PROGRAMMI DI RILEVANZA EUROPEA

Un forte impulso alla realizzazione di progetti innovativi e ad alto contenuto tecnologico è venuto dall'Unione europea che, con diversi strumenti, ha fornito importanti leve finanziarie a sostegno della cybersicurezza e dell'applicazione delle nuove tecnologie, in particolare l'intelligenza artificiale.

L'Agenzia, nel corso del 2025, ha proseguito le sue funzioni di Centro nazionale di coordinamento (NCC), a supporto del Centro europeo di competenza in cybersicurezza (*European Cybersecurity Competence Centre*-ECCC) nell'attuazione di iniziative volte a rafforzare lo sviluppo industriale, tecnologico e di ricerca in *cybersecurity*.

L'ACN ha complessivamente partecipato in questi anni a 7 bandi *Digital Europe Programme* (DEP) e *Horizon Europe*, aggiudicandosi le relative opportunità di finanziamento messe a disposizione dall'ECCC. L'Agenzia ha, infatti, promosso e sostenuto la partecipazione a progetti di ricerca e sviluppo in risposta ai programmi di finanziamento europei, elaborando proposte progettuali in collaborazione con il mondo accademico e produttivo. Nel 2025 l'ACN ha lavorato per portare avanti i seguenti progetti finanziati dall'Unione europea: NCC-IT, SECURE, ENSOC, CHIEF, IT4LIA, EUSAiR e AKADIMOS (Figura 4). Mentre AKADIMOS è un progetto dedicato alla formazione ed è più approfonditamente descritto in seguito (vedasi Capitolo 7), per gli altri progetti viene fornita una breve sintesi nel prosieguo.

	Progetto	Durata	Budget totale	Soggetti coinvolti	Obiettivo principale
	NCC-IT	2023-2025	€1.996.620	1	Rafforzamento del Centro nazionale di coordinamento
	SECURE	2025-2027	€21.921.036	8	Sostegno alle PMI europee nell'implementazione del *Cyber Resilience Act*
	ENSOC	2024-2028	€24.326.757	7	Sviluppo di una piattaforma *cross-border* di individuazione e analisi delle minacce cyber
	CHIEF	2026-2028	€1.970.672	5	Supporto all'implementazione del *Cyber Solidarity Act*
	IT4LIA	2025-2028	€420.000.000	13	Sviluppo di una *AI Factory* italiana
	EUSAiR	2024-2026	€1.907.000	13	Supporto all'implementazione dell'*AI Act*
	AKADIMOS	2025-2027	€3.999.660	9	Supporto alla creazione e all'avvio operativo della *European Cybersecurity Skills Academy*

ACN coordinatore ACN partner

Figura 4 – Progetti finanziati dall'UE cui partecipa l'ACN

Con la piena operatività del Centro nazionale di coordinamento, nel 2025 si è anche concluso il progetto NCC-IT, che ha beneficiato di un finanziamento DEP. Tra i principali risultati raggiunti, si segnala l'organizzazione di 13 eventi tra *matchmaking*, *training* e disseminazione, la creazione e pubblicazione della newsletter trimestrale dell'NCC, la gestione di oltre 60 richieste di supporto e la pubblicazione di oltre 60 contenuti informativi.

Il progetto SECURE (*Strengthening EU SMEs Cyber Resilience*), portato avanti da un consorzio coordinato dall'Agenzia e composto da partner istituzionali e imprenditoriali di 7 Paesi UE, è volto a supportare le PMI europee attraverso l'erogazione di finanziamenti a cascata per sostenere la *compliance* con il *Cyber Resilience Act*. Il progetto, lanciato nel gennaio 2025 e con scadenza a dicembre 2027, ha una dotazione finanziaria di circa 22 milioni di euro, di cui il 75% sarà destinato ai finanziamenti diretti alle PMI.

Nel 2025 SECURE si è focalizzato sullo sviluppo della piattaforma digitale destinata a raccogliere le richieste progettuali delle PMI, nonché sul coinvolgimento di tutti gli Stati membri, attraverso i propri NCC, per garantire

un'ampia promozione del progetto in tutta l'UE e il massimo supporto nei controlli di eleggibilità delle candidature delle PMI. In stretta collaborazione con la Commissione europea, il progetto SECURE ha sviluppato sinergie con gli altri progetti finanziati dal DEP dedicati a sostenere la *compliance* col CRA e con i relativi atti implementativi.

L'Agenzia partecipa, all'interno di un consorzio finanziato con fondi DEP che include rilevanti Amministrazioni di altri 6 Stati membri, al progetto europeo ENSOC (*European Network of SOC*), che ha un budget di oltre 24 milioni di euro. ENSOC, in linea con quanto previsto dal *Cyber Solidarity Act*, sostiene la creazione di una rete europea di *cyber hub* per facilitare lo scambio di informazioni di cybersicurezza, contribuendo così a migliorare la postura di sicurezza dei Paesi dell'Unione europea. Il progetto consiste nello sviluppo di una piattaforma informatica collaborativa, interoperabile e scalabile, che automatizzi tale condivisione di informazioni tra i Paesi partecipanti, nonché verso altre reti di SOC europee e verso il *CSIRTs Network*, velocizzando le attività di rilevamento, analisi e risposta alle minacce cyber transnazionali.

Nel corso del 2025 l'ACN ha contribuito alle attività di ENSOC, in particolare nella definizione della piattaforma informatica e nell'attuazione del *joint procurement* finalizzato all'approvvigionamento dei componenti infrastrutturali e tecnologici necessari all'installazione della piattaforma.

L'Agenzia è anche coordinatore di un consorzio che include partner di altri 4 Stati membri, e guida il progetto europeo CHIEF (*Cybersecurity Hubs Interoperability and Cooperation Framework*), che nel 2025 si è assicurato un finanziamento DEP di circa 2 milioni di euro. CHIEF ha l'obiettivo di sostenere l'attuazione del CSoA, attraverso la definizione di *best practice*, modelli e protocolli che favoriscano la cooperazione tra i diversi livelli di SOC (locali, nazionali e transfrontalieri), la collaborazione pubblico-privato e l'integrazione nelle attività dei SOC di tecnologie quali IA e HPC. Il progetto ha una durata di 3 anni a partire da gennaio 2026.

In ambito di intelligenza artificiale, l'ACN è tra i promotori del progetto IT4LIA AI Factory, selezionato tra le *AI Factory* europee con l'obiettivo di mettere a fattor comune capacità computazionali, dati e competenze, così da favorire lo sviluppo, l'adozione e l'utilizzo sicuro e affidabile dell'intelligenza artificiale in Italia e nell'UE. Il progetto, guidato dall'Italia con la partecipazione di Austria e Slovenia, dispone di un budget complessivo di 420 milioni di euro, cofinanziato al 50% dalla Commissione europea ed è coordinato dal Cineca, nonché sostenuto, tra gli altri, dal MUR e dalla Regione Emilia-Romagna.

IT4LIA prevede il potenziamento e l'integrazione delle infrastrutture di supercalcolo e degli strumenti di intelligenza artificiale localizzati presso il DAMA Tecnopolo di Bologna, creando un ecosistema di servizi e capacità elaborativa in stretto raccordo con il mondo della ricerca, dell'industria e della PA. Tale ecosistema consente l'accesso a un'elevata potenza computazionale e a servizi specialistici, favorendo l'adozione dell'IA anche in contesti complessi e critici, quali i settori *agritech*, scienze della terra e del clima, manifatturiero e cybersicurezza, contribuendo così allo sviluppo di *startup* e *spin-off* operanti in ambiti ad alto contenuto innovativo. La partecipazione dell'Agenzia al progetto risponde anche all'esigenza di poter offrire un servizio di alto valore tecnologico alla rete del Cyber Innovation Network, nell'ottica di rafforzare la sovranità tecnologica, la sicurezza e la resilienza del sistema digitale nazionale, assicurando che lo sviluppo e l'adozione dell'IA avvengano in modo coerente con gli interessi strategici del Paese.

Nel corso del 2025, IT4LIA ha avviato la fase operativa, rendendo progressivamente disponibili i primi servizi e meccanismi di accesso alla piattaforma. In tale contesto, l'Agenzia ha assicurato il proprio contributo di indirizzo strategico e di messa a terra del progetto, verso lo sviluppo e l'utilizzo sicuro e affidabile di soluzioni di intelligenza artificiale.

Sempre in ambito di IA, è stato avviato nel gennaio 2025 il progetto EUSAiR (*AI Regulatory Sandboxes: EU-Level Coordination and Support*), che getta le basi per un approccio coordinato a livello UE alla costruzione di *sandbox* per la sperimentazione normativa, favorendo l'attuazione dell'*AI Act*, anche a beneficio di PMI e *startup*.

EUSAiR è realizzato da un consorzio, coordinato dal Centro nazionale di ricerca in HPC di Bologna, al quale l'Agenzia partecipa insieme a partner di altri 6 Paesi UE. Il consorzio dispone di un budget di circa 2 milioni di euro, finanziato interamente dal programma DEP. Tra le altre cose, EUSAiR intende promuovere sinergie con iniziative quali l'EuroHPC (Impresa comune europea per il calcolo ad alte prestazioni) e con analoghe strutture di prova e sperimentazione dell'IA (*AI Testing and Experimentation Facilities*), nonché con IT4LIA. Infatti, EUSAiR mira a valorizzare le infrastrutture e i servizi offerti da IT4LIA, creando un percorso bidirezionale composto, da un lato, dalla *guidance* regolatoria che preceda lo sviluppo e test di sistemi di IA e, dall'altro, dalla progettazione di modelli conformi alla regolamentazione.

Durante il 2025, si è tenuto il primo *workshop* per avviare lo sviluppo di linee guida, *framework*, casi d'uso, processi e strumenti per il funzionamento delle *sandbox* normative sull'intelligenza artificiale. EUSAiR ha compiuto progressi significativi attivando progetti pilota che consentiranno a sviluppatori e fornitori di IA, autorità di regolamentazione e altri attori interessati di sperimentare casi d'uso e contribuire all'ideazione di procedure per le *sandbox* regolatorie.

FOCUS

La valutazione dei programmi di investimento

Nel corso del 2025, l'Agenzia ha avviato gli studi per la definizione di un modello di valutazione dei programmi di investimento in sicurezza informatica che gestisce. L'obiettivo è lo sviluppo di un modello alla base del calcolo del ROSI (Return on Security Investment), ovvero una metrica che quantifica il valore degli investimenti in sicurezza informatica. Lo scopo del ROSI è supportare tali investimenti, evidenziandone il ritorno finanziario. Il modello di calcolo prevede la stima della potenziale perdita economica che un'organizzazione avrebbe potuto subire in assenza di un investimento in sicurezza, confrontandola con il costo complessivo dell'intervento.

Il ROSI è stato applicato dall'Agenzia per una prima valutazione degli interventi PNRR attivati a favore della PA centrale e locale. Tra le attività correlate al calcolo, particolare attenzione è stata prestata agli impatti relativi alle variazioni dell'efficacia della protezione cyber di un'organizzazione al variare della postura cibernetica della stessa. Il modello ha potuto beneficiare di un confronto tra esperti dell'ACN e rappresentanti del mondo accademico e industriale.

6

Cooperazione internazionale

In linea con le politiche e gli indirizzi del Governo e alla luce del suo mandato istituzionale, l'Agenzia per la cybersicurezza nazionale ha consolidato e ampliato la rete di relazioni e di collaborazioni con partner esteri strategici, facendo leva sulla cooperazione internazionale quale strumento indispensabile per salvaguardare la sicurezza nazionale ed economica dell'Italia, esposta in misura crescente a pressioni e mutamenti geopolitici.

A fronte del rapido e dirompente sviluppo di nuove tecnologie su scala globale, l'ACN ha lavorato con le agenzie partner per rafforzare le politiche internazionali volte a ridurre o prevenire rischi e minacce alla cybersicurezza.

In ambito multilaterale, l'Agenzia, oltre a confermare il proprio impegno all'interno di tavoli dei quali faceva già parte, ha allargato il suo raggio d'azione a nuovi consessi e iniziative. Quanto ai primi, ha continuato a fornire il proprio contributo al Gruppo di lavoro G7 sulla cybersicurezza, istituito nel 2024 durante la Presidenza italiana su impulso della stessa Agenzia, nonché ad attestarsi quale partner credibile e autorevole della *Counter Ransomware Initiative* (CRI). Quanto alle attività di più recente avviamento, l'ACN ha aderito a iniziative che dimostrano il crescente interesse nella cybersicurezza e riconoscono l'interdipendenza tra stabilità economico-finanziaria, sicurezza cibernetica e tutela degli interessi strategici nazionali.

A livello di Unione europea, l'Agenzia partecipa attivamente a tutti i principali forum in materia di cybersicurezza e, quale nuovo ambito di competenza, di intelligenza artificiale. Si tratta di una collaborazione a tutto tondo, che parte dal contributo alla regolamentazione, alla strategia e all'ideazione delle *policy*, per arrivare alle molteplici iniziative che concretamente le rendano effettive. A tale riguardo, nel 2025 l'attività dell'ACN ha garantito il presidio di numerosi consessi, dedicati a temi quali la gestione degli incidenti, la certificazione e il sostegno agli investimenti.

Sul piano bilaterale, l'Agenzia ha elevato di livello le collaborazioni con i centri cyber dei Paesi G7 ed europei e con quelli appartenenti alla regione del Mediterraneo allargato, coerentemente con la proiezione internazionale verso aree di grande importanza sotto il profilo della cybersicurezza. Una rete di rapporti che le consente, attraverso le interlocuzioni con i partner e le attività di cooperazione a livello tecnico, non solo di garantire una più efficace prevenzione e gestione dei rischi cyber e delle vulnerabilità tecnologiche, ma anche di estendere la proiezione internazionale dell'Italia, a beneficio di tutto l'ecosistema nazionale di cybersicurezza.

6.1 COOPERAZIONE MULTILATERALE

L'Agenzia ha continuato a lavorare insieme ai centri e alle autorità cyber del Gruppo di lavoro G7 sulla cybersicurezza per affinare, consolidare e ottimizzare le rispettive capacità di protezione dello spazio cibernetico, a vantaggio della sicurezza nazionale e collettiva dei Paesi G7. L'Agenzia ha sostenuto la realizzazione dell'ambiziosa agenda della Presidenza canadese 2025 del Gruppo, che ha ampliato il ventaglio della cooperazione interagenzie a ulteriori temi prioritari: intelligenza artificiale e cybersicurezza, transizione alla crittografia post-quantistica, politiche di incentivo alla sicurezza cyber, sicurezza delle soluzioni IoT e meccanismi di condivisione delle informazioni sulle minacce cyber.

In materia di intelligenza artificiale, l'ACN ha guidato con l'omologa agenzia tedesca (BSI) l'adozione da parte del Gruppo della visione condivisa sulla trasparenza nelle catene di approvvigionamento dei sistemi di IA, incentrata sull'approccio *Software Bill of Materials* (SBOM) applicato a questa tecnologia, avviando l'elaborazione di linee guida tecniche dedicate. L'Agenzia ha, inoltre, contribuito alla redazione di un documento congiunto che individua le linee d'azione operative per pianificare e attuare la transizione alla crittografia post-quantistica, elevandola a priorità cyber e non a mero aggiornamento tecnico. Ha, infine, sostenuto l'adozione della Dichiarazione del G7 sulla sicurezza dell'IoT.

I progressi realizzati, anche con l'apporto dell'ACN, sono stati riconosciuti durante le riunioni del Gruppo a Ottawa (12-13 maggio) e a Parigi (25 novembre) e ulteriormente valorizzati sia nel Comunicato adottato dai Ministri dell'interno e della sicurezza del G7 (23 novembre), sia in quello dei Ministri dell'industria, del digitale e della tecnologia (9 dicembre). I due comunicati supportano la visione condivisa sulle SBOM per l'intelligenza artificiale e la Dichiarazione sulla sicurezza dell'IoT, enfatizzando l'importanza delle partnership internazionali e pubblico-private per aumentare la resilienza informatica e rafforzare la sicurezza condivisa attraverso la difesa delle infrastrutture e dei servizi critici.

L'operato dell'ACN all'interno del Gruppo le ha consentito di rinsaldare ulteriormente i legami con le agenzie partner di Canada, Francia, Germania, Stati Uniti, Regno Unito e Giappone, avviando dialoghi strutturati su ulteriori questioni di sicurezza cyber: dalla gestione di grandi eventi (Olimpiadi Milano Cortina 2026) all'impiego sicuro di tecnologie nuove, emergenti e dirompenti, fino all'applicazione dell'approccio *Bills of Materials* per individuare potenziali vulnerabilità e rischi cyber. A quest'ultimo riguardo, ad esempio, l'ACN ha aderito, insieme a 16 agenzie, al documento *A Shared Vision of Software Bill of Materials for Cybersecurity* pubblicato dall'Agenzia per la cybersicurezza e la sicurezza delle infrastrutture degli Stati Uniti (CISA). Tale documento fornisce orientamenti sui vantaggi derivanti dall'utilizzo delle SBOM in termini di cybersicurezza e trasparenza del software, lungo tutta la filiera di approvvigionamento.

Sempre in ambito G7, oltre alle attività condotte nel Gruppo di lavoro sulla cybersicurezza, l'ACN ha collaborato, con il MAECI, alla redazione di un documento di analisi delle minacce ibride rivolte alle infrastrutture critiche sottomarine, redatto dal Gruppo di lavoro G7 *Policy Planners*. Si tratta di un tema di crescente rilevanza strategica, considerato il ruolo svolto da tali infrastrutture per la connettività globale, la sicurezza economica e la resilienza degli Stati.

Con l'obiettivo di incidere sulle attività di cooperazione internazionale rilevanti in ambito economico, l'ACN ha aderito al Gruppo di lavoro sulla sicurezza digitale dell'Organizzazione per la cooperazione e lo sviluppo

Trasparenza e cybersicurezza: il ruolo delle *Bill of Materials*

Durante il 2025, l'ACN ha supportato l'applicazione del concetto di *Bill of Materials* al software, ai sistemi di intelligenza artificiale e a quelli crittografici, sia a livello di cooperazione multilaterale che nelle relazioni bilaterali.

Bill of Materials (BOM)
Sono un elenco strutturato di tutti i componenti che costituiscono un prodotto o un sistema. Il concetto di BOM è applicato anche ai sistemi digitali per garantire trasparenza e tracciabilità lungo le catene di fornitura.

Software Bill of Materials (SBOM)
Applicano questo concetto al software, fornendo un inventario delle librerie, dei moduli e delle dipendenze che compongono un'applicazione. Le SBOM sono uno strumento fondamentale per migliorare la sicurezza informatica e facilitare la cooperazione internazionale nella gestione delle vulnerabilità.

SBOM per l'intelligenza artificiale (SBOM for AI)
Estendono ulteriormente questo approccio ai sistemi di IA, includendo modelli, *dataset* e componenti specifiche dell'ecosistema dell'intelligenza artificiale. Contribuiscono a una maggiore trasparenza, fiducia e responsabilità nello sviluppo e nell'uso dell'IA.

Cryptographic Bill of Materials (CBOM)
Sono versioni specializzate dello SBOM che elencano gli *asset* crittografici utilizzati in un sistema. Aiutano a individuare rischi e vulnerabilità, incluse quelle legate al calcolo quantistico, e a pianificare il passaggio verso soluzioni di crittografia post-quantum.

economico (OCSE). Il Gruppo elabora iniziative di *policy* riguardanti la dimensione economica e sociale della cybersicurezza. L'ingresso nel Gruppo OCSE consentirà all'Agenzia, tra le altre cose, di fornire il proprio apporto alla *governance* dell'intelligenza artificiale e della transizione alla crittografia post-quantistica, nonché alla definizione di iniziative per far fronte alla frammentazione del quadro regolatorio internazionale.

FOCUS

Gruppo di lavoro sulla sicurezza digitale dell'OCSE

Il Gruppo di lavoro sulla sicurezza digitale (Working Party on Digital Security) opera nell'ambito del Comitato sulla politica digitale (Digital Policy Committee) dell'OCSE. Il Gruppo promuove lo scambio di conoscenze, esperienze e buone pratiche, con l'obiettivo di elaborare analisi, raccomandazioni e policy riguardanti la dimensione economica e sociale della cybersicurezza, che si aggiunge a quella di sicurezza nazionale. Il Gruppo si compone dei rappresentanti sia di agenzie nazionali di cybersicurezza, sia di istituzioni responsabili per le politiche digitali dei 38 Paesi che fanno parte dell'OCSE. Questa pluralità di attori consente un confronto ampio e multidisciplinare, favorendo l'elaborazione di approcci condivisi e soluzioni coordinate alle sfide emergenti nel panorama della sicurezza digitale.

Con il coordinamento della Banca d'Italia, l'Agenzia ha, inoltre, contribuito al *Financial Sector Assessment Program*, ossia alla valutazione periodica sulla stabilità del sistema finanziario nazionale condotta dal Fondo monetario internazionale (FMI). Tale esercizio, per la prima volta, ha incluso in modo strutturato la dimensione della *governance* nazionale del rischio cyber, a dimostrazione dell'esistente interdipendenza tra stabilità economico-finanziaria, sicurezza cibernetica e tutela degli interessi strategici nazionali. La partecipazione dell'ACN ha permesso di valorizzare i punti di forza dell'architettura nazionale di cybersicurezza, compresi la *leadership* assegnata in questa materia all'autorità politica e il coordinamento interistituzionale assicurato dal Nucleo per la cybersicurezza, istituito presso l'ACN, che consente una visione trasversale del rischio cyber nei principali settori critici del Paese.

Sempre sul piano multilaterale, l'Agenzia ha operato per accrescere il posizionamento dell'Italia nell'ambito della *Counter Ransomware Initiative*. In particolare, ha condiviso con i 74 Paesi e organizzazioni membri dell'iniziativa la riflessione nazionale sull'adozione di legislazione mirata per il contrasto al *ransomware*. Il documento finale adottato nel corso del Summit di Singapore (24 ottobre) sancisce che le misure legislative all'esame del Parlamento italiano rappresentano ambiti da cui i membri della CRI potrebbero trarre spunto per future riflessioni congiunte. L'azione dell'Agenzia su questo tema è stata strumentale anche a rafforzare il dialogo bilaterale sul contrasto a tale minaccia, in particolare con le omologhe autorità del Regno Unito e dei Paesi Bassi.

L'ACN ha poi continuato a mettere a disposizione del MAECI le proprie competenze specialistiche, supportando il Dicastero nelle attività di cooperazione di cybersicurezza che si svolgono nei tavoli internazionali. Di rilievo il contributo fornito, unitamente alle altre Amministrazioni nazionali, al processo di Pall Mall, iniziativa internazionale a guida franco-britannica, che coinvolge rappresentanti governativi, del settore privato e della società civile, e che mira a promuovere l'impiego responsabile e a limitare la proliferazione di strumenti e servizi di intrusione cyber (inclusi gli *spyware*). Ciò ha permesso di dare un apporto all'iter di negoziazione del Codice di condotta volontario degli Stati, approvato durante la Conferenza di Parigi dell'aprile 2025, che individua una serie di buone pratiche volte a controllare la diffusione di tali tecnologie e scongiurarne l'impiego pregiudizievole per la sicurezza nazionale, i diritti fondamentali dell'individuo e la stabilità del cyberspazio, salvaguardandone al contempo l'uso legale e legittimo, anche per finalità di cybersicurezza.

L'ACN ha, inoltre, preso parte all'incontro del Gruppo di Paesi *like-minded* sulla deterrenza cyber, organizzato a Roma dal MAECI con il contributo dell'Agenzia e del DIS, da cui è emersa l'importanza della cooperazione nella

protezione delle reti digitali come fattore di deterrenza. Il Gruppo di Paesi *like-minded* sulla deterrenza cyber è un'iniziativa informale e multilaterale, nata nel 2019 con l'obiettivo di rafforzare la cooperazione diplomatica e la condivisione delle informazioni per prevenire attività cibernetiche dannose e coordinare le risposte globali.

Inoltre, l'Agenzia ha collaborato con la Farnesina a definire il contributo nazionale alle quattro sessioni annuali dell'*Informal Working Group on Cyber Issues* dell'OSCE (Organizzazione per la sicurezza e la cooperazione in Europa), che promuove l'attuazione delle 16 *Confidence-Building Measure* (CBM) concordate dai suoi membri. In tale contesto, l'Agenzia ha alimentato il canale di comunicazione stabilito tra i punti di contatto nazionali in ottemperanza alla CBM8, condividendo informazioni su vulnerabilità cyber a favore di membri che ne avevano fatto richiesta.

In ambito Nazioni Unite, l'ACN ha partecipato con il MAECI alle sessioni del Gruppo di lavoro aperto sulla cybersicurezza (*Open-Ended Working Group*-OEWG), compresa l'ultima, di luglio, ad esito della quale gli Stati membri hanno approvato il Rapporto finale istitutivo di un nuovo "Meccanismo permanente sulle tecnologie dell'informazione e comunicazione nell'ambito della sicurezza internazionale e della promozione del comportamento responsabile degli Stati nell'uso delle ICT". Sempre a livello ONU, l'Agenzia ha, inoltre, seguito con la Farnesina i lavori preliminari per la costituzione dei due nuovi meccanismi di *governance* internazionale dell'intelligenza artificiale: il Panel scientifico internazionale indipendente e il Dialogo globale sulla *governance* dell'IA. Queste piattaforme mirano a favorire un approccio condiviso e responsabile allo sviluppo e all'uso dell'IA, rafforzando la cooperazione tra Stati, comunità scientifica e attori privati.

In ambito NATO, insieme a MAECI e Ministero della difesa, l'ACN anche nel 2025 ha seguito le attività del *Cyber Defence Committee*, curando gli aspetti di resilienza cibernetica all'interno del più ampio dibattito sull'evoluzione delle politiche in materia di difesa cyber. Mettendo a disposizione il proprio osservatorio sulla minaccia cyber e la capacità di coordinare diverse Amministrazioni e di interagire agilmente con operatori economici, l'Agenzia ha fornito il proprio apporto all'esercizio annuale *Cyber Defence Pledge* e partecipato alla Conferenza di presentazione dei risultati. In continuità con gli anni passati, l'ACN ha anche integrato le delegazioni nazionali delle principali conferenze di cybersicurezza organizzate annualmente dall'Alleanza: la *NATO Enterprise Cybersecurity Conference* e l'*Annual Cyber Defence Conference*. Infine, l'Agenzia partecipa, insieme al MAECI e al Ministero della difesa, alla *Transatlantic Quantum Community* della NATO che riunisce esperti di tecnologie quantistiche provenienti anche dall'industria, dal mondo accademico, dagli enti di finanziamento e dagli istituti di ricerca.

6.2 L'ACN E L'UNIONE EUROPEA

L'Agenzia attribuisce un'importanza centrale alla collaborazione in ambito UE, sia per quanto riguarda le iniziative di *policy* e strategiche, sia riguardo ai molteplici forum di livello tecnico.

Con l'obiettivo di valorizzare le numerose iniziative realizzate dall'ACN e di condividere aspetti strategici di reciproco interesse, il Direttore generale dell'Agenzia ha incontrato il Commissario europeo per gli Affari interni e l'immigrazione, Magnus Brunner, con il quale sono stati affrontati temi quali la protezione delle infrastrutture critiche, con particolare riguardo a una panoramica sull'attuazione della Direttiva NIS2, il Piano d'azione europeo sulla cybersicurezza degli ospedali e dei prestatori di servizi di assistenza sanitaria e il contrasto alla minaccia *ransomware*. Si è svolto, inoltre, un incontro con il Direttore della DG CONNECT (Direzione generale della Commissione europea per le reti di comunicazione, i contenuti e le tecnologie), Roberto Viola, che ha permesso di approfondire il progetto dell'*AI Factory* IT4LIA, la proposta italiana di istituire sul proprio territorio una *AI Gigafactory* e la prossima definizione degli standard europei per l'intelligenza artificiale.

Anche alla luce delle nuove competenze attribuite all'ACN in materia di intelligenza artificiale, il 2025 ha visto un significativo impegno per l'implementazione del Regolamento (UE) 2024/1689 (*AI Act*) attraverso l'operatività del Consiglio europeo per l'IA (il cosiddetto *AI Board*). In tale organismo, composto da rappresentanti dei 27 Stati membri dell'UE, dal Garante europeo della protezione dei dati in veste di osservatore e dall'Ufficio per l'IA della Commissione, l'Italia è oggi rappresentata dall'Agenzia e dall'AgID che, conseguentemente, prendono parte a tutte le relative attività. L'ACN, in qualità di Autorità di vigilanza del mercato nazionale e punto unico di contatto con le istituzioni UE, ha provveduto a fornire alla Commissione aggiornamenti sullo stato di implementazione dell'*AI Act* con riguardo agli aspetti di *governance* nazionale, nonché a comunicare le autorità nazionali competenti ad applicare l'*AI Act*.

Inoltre, il rilevante ampliamento del novero dei sottogruppi tematici dell'*AI Board* dedicati a specifici ambiti tecnici e regolatori, che si è registrato nel 2025, ha richiesto un coinvolgimento a tutto spettro da parte dell'ACN. L'Agenzia fornisce il proprio contributo – congiuntamente ad altre Amministrazioni competenti per materia, in primis AgID, nonché DTD, Banca d'Italia, CONSOB e IVASS – a 14 dei 15 sottogruppi esistenti (Figura 1).

Figura 1 – Sottogruppi dell'*AI Board* cui partecipa l'ACN

Con lo scopo di ricevere utili contributi da portare ai tavoli dei vari sottogruppi tematici, durante tutto l'anno l'Agenzia ha promosso costanti interlocuzioni con i vari *stakeholder*, istituzionali e privati. Ciò ha consentito, in particolare, di sostenere la redazione di documenti che sono stati concordati nel corso del 2025, come il Codice di buone pratiche per i sistemi di IA per scopi generali (GPAI), nonché le Linee guida sulle pratiche proibite e quelle per i fornitori di modelli GPAI. In altri casi è previsto che il confronto all'interno dei sottogruppi si concretizzi in specifici documenti già nel 2026, come nel caso del Codice di buone pratiche sulla trasparenza e la mappatura degli standard internazionali per l'attuazione dell'*AI Act*. L'Agenzia ha, inoltre, potuto condividere i progressi nazionali in materia di *sandbox* per la sperimentazione normativa sull'intelligenza artificiale evidenziando le sinergie con i progetti IT4LIA e EUSAiR (vedasi Capitolo 5).

HWPCI

L'Agenzia ha profuso ogni sforzo per rafforzare – sempre in stretto raccordo con il MAECI e, in particolare, con la Rappresentanza Permanente d'Italia presso l'Unione europea – il proprio contributo ai lavori dell'*Horizontal Working Party on Cyber Issues* (HWPCI) del Consiglio dell'UE, per la trattazione di dossier non solo normativi ma anche di *policy*. Nel corso del 2025, si è lavorato all'elaborazione di un piano per la gestione delle crisi cyber, nonché di un piano per la cybersicurezza in ambito sanitario.

La nuova Raccomandazione del Consiglio sul Piano europeo per la gestione delle crisi in materia di cybersicurezza (*Cyber Blueprint*) mira a migliorare la gestione degli incidenti e delle crisi cyber su vasta scala a livello dell'Unione europea. Il documento, adottato il 6 giugno in occasione del Consiglio trasporti, telecomunicazioni ed energia, recepisce i contributi forniti dall'ACN, con particolare riguardo alla necessità di rafforzare il ruolo delle reti europee di gestione di incidenti e crisi cyber. Un primo banco di prova del nuovo *Blueprint* è stato rappresentato dalla relativa esercitazione di tipo *table-top*, illustrata nel Capitolo 3.

FOCUS

Cyber Blueprint

La Raccomandazione costituisce una versione aggiornata del precedente framework del 2017, il cui impianto complessivo è stato rivisto alla luce del mutato quadro legislativo europeo. Si è, infatti, posta l'esigenza di allineare il Blueprint rispetto alla Direttiva NIS2, vista anche la formalizzazione della rete EU-CyCLONe, e al Cyber Solidarity Act che ha introdotto una rete di poli informatici (c.d. cyber hub) che compongono il sistema europeo di allerta per la cybersicurezza.
Il nuovo Blueprint chiarisce la ripartizione delle responsabilità tra i diversi livelli di gestione delle crisi: tecnico, affidato alla rete dei CSIRT nazionali; operativo, attribuito a EU-CyCLONe per il coordinamento tra Stati membri e istituzioni UE; politico-strategico, esercitato dal Consiglio dell'Unione europea anche attraverso l'eventuale attivazione del meccanismo IPCR (Integrated Political Crisis Response). Il documento mira, inoltre, a promuovere una cooperazione più strutturata tra attori civili e militari.

Il Piano d'azione europeo sulla cybersicurezza degli ospedali e dei prestatori di servizi di assistenza sanitaria, pubblicato il 15 gennaio, ha l'obiettivo di rafforzare la preparazione e la resilienza dell'UE e degli Stati membri per far fronte agli attacchi di natura cyber e ibrida in un settore estremamente sensibile come quello sanitario. Al riguardo, l'ACN ha fornito il proprio contributo segnalando la necessità di garantire mirate campagne di sensibilizzazione, nonché di dotare gli ospedali di infrastrutture, tecnologie e personale formato che possano concorrere all'obiettivo di una maggiore cybersicurezza. Quanto all'attuazione nazionale del Piano, l'ACN si sta confrontando attivamente con il Ministero della salute in qualità di Autorità di settore NIS.

EU-CyCLONe

Nel quadro della gestione delle crisi di cybersicurezza a livello di Unione europea, l'Agenzia continua a rappresentare l'Italia all'interno della rete EU-CyCLONe

(*European Cyber Crisis Liaison Organisation Network*), istituita nel 2020 e formalmente riconosciuta dalla Direttiva NIS2 quale strumento di riferimento per il coordinamento operativo degli incidenti e delle crisi cyber su vasta scala. La rete assicura il regolare e strutturato scambio di informazioni tra gli Stati membri e con le istituzioni, gli organi e gli organismi dell'Unione, a supporto di una risposta europea coerente e tempestiva.

Nel corso del 2025, l'ACN ha preso parte in maniera continuativa alle attività di coordinamento della rete, contribuendo sia alle riunioni operative, sia ai lavori di sviluppo e consolidamento dei meccanismi comuni di gestione delle crisi. Ciò in particolar modo nell'ambito delle attività esercitative della rete, per le quali l'ACN guida il *Working Group* dedicato all'organizzazione e alla pianificazione. Tali fruttuose attività hanno trovato una sintesi significativa nell'esercitazione BlueOLEx25, organizzata dal citato *Working Group* nel mese di novembre (vedasi Capitolo 3).

In continuità con il lavoro avviato negli anni precedenti, sono stati ulteriormente affinati i processi operativi e le procedure standard di gestione delle crisi, con particolare attenzione alle modalità di interazione tra il livello operativo, tecnico e politico dell'Unione. L'ACN ha inoltre contribuito alle attività di valutazione complessiva del lavoro della rete, anche a supporto delle iniziative di rendicontazione e indirizzo verso le istituzioni europee.

CSIRTs Network

L'Agenzia, attraverso il CSIRT Italia, ha proseguito e rafforzato la propria partecipazione all'interno del *CSIRTs Network*, la rete dei CSIRT dei 27 Stati membri dell'Unione europea istituita dalla Direttiva NIS e ulteriormente valorizzata dalla Direttiva NIS2. La rete continua a rappresentare un elemento cardine per il coordinamento tecnico-operativo a livello europeo, contribuendo al rafforzamento della capacità di prevenzione, rilevazione e risposta agli incidenti di cybersicurezza che possono colpire infrastrutture critiche e servizi essenziali.

In tale contesto, prevalentemente tecnico, il CSIRT Italia ha operato in costante raccordo con gli omologhi degli altri Stati membri tramite canali dedicati, assicurando una partecipazione continuativa alle riunioni plenarie e agli incontri di coordinamento della rete. Tali momenti di confronto hanno consentito di condividere informazioni su minacce emergenti, vulnerabilità significative e incidenti di sicurezza rilevanti, favorendo una comune consapevolezza situazionale a livello europeo.

Nel corso dell'anno, il CSIRT Italia ha anche preso parte attivamente ai gruppi di lavoro tematici del *CSIRTs Network*, contribuendo allo sviluppo e al miglioramento delle procedure operative, dei meccanismi di cooperazione e degli strumenti tecnici utilizzati dalla rete. Questo contributo ha sostenuto il progressivo rafforzamento dell'efficacia complessiva del *Network*, in linea con l'evoluzione del contesto della minaccia e con le esigenze di una gestione sempre più integrata e tempestiva degli incidenti cyber transfrontalieri.

NIS Cooperation Group

L'Agenzia partecipa al Gruppo di cooperazione NIS (*NIS Cooperation Group*-NISCG), creato dall'omonima Direttiva per favorire l'applicazione uniforme e concreta della normativa, attraverso discussioni tra gli specialisti delle autorità NIS dei vari Stati membri su questioni trasversali e di settore.

I lavori del NISCG si articolano, oltre che nelle riunioni plenarie, nelle attività condotte in oltre 15 *Work Stream* su aspetti orizzontali e settoriali specifici all'attuazione della disciplina NIS, nonché su specifiche tematiche come la crittografia post-quantistica. Inoltre, è stato assicurato il co-coordinamento di due gruppi di lavoro di particolare rilievo: quello inerente alla sicurezza del settore delle telecomunicazioni, con specifico riguardo all'attuazione del *Toolbox* 5G, nonché quello relativo allo sviluppo delle analisi del rischio cyber a livello europeo.

Nel corso del 2025, le attività coordinate dall'ACN o per le quali è stata assicurata una partecipazione attiva hanno dato luogo all'elaborazione dell'*ICT Toolbox* sulla

supply chain e a due documenti sulla valutazione del rischio, rispettivamente sui veicoli autonomi connessi e sui *detection equipment*.

Inoltre, anche nell'ottica di rafforzare il posizionamento dell'Italia a livello UE, capitalizzando sull'esempio virtuoso nel contesto del recepimento della Direttiva NIS2, si sono sviluppate molteplici attività di condivisione dell'approccio nazionale con omologhi di altri Stati membri.

Un ultimo filone di attività cui l'Agenzia ha fornito il proprio contributo è stata la revisione tra pari a favore di Cipro, primo esercizio pilota della procedura che ha permesso lo scambio di informazioni sulle migliori pratiche di recepimento della Direttiva NIS2, nonché su capacità e politiche in materia di cybersicurezza.

ECCC

L'ACN continua ad assicurare la rappresentanza italiana nel *Governing Board* dell'ECCC, nei suoi gruppi di lavoro tematici e nella rete europea degli NCC. In particolare, nel corso del 2025 è stata assunta da parte dell'Agenzia la guida del gruppo di lavoro dedicato al tema dei *cyber hub*, per assicurare continuità con le attività già avviate con i progetti ENSOC e CHIEF e in virtù dell'esperienza già acquisita per la realizzazione del *cyber hub* nazionale, l'HyperSOC (vedasi Capitolo 5).

Tra i principali risultati conseguiti dal *Governing Board* nel 2025 vi è l'adozione del *DEP Cybersecurity Work Programme 2025-2027*, contenente le azioni in cybersicurezza finanziate nel triennio. Il programma prevede l'allocazione di un budget di 355 milioni di euro per supportare iniziative strategiche, tra cui le *AI Gigafactory* e i *cable hub* regionali. L'ACN ha contribuito a portare le priorità italiane all'interno delle discussioni nel *Governing Board*. L'adozione di tale documento e il conseguimento dell'autonomia finanziaria a fine 2024 dimostrano il consolidamento del ruolo dell'ECCC, responsabile dell'attuazione delle parti relative alla cybersicurezza dei programmi DEP e *Horizon Europe*, nonché dell'adozione dei relativi *Work Programmes*. In tale ambito, l'Agenzia ha potuto contribuire alla definizione delle priorità strategiche di investimento, sostenendo l'importanza di assegnare adeguati fondi per le PMI e il settore sanitario.

Ulteriore testimonianza dell'accresciuto posizionamento dell'ECCC è stata anche l'organizzazione della riunione congiunta degli organi direttivi dell'ECCC e di ENISA a Varsavia l'8 aprile. I membri dei due consessi hanno avuto l'opportunità di discutere nuove opportunità di collaborazione e questioni chiave, tra cui l'attuazione del *Cyber Solidarity Act*, le priorità di ricerca e innovazione e lo sviluppo di competenze in cybersicurezza.

Inoltre, dall'1 al 3 luglio, l'ACN ha ospitato, in qualità di NCC italiano, il tredicesimo *meeting* del *Governing Board* dell'ECCC e della rete europea degli NCC. Tale riunione ha consentito di approfondire le discussioni sugli obiettivi strategici e le prospettive di lungo periodo del Centro europeo, anche in considerazione dei nuovi programmi di finanziamento che saranno avviati dal 2027.

ECCG

La collaborazione europea dell'Agenzia si estende anche allo *European Cybersecurity Certification Group*, che riunisce le varie Autorità nazionali di certificazione della cybersicurezza dei Paesi UE per portare avanti quanto previsto dal *Cybersecurity Act* in tema di certificazione della cybersicurezza. In tale contesto, l'ACN segue da vicino le attività riguardanti i sistemi di certificazione europei, a partire dall'EUCC, già approfondito nel Capitolo 4. A tale riguardo, sono stati esaminati anche i profili di interconnessione tra il sistema europeo e quello internazionale basato sull'accordo di mutuo riconoscimento CCRA, che comprende 36 agenzie governative di Paesi di tutto il mondo.

Parallelamente, l'Agenzia partecipa anche al *Crypto Working Group* dell'ECCG, nel cui ambito ha contribuito alla definizione dell'*Agreed Cryptographic Mechanisms*, ovvero il documento di riferimento per sviluppatori e valutatori sui criteri di certificazione europei, contenente gli schemi crittografici riconosciuti validi da tutti i partecipanti al

gruppo. Tali attività rafforzano il ruolo dell'ACN nel panorama europeo della sicurezza digitale, garantendo coerenza, qualità e uniformità nei processi di certificazione crittografica. Concordare standard internazionali condivisi è anche al centro delle attività del *Crypto Working Group* in ambito *Common Criteria*, che ha l'obiettivo di armonizzare e definire le procedure di certificazione e valutazione di prodotti ICT per dettare le raccomandazioni sugli schemi crittografici e le metodologie di test per verificare la corretta implementazione delle funzionalità crittografiche presenti in prodotti oggetto di certificazioni CCRA.

ENISA

Nell'ambito delle attività di ENISA, l'ACN, oltre all'assidua partecipazione ai lavori del suo *Management Board* e della rete dei funzionari nazionali di collegamento (*National Liaison Officer*), ha aderito a un gruppo per l'aggiornamento della Strategia internazionale di ENISA. In tale contesto, si è sottolineata l'importanza che l'Agenzia europea continui a essere coinvolta nel gruppo di lavoro del G7 dedicato alla cybersicurezza. Nel corso del 2025 le attività sono proseguite per la predisposizione di documenti di indirizzo strategico, successivamente portati all'approvazione del *Management Board*.

Ulteriori formati

Quanto all'apporto dell'ACN alle attività europee in ambito di difesa cyber, è stato fornito il contributo di competenza al *Cyber Census 2025*, che monitora l'attuazione, a livello nazionale, della Politica UE sulla *cyber defence* e delle relative Conclusioni del Consiglio. Il Direttore generale dell'Agenzia ha, inoltre, partecipato agli Stati generali difesa, spazio e *cybersecurity*, organizzati dal Parlamento europeo e dalla Commissione, in collaborazione con l'Agenzia spaziale europea. L'evento, che ha visto la partecipazione anche di aziende nazionali del settore, ha consentito un confronto su innovazione, competitività industriale, economie di scala ed efficienza della spesa, oltre che sulla sicurezza dei cittadini e la protezione delle infrastrutture critiche.

L'ACN ha, infine, partecipato alle riunioni dei Direttori delle Agenzie europee per la cybersicurezza (*Cybersecurity Directors Meeting*), gestite dal BSI tedesco e alle quali partecipano anche Regno Unito e Ucraina, oltre agli Stati membri dell'UE. In tale contesto, l'Agenzia ha sostenuto una Dichiarazione congiunta, in cui si sottolinea l'importanza di valorizzare le esperienze nazionali degli Stati membri nel processo decisionale a livello dell'Unione, enfatizzando la necessità di garantire l'effettiva e uniforme attuazione della legislazione in ambito cyber, nonché di preservare l'approccio orizzontale della Direttiva NIS2 per mantenere un quadro armonizzato e coerente in tutti i settori.

6.3 COOPERAZIONE BILATERALE

L'ACN, d'intesa con il MAECI, ha esteso, in maniera strutturata, la rete di rapporti bilaterali con autorità cyber in aree di interesse strategico, in linea con le priorità della politica estera nazionale.

Fra le interazioni a livello di vertice, si segnalano in particolare le visite in Agenzia del Ministro per la giustizia, gli affari interni e la migrazione della Repubblica d'Irlanda, del Ministro della Pubblica Amministrazione del Montenegro, del Ministro Capo del Gabinetto di Sicurezza istituzionale del Brasile, dell'Assistente Segretario generale della NATO per la cybersicurezza e del Direttore generale dell'autorità cyber del Ghana. Numerose sono state anche le occasioni di incontro e interazione con Ambasciate e Rappresentanze estere a Roma.

Nel 2025, l'ACN ha siglato due nuovi protocolli d'intesa che allargano il campo delle collaborazioni avviate negli anni precedenti (Figura 2). Il primo, con l'Autorità di sicurezza cyber della Grecia, è funzionale a rafforzare la protezione di infrastrutture critiche transfrontaliere e la sicurezza della connettività nel Mediterraneo. Il secondo protocollo è stato siglato con il Servizio di Stato per le comunicazioni speciali e la protezione delle informazioni dell'Ucraina (SSSCIP), per la condivisione di elementi sulla minaccia, lezioni apprese e buone pratiche cyber.

Figura 2 – Accordi di collaborazione internazionali dell'ACN

L'Agenzia ha dato, inoltre, attuazione ai protocolli d'intesa precedentemente conclusi con le omologhe agenzia di Spagna (INCIBE), Tunisia (ANCS), Albania (AKSK), Romania (DNSC) e del Governatorato dello Stato della Città del Vaticano. In particolare, tali protocolli hanno permesso confronti strutturati in merito a diversi temi, inclusi lo scambio informativo sui rischi cibernetici, i meccanismi di gestione delle crisi cyber, le priorità di cybersicurezza in occasione di grandi eventi e le iniziative formative. Sono stati, inoltre, avviati dialoghi strategici finalizzati a future intese con gli omologhi centri cyber di alcuni Paesi del Golfo (Arabia Saudita, Emirati Arabi Uniti, Qatar e Oman) e del Ghana.

Le interlocuzioni di natura operativa e specialistica sono cresciute in maniera proporzionale all'estensione della rete di partenariati. Il tema della cybersicurezza dei Giochi olimpici, in preparazione alle Olimpiadi invernali di Milano Cortina 2026, è stato al centro della cooperazione con le agenzie per la cybersicurezza di Francia (ANSSI) e Stati Uniti (CISA) e con altre autorità estere di sicurezza. Con l'ANSSI è stato, inoltre, approfondito il dialogo sulla cybersicurezza delle infrastrutture critiche transfrontaliere, mentre con il Centro per la cybersicurezza del Belgio (CCB) si è stabilito un canale d'*infosharing* dedicato. È, infine, proseguita l'interlocuzione con le autorità cyber indiane, secondo gli esiti del primo Dialogo cyber India-Italia del 2024, contribuendo alle attività preparatorie dell'*India AI Impact Summit 2026*.

Notevole, infine, è l'attenzione riservata dall'Agenzia al rafforzamento delle capacità in materia cyber di Paesi di interesse strategico, importante volano della propria proiezione all'estero. In partnership con il MAECI, l'ACN ha organizzato la seconda Conferenza nazionale sul *cyber capacity building*, svoltasi a Roma il 5 dicembre. Nel corso della Conferenza, sono stati presentati i progressi realizzati nell'istituzione dell'ecosistema nazionale di *capacity building* in ambito cybersicurezza, discutendo le opportunità di sviluppo attraverso collaborazioni pubblico-privato, con un focus sui Balcani occidentali, l'Ucraina e l'Africa. A tale riguardo, in collaborazione con la Fondazione Med-Or, l'ACN ha anche avviato il progetto di *cyber capacity building CyberBridge* rivolto a Paesi africani, in coerenza con le priorità del Piano Mattei (vedasi Capitolo 7).

7

La formazione e la promozione della cultura della cybersicurezza

L'Agenzia per la cybersicurezza nazionale, anche nel corso del 2025, ha operato per accrescere la formazione cyber tra gli studenti, espandere le conoscenze dei lavoratori e favorire comportamenti digitali responsabili da parte dei cittadini.

Varie sono state le iniziative di formazione, di divulgazione e di sensibilizzazione realizzate in sinergia con soggetti pubblici e privati per la diffusione di competenze specialistiche e l'affermazione di una solida cultura della sicurezza informatica.

In un contesto caratterizzato da minacce cibernetiche in costante evoluzione, tali attività assumono un ruolo determinante nel consolidare la capacità nazionale di prevenire e contrastare gli incidenti informatici e porre al centro il fattore umano come primo baluardo difensivo per prevenire e mitigare eventi e incidenti cyber. Gli attacchi informatici sfruttano, infatti, non solo vulnerabilità tecniche, ma anche comportamenti inconsapevoli, errori umani e carenze di conoscenza.

La sicurezza cibernetica dipende, quindi, in misura rilevante dalle modalità con cui le tecnologie vengono concretamente utilizzate e dai comportamenti dei soggetti che operano all'interno dei sistemi digitali, siano essi professionisti o utenti. In tale prospettiva, la formazione continua e la diffusione della consapevolezza assumono una funzione centrale per rafforzare la capacità di riconoscere i rischi, adottare comportamenti responsabili e contribuire in modo attivo alla prevenzione e alla gestione degli eventi cyber. Investire nelle iniziative di formazione e *awareness* in materia di cybersicurezza significa sviluppare una forza lavoro adeguatamente preparata e una cittadinanza consapevole, in grado di impiegare in modo più sicuro gli strumenti digitali e di contribuire alla resilienza complessiva del Paese.

7.1 LE INIZIATIVE DI FORMAZIONE

Nel corso del 2025, l'Agenzia ha ampliato in modo significativo la portata e l'impatto delle iniziative formative avviate negli anni precedenti, nella consapevolezza che intervenire sul fattore umano contribuisce a rendere il Paese più resiliente agli attacchi cibernetici e pronto in termini di autonomia tecnologica. Le diverse attività hanno consolidato percorsi strutturati volti alla creazione di una forza lavoro nazionale altamente qualificata, capace di rispondere alle esigenze di imprese e Pubbliche Amministrazioni e di operare con competenze avanzate nell'ambito delle tecnologie informatiche e della sicurezza cibernetica.

A tal fine, l'Agenzia si è impegnata particolarmente per rafforzare le competenze dei dipendenti della PA: si è, infatti, contribuito ad ampliare ulteriormente la platea dei destinatari a cui sono stati offerti elementi facilmente accessibili di approfondimento delle conoscenze, al fine di rafforzare la capacità delle Amministrazioni di riconoscere e gestire i rischi cyber in modo consapevole e tempestivo.

Un altro *target* prioritario delle attività formative dell'Agenzia è stato rappresentato dagli studenti a tutti i livelli, con l'obiettivo di metterli nelle condizioni di operare nell'ambito della cybersicurezza. Oltre a iniziative indirizzate a giovani e ragazzi di scuole, università e Istituti tecnologici superiori (ITS), l'impegno dell'ACN ha riguardato anche la formazione del personale scolastico, considerando che sostenerne le competenze costituisce un presupposto essenziale per diffondere un utilizzo consapevole e sicuro delle tecnologie digitali a beneficio dell'intero sistema scolastico.

Formazione per i dipendenti della PA

SNA

+1.200

personale della Pubblica Amministrazione centrale e locale

MIM

+900

dirigenti e docenti degli istituti scolastici

MAECI

+1.100

persone appartenenti al personale diplomatico

Vademecum

12

buone pratiche di *cybersecurity* di base

7.1.1 La formazione per i dipendenti delle Pubbliche Amministrazioni

Numerose sono state le iniziative di formazione rivolte alla Pubblica Amministrazione nel 2025, in considerazione dell'elevata esposizione di questa al rischio cyber. In particolare, l'ACN ha consolidato la collaborazione con la Scuola nazionale dell'Amministrazione (SNA), curando la realizzazione di percorsi formativi strutturati, destinati ai dipendenti delle PA centrali e locali. Tali percorsi hanno affrontato, accanto ai temi tradizionali della sicurezza delle reti e dei sistemi informativi, anche profili connessi alla gestione del rischio cyber, alla continuità operativa dei servizi e all'impiego dell'intelligenza artificiale nei procedimenti amministrativi, con riguardo alla trasparenza delle decisioni, alla prevenzione di effetti discriminatori, alla responsabilità e alla gestione dei dati. Le iniziative realizzate con la SNA hanno raggiunto oltre 1.200 partecipanti, contribuendo al rafforzamento complessivo della capacità amministrativa e alla protezione cyber.

Formazione SNA: il contributo dell'Agenzia

Principali moduli e corsi

- Architettura di cybersicurezza – Ruolo e funzioni dell'ACN – *Cyber hygiene*
- Gestire la sicurezza nella PA
- Cybersicurezza e IA – Corso sistemi decisionali e supporto alla PA: il ruolo dei dati e dell'intelligenza artificiale
- Cybersicurezza e IA – Video lezioni per il 10° Corso-concorso per dirigenti della PA
- Cybersicurezza per la PA: elementi introduttivi per neo-dirigenti
- Introduzione alla cybersicurezza
- La sicurezza dei dati nella PA
- Dati e intelligenza artificiale

Parallelamente, l'Agenzia, in collaborazione con il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri, ha predisposto un Vademecum sulle buone pratiche di *cybersecurity* di base; si tratta di 12 indicazioni semplici e concrete, dedicate a orientare i dipendenti pubblici verso comportamenti sicuri e consapevoli da adottare ogni giorno. Per la diffusione del Vademecum – pubblicato su Syllabus, la piattaforma dedicata al rafforzamento del capitale umano delle PA – l'Agenzia ha curato la realizzazione di video pillole, progettate per essere fruibili in modo agile e immediato, che hanno affrontato temi chiave della cybersicurezza favorendo un apprendimento continuo e diffuso da parte dei dipendenti della PA.

Al fine di raggiungere una sempre maggiore capillarità sul territorio e una crescente diffusione tra settori strategici, l'Agenzia ha realizzato iniziative di formazione anche in favore dell'Associazione nazionale dei Comuni italiani (ANCI), dell'Unione nazionale Comuni, comunità ed enti montani, di alcune Aziende regionali della salute e dell'E-NAV. Sono state, altresì, realizzate specifiche sessioni destinate alle Forze Armate e alle forze dell'ordine nel contesto di percorsi formativi del Centro alti studi difesa.

La formazione del personale diplomatico

Misura #69

In attuazione della misura #69 del Piano di implementazione della Strategia nazionale di cybersicurezza 2022-2026, volta a potenziare la formazione del personale diplomatico così da rafforzare le capacità di *cyber diplomacy*, è stata avviata una collaborazione con il MAECI al fine di organizzare corsi di formazione e diffusione della cultura della cybersicurezza.

Nello specifico, sono stati predisposti due percorsi formativi:

- il primo, da remoto e in modalità asincrona, articolato in 3 moduli didattici, a cui hanno partecipato oltre 1.100 dipendenti;
- il secondo, in presenza, da svolgersi nel 2026 presso la sede dell'Agenzia, destinato ai Segretari e Consiglieri di legazione di nuova nomina.

7.1.2 La formazione per il personale del settore scolastico

Nel corso del 2025 sono proseguite le attività di collaborazione con il Ministero dell'istruzione e del merito (MIM) avviate all'indomani della sottoscrizione del Protocollo d'intesa del dicembre 2024 che mira a favorire, presso tutte le istituzioni scolastiche, lo sviluppo e la realizzazione di iniziative riguardanti attività didattiche e formative di promozione della cultura della cybersicurezza.

Sul solco di tale sinergia, è stato avviato un progetto pilota con l'Ufficio scolastico regionale del Lazio per l'organizzazione di percorsi di sensibilizzazione in materia di cybersicurezza riservati a dirigenti e docenti degli istituti scolastici di ogni ordine e grado. L'iniziativa prevede il coinvolgimento di oltre 900 dipendenti del MIM e si pone l'obiettivo di affrontare tematiche che vanno dall'informatica di base alla cybersicurezza, senza tralasciare l'intelligenza artificiale.

In particolare, il corpo docente svolge un ruolo decisivo nel trasferire competenze, orientare gli studenti e vigilare sui loro comportamenti online, rendendo imprescindibile un aggiornamento continuo e qualificato. Supportare la preparazione dei docenti significa consolidare un sistema educativo capace di affrontare con maturità e sicurezza le sfide del digitale.

Considerato lo stretto legame tra la materia della cybersicurezza e la *data protection*, l'ACN, d'intesa con associazioni impegnate in ambiti quali la riservatezza dei dati personali, ha organizzato una formazione mirata dedi-

cata al personale amministrativo delle scuole, nell'ottica di aumentare la consapevolezza di quanto, nel mondo digitale, solo attraverso corretti comportamenti si possono prevenire gravi violazioni della *privacy*.

7.1.3 Le attività di formazione rivolte agli studenti

Le iniziative di formazione realizzate dall'Agenzia a sostegno degli studenti sono state rivolte a stimolare la creazione di competenze nazionali necessarie per le imprese e per le Pubbliche Amministrazioni, con riferimento alle tecnologie informatiche in generale e a quelle relative alla sicurezza cibernetica in particolare.

In questo ambito, anche nel corso del 2025 è proseguita la collaborazione tra l'ACN e il Consorzio interuniversitario nazionale per l'informatica (CINI) nell'organizzazione e nel successivo monitoraggio di iniziative e competizioni nazionali in materia di cybersicurezza e innovazione tecnologica, nell'ottica di valorizzare le risorse specializzate in tali materie attraverso l'individuazione di giovani talenti tra studenti e studentesse. Nell'ambito della convezione con il CINI, l'Agenzia ha contribuito alla realizzazione di conferenze, dibattiti, seminari, attività di divulgazione e promozione, ivi inclusa l'organizzazione della filiera di formazione e addestramento del Laboratorio nazionale di *cybersecurity*, che include i programmi CyberChallenge, CyberCup, OliCyber, ITSCyberGame, CyberHighSchools, CyberTrials. Queste iniziative sono dedicate a specifici target studenteschi e prevedono attività di vario tipo, incluse competizioni pratiche tra diverse squadre.

Tali competizioni, tra le altre cose, hanno permesso di costruire la squadra nazionale dei *cyberdefender*, nota come TeamItaly, che nel 2025 si è aggiudicata la vittoria tra i 40 Paesi partecipanti all'undicesima edizione dell'*European Cybersecurity Challenge* (ECSC), campionato europeo di cybersicurezza organizzato da ENISA, che mira a coltivare le competenze in materia di sicurezza informatica riunendo i migliori talenti europei in questo campo.

Attraverso il programma OliCyber sono stati, inoltre, individuati i componenti della nazionale italiana chiamati a gareggiare nella prima edizione delle Olimpiadi internazionali di *cybersecurity*, tenutasi a giugno a Singapore tra le squadre di 30 Paesi. La nazionale italiana si è aggiudicata il primo posto come punteggio medio, conquistando 2 medaglie d'oro e 2 d'argento. Grazie ai risultati ottenuti in questa competizione, nonché all'esperienza maturata con l'organizzazione dell'ECSC a Torino nel 2024, l'Italia è stata selezionata per ospitare la terza edizione delle Olimpiadi internazionali di *cybersecurity* nel 2027.

Le competizioni di cybersicurezza nel 2025

CyberChallenge è il programma nazionale di formazione e competizione in cybersicurezza per studenti e studentesse dai 16 ai 24 anni. L'edizione 2025 ha coinvolto 40 università e accademie nazionali con il supporto di più di 500 istruttori tra professori, ricercatori, esperti del settore ed ex partecipanti e ha raccolto l'adesione di 3.000 iscritti di cui 810 ammessi al percorso di formazione della durata di 4 mesi. L'edizione si è conclusa con la competizione nazionale tenutasi a luglio a Torino con la vittoria del team della Sapienza Università di Roma.

OliCyber, Olimpiadi italiane di cybersicurezza, è un programma di formazione e competizione in cybersicurezza dedicato a studenti e studentesse degli istituti superiori. Nell'edizione 2025 vi sono stati più di 3.000 iscritti e 635 istituti coinvolti. Le competizioni sono state articolate in 3 fasi: a gennaio vi è stata la selezione dei partecipanti nelle scuole, a marzo si è svolta una selezione territoriale e, infine, a maggio la competizione nazionale con i 100 finalisti. Nell'ambito delle attività formative di OliCyber, sono stati organizzati, tra febbraio e marzo, 3 *training camp*, della durata di una settimana, destinati complessivamente a circa 450 studenti di tutto il Paese.

CyberHighSchools è un'iniziativa dedicata alle scuole superiori di II grado con l'obiettivo di attivare una rete tra questi istituti, offrire opportunità di formazione e interazione agli studenti e creare una *community* di docenti attenti alle tematiche cyber. L'iniziativa conta ormai 690 scuole federate al programma e più di 1.500 docenti aderenti. Nel 2025 si sono tenuti corsi di introduzione alla cybersicurezza per 400 docenti, 22 moduli avanzati per circa 1.100 docenti e 5 *workshop* tecnici a Bologna, Andria e Arezzo destinati a più di 500 studenti.

CyberCup è il torneo nazionale professionale di competizioni di cybersicurezza organizzato dalle squadre italiane afferenti a sedi universitarie, ideato con l'obiettivo di dare seguito al programma CyberChallenge e valorizzare maggiormente le competenze acquisite dai partecipanti, nonché le squadre createsi nelle università. L'edizione 2025 si è svolta da gennaio a giugno con più di 300 partecipanti provenienti da 17 squadre universitarie e 5 diversi *round* di competizioni. In concomitanza con la finale di luglio del programma CyberChallenge, si è poi svolto un *workshop* e la cerimonia di premiazione di CyberCup.

Nel 2025 si è tenuta la prima edizione di **ITSCyberGame**, programma di competizioni dedicato a studenti e studentesse degli ITS italiani. L'edizione pilota, a cui hanno partecipato oltre 260 studenti di 28 squadre da ITS di tutta Italia, ha visto, tra marzo e aprile, un campionato a squadre organizzato in 3 fasi di gironi di selezione presso gli ITS, e una finale in presenza per 138 finalisti di 16 squadre con una serie di sfide a eliminazione diretta organizzata presso l'ITS di Verona nel mese di aprile.

CyberTrials è un programma di formazione avanzata e *gaming* rivolto alle studentesse degli istituti superiori di II grado. Per partecipare non occorrono conoscenze tecniche pregresse, ma la curiosità di esplorare il mondo di Internet e della *cybersecurity*. L'edizione 2025 ha visto la partecipazione di circa 500 scuole superiori e la selezione, dopo una prima fase di formazione e prove online, di 100 studentesse che hanno partecipato alla fase finale in presenza, tenutasi a Verona nel mese di giugno. Le finaliste hanno affrontato un programma immersivo con esercitazioni e sfide investigative cyber, approfondimenti tematici, simulazioni di gioco e momenti di *mentoring*.

Particolare attenzione è stata, inoltre, dedicata alle categorie più fragili della società attraverso specifiche attività pensate e realizzate per persone con disabilità, grazie a una proficua collaborazione con Fondazioni senza scopo di lucro operanti anche nel contesto della *cybersecurity*. Tali iniziative formative, utili per il collocamento nel mondo del lavoro, hanno avuto l'obiettivo di far conoscere loro i principali rischi cibernetici e le migliori pratiche di *cyber hygiene*.

L'impegno dell'Agenzia per la formazione degli studenti si è rivolto anche al segmento post-diploma. In tale ottica, anche nel corso dell'anno in esame, è risultato strategico il rapporto con la rete degli ITS Academy che in Italia offrono ai propri studenti percorsi di formazione in cybersicurezza, programmazione, sistemi di intelligenza artificiale, *cloud*, crittografia. Per incentivare i percorsi di studio negli ITS, l'Agenzia ha anche finanziato l'erogazione di borse di studio dedicate.

Le iniziative a sostegno degli ITS

Misura #59

L'Agenzia ha avviato un percorso volto al sostegno degli ITS al fine di rispondere alle esigenze delle imprese di poter usufruire di nuove ed elevate competenze tecniche e tecnologiche. Tali attività si collocano nel solco della misura #59 del Piano di implementazione della Strategia nazionale di cybersicurezza 2022-2026 e si sono sostanziate in 2 linee di azione:

- finanziamento di 125 borse di studio, per complessivi 500.000 euro, volte a sostenere i percorsi in materia di cybersicurezza erogati dagli ITS Academy nel biennio 2024-2026;
- partecipazione di relatori dell'Agenzia a eventi inaugurali e di orientamento organizzati dalla rete degli ITS Academy della Sardegna e della Puglia che hanno visto la presenza di oltre 1.000 persone tra studenti, docenti e rappresentanti delle imprese di settore.

Molteplici sono stati, poi, gli interventi formativi realizzati nelle università come l'Università Roma Tre e il Campus Bio-Medico di Roma, nonché in istituti scolastici di ogni ordine e grado dislocati su tutto il territorio nazionale.

Nel corso del 2025, l'ACN si è, altresì, dotata di un Regolamento per lo svolgimento dei tirocini curriculari presso l'Agenzia. Il Regolamento prevede che venga preventivamente sottoscritta una convenzione tra l'ACN e l'università o l'ITS che intende offrire tali opportunità di tirocinio ai propri studenti. Sulla base di una ricognizione delle disponibilità per aree funzionali dell'Agenzia, inoltre, viene identificato il settore in cui sarà inserito il tirocinante, il quale viene seguito da un tutor dell'ACN, oltre che da un tutor designato dall'ente di provenienza. A seguito della pubblicazione del Regolamento, sono state stipulate le prime convenzioni con Atenei e ITS interessati ed è stata effettuata la rilevazione delle disponibilità delle strutture dell'Agenzia, attività propedeutiche per poter accogliere, già nel 2026, i primi tirocinanti.

7.2 LE INIZIATIVE DI CONSAPEVOLEZZA

L'importanza della consapevolezza dei rischi cyber è diventata ancora più evidente nel 2025, in un contesto in cui la dipendenza dalla tecnologia e dalla connettività è ulteriormente aumentata. Le minacce informatiche si sono moltiplicate, colpendo Pubbliche Amministrazioni, imprese e cittadini, e rendendo la consapevolezza del rischio un elemento essenziale per la protezione dei dati, la prevenzione degli incidenti e la continuità dei servizi.

La crescente sofisticazione degli attacchi ha confermato la necessità di rafforzare la cultura della sicurezza cibernetica. In questo quadro, l'Agenzia ha svolto un ruolo sempre più centrale nel promuovere comportamenti responsabili e sicuri, contribuendo a diffondere una maggiore attenzione ai rischi del cyberspazio.

Sebbene non sia possibile tracciare un confine netto tra le attività dedicate alla formazione e quelle volte alla promozione della cultura cyber, dato che il più ampio obiettivo di rafforzare le competenze e capacità nazionali richiede un approccio integrato e una visione olistica, i paragrafi che seguono riassumono le iniziative di natura più spiccatamente divulgativa. In tal senso, in continuità con le iniziative avviate nel 2024, nel 2025 l'Agenzia ha realizzato numerose attività di sensibilizzazione che hanno assunto un'importanza crescente.

7.2.1 Le campagne di *awareness*

Nel corso dell'anno, le campagne di *awareness* hanno via via acquisito un'importanza sempre maggiore, sia per l'ampiezza e il costante aggiornamento dei temi affrontati, sia per la capacità di raggiungere un pubblico più vasto e diversificato, contribuendo in modo significativo alla diffusione di una cultura della sicurezza digitale matura, condivisa e orientata, nonché al riconoscimento dell'Agenzia quale riferimento istituzionale primario.

Le diverse tappe delle campagne sono diventate progressivamente appuntamenti attesi, riconosciuti come momenti di confronto e aggiornamento di particolare rilievo per PA, operatori privati e cittadini. La crescente partecipazione e l'interesse manifestato dai destinatari hanno confermato la rilevanza di tali iniziative, strumenti essenziali per sensibilizzare il Paese sulle minacce emergenti e sulle buone pratiche da adottare nello spazio cibernetico.

Nell'anno in esame, l'Agenzia ha proceduto ad aggiornare il report "La minaccia cibernetica al settore sanitario", confermando come l'ambito sanitario continui a essere tra quelli maggiormente impattati in caso di attacchi cyber. Questi ultimi possono, infatti, dar luogo a incidenti in grado di generare un impatto sui servizi erogati, causandone talvolta il blocco con gravi ripercussioni ai danni dell'utenza e mettendo potenzialmente a rischio il diritto fondamentale alla salute. Proprio per diffondere la consapevolezza del rischio cyber in tale settore e illustrare i contenuti del report, l'ACN ha proseguito l'iniziativa cominciata a settembre 2024, partecipando anche nel 2025 a numerosi incontri divulgativi sul territorio che hanno toccato molte Regioni italiane (Lazio, Lombardia, Sicilia, Basilicata, Sardegna, Piemonte, Puglia, Abruzzo, Veneto, Marche, Campania) e coinvolto circa 4.000 professionisti impiegati in ospedali, centri medici, cliniche e altre strutture sanitarie.

La minaccia cibernetica al settore sanitario

Il rapporto, soggetto a revisione periodica, fornisce una panoramica sulle principali minacce cyber nel settore sanitario, nonché raccomandazioni e misure per potenziare la sicurezza informatica. La versione pubblicata nel 2025 evidenzia come nel corso dell'anno il numero complessivo degli eventi cyber sia aumentato di oltre il 40% rispetto al 2024. Tra le principali tipologie di minacce rilevate si segnalano: la scansione attiva su credenziali, il *phishing*, la compromissione delle caselle e-mail e l'esposizione dati. Ciò a conferma della centralità del vettore e-mail e dell'utilizzo di tecniche basate sull'ingegneria sociale per la diffusione di campagne malevole. Gli attacchi di tipo *ransomware*, nel 2025, sono diminuiti, anche se continuano a rappresentare la tipologia di minaccia con l'impatto più elevato.

Di estremo rilievo è stata, inoltre, la prosecuzione dell'iniziativa Roadshow PMI, ciclo di eventi sul territorio volti a sensibilizzare le piccole e medie imprese italiane sui rischi informatici e sulle soluzioni per una efficace protezione cyber. L'iniziativa nel 2025 ha toccato, in collaborazione con la rete di Confindustria e con i *Digital Innovation Hub* a livello territoriale, 7 città e si è conclusa con la tappa di Catania. Tali eventi hanno permesso, inoltre, la diffusione della campagna di comunicazione "Accendiamo la cybersicurezza. Proteggiamo le nostre imprese" realizzata dall'ACN e dal Dipartimento per l'informazione e l'editoria della Presidenza del Consiglio dei ministri per informare gli operatori economici e i loro clienti dell'importanza di essere preparati per affrontare i rischi cyber.

Tappe del Roadshow PMI

Nel complesso, il 2025 ha confermato la rilevanza di modelli sinergici per l'organizzazione di eventi finalizzati alla diffusione della cultura della sicurezza digitale.

Le collaborazioni con gli ordini professionali, avviate nel 2024, hanno dimostrato la solidità del percorso intrapreso e sono state ulteriormente ampliate con il coinvolgimento di nuovi attori istituzionali. In particolare, è stata attivata una collaborazione con il Consiglio nazionale degli ingegneri, che ha portato all'organizzazione di una giornata di formazione dedicata, caratterizzata da un'ampia partecipazione e da un riscontro estremamente positivo.

Inoltre, l'Agenzia ha promosso un'iniziativa di studio in favore di una delegazione di personale dirigenziale responsabile dei servizi IT della Presidenza della Repubblica, del Parlamento italiano ed europeo e della Corte costituzionale, che, oltre a una sessione presso l'ACN, ha previsto una simulazione presso la IBM Academy.

7.2.2 Il supporto all'inclusione digitale

Nel 2025 è stata realizzata una collaborazione con il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri nell'ambito del progetto "Rete dei servizi di facilitazione digitale". In tale contesto, l'ACN ha svolto attività di formazione agli operatori presso i c.d. "Punti di facilitazione digitale", istituiti sul territorio, attraverso l'erogazione di lezioni frontali e la divulgazione di materiali didattici dedicati. Si tratta di un intervento volto a formare i facilitatori digitali sui principali rischi cibernetici e sulle corrette pratiche di sicurezza informatica.

I soggetti formati hanno operato quali moltiplicatori di conoscenze, trasferendo le competenze acquisite agli utenti dei punti di facilitazione. In tal modo, l'intervento ha prodotto non soltanto benefici immediati sui destinatari diretti della formazione, ma ha contribuito a elevare il livello complessivo di consapevolezza e sicurezza digitale dell'intera comunità, raggiungendo in maniera indiretta un pubblico potenzialmente molto più ampio.

Il progetto ha perseguito l'obiettivo di sostenere efficacemente l'inclusione digitale, realizzando una nuova opportunità educativa rivolta a giovani e adulti per sviluppare le competenze digitali di base necessarie nel mondo del lavoro, nonché per la crescita personale, l'inclusione sociale e la cittadinanza attiva, come definite nel quadro europeo delle competenze digitali.

Il progetto E-Academy

Misura #62

In attuazione della misura #62 del Piano di implementazione della Strategia nazionale di cybersicurezza 2022-2026, l'ACN ha lanciato E-Academy sul proprio sito istituzionale al fine di diffondere conoscenze di sicurezza informatica e buone pratiche di *cyber hygiene*. Nell'ambito dell'iniziativa è stata curata la realizzazione di contenuti formativi e di *awareness* per offrire alla cittadinanza uno strumento affidabile di informazione e sensibilizzazione sulle tematiche della cybersicurezza, accessibile e in continuo aggiornamento.

L'E-Academy presenta contenuti formativi e informativi destinati a diversi *target* e categorie di lavoratori. In particolare, nella sua fase iniziale, E-Academy ha pubblicato video-pillole, realizzate in collaborazione con la Fondazione SERICS per rafforzare le competenze digitali della cittadinanza, nonché materiali informativi con indicazioni pratiche per chi opera nelle PMI.

7.3 LE ATTIVITÀ DI FORMAZIONE E *AWARENESS* INTERNAZIONALI

Al fine di consolidare la presenza dell'Italia nei tavoli di lavoro comunitari e internazionali anche in questo importante ambito, l'ACN ha partecipato ad attività promosse da ENISA quali le riunioni dell'*Awareness Raising and Cyber-Hygiene Ad-Hoc Working Group*, nonché alla seconda conferenza sulla consapevolezza in materia di cybersicurezza, organizzata a Zagabria nel mese di novembre, dal titolo "*Empowering the Human Element*". La partecipazione a tale conferenza europea ha permesso di rafforzare la collaborazione istituzionale tra l'ACN e i competenti uffici, istituzioni e agenzie UE e di esplorare come le tecnologie emergenti, le metriche di valutazione e le innovative metodologie di apprendimento possano contribuire a sostenere una maggiore consapevolezza cyber in Europa.

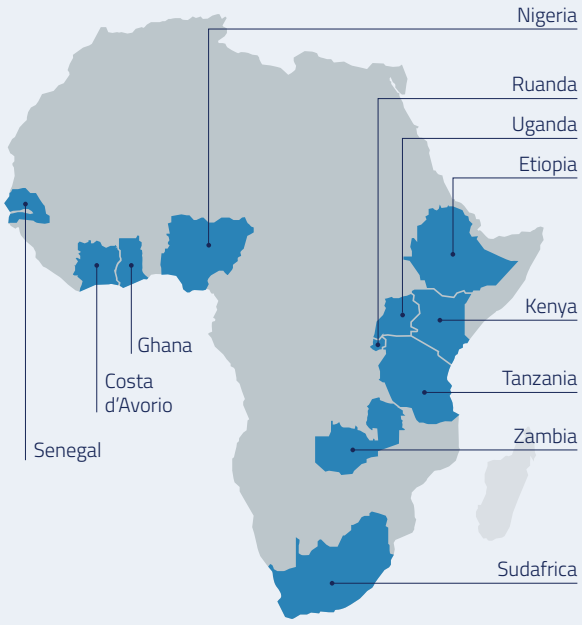
Nel 2025 è stato avviato il progetto AKADIMOS, finanziato dal programma DEP, che mira a costruire la *European Cybersecurity Skills Academy*, quale punto di riferimento unico per l'Unione europea in materia di formazione sulla cybersicurezza. Il progetto, a cui l'Agenzia partecipa insieme ad altri 8 partner da 5 Paesi europei (Grecia, Cipro, Spagna, Slovenia e Italia), vede coinvolti Autorità nazionali di cybersicurezza, università e centri di ricerca, e si propone di colmare il divario di competenze dei professionisti in ambito cyber in tutta l'UE. Le attività condotte dall'ACN nel 2025 hanno avuto l'obiettivo di impostare un modello per facilitare lo scambio di dati tra istituzioni e altri soggetti che promuovono iniziative di formazione, in vista della predisposizione del sistema informatico che raccoglierà informazioni su corsi e programmi.

CyberBridge: formazione strategica per la resilienza digitale in Africa

L'Agenzia, in collaborazione con la Fondazione Med-Or, ha lanciato *CyberBridge*, un percorso formativo avanzato volto a rafforzare le competenze in materia di cybersicurezza di funzionari pubblici di Paesi africani. Il progetto, avviato nel novembre 2025 e che vedrà la sua conclusione a maggio 2026, è sostenuto dal MAECI e si pone in linea con il Piano Mattei per l'Africa, mirando a rafforzare il dialogo strategico tra l'Italia e il continente nel campo della cybersicurezza.

Il progetto prevede un intervento formativo articolato, destinato a 30 funzionari, in servizio presso Amministrazioni centrali di 11 Paesi africani partner (Costa d'Avorio, Etiopia, Ghana, Kenya, Nigeria, Ruanda, Senegal, Sudafrica, Tanzania, Uganda e Zambia). I percorsi formativi permetteranno ai discenti di acquisire competenze tecniche e capacità di *policy*, favorendo un approccio multilivello alla resilienza digitale che integri formazione specialistica, diplomazia e *governance* del cyberspazio.

11 Paesi partner



8

Stato di attuazione della Strategia nazionale di cybersicurezza 2022-2026

La Strategia nazionale di cybersicurezza rappresenta la bussola che guida il Paese nell'innalzamento dei livelli di sicurezza e resilienza cibernetiche. A partire dalla sua adozione da parte del Presidente del Consiglio dei ministri, l'attuazione della Strategia 2022-2026 si è consolidata attraverso il coinvolgimento sempre più capillare delle Amministrazioni Pubbliche e il sostegno offerto dalle risorse finanziarie rese disponibili dai c.d. Fondi Strategia.

L'Agenzia per la cybersicurezza nazionale, garantendo una funzione di indirizzo, coordinamento e monitoraggio, continua a promuovere l'impiego della Strategia come strumento di rafforzamento costante e progressivo della postura di sicurezza cibernetica del Paese. A tale riguardo, nel 2025 l'Agenzia ha esteso la platea di Amministrazioni beneficiarie dei citati Fondi, ampliando il coinvolgimento delle Regioni e delle Province autonome e includendo le Autorità amministrative indipendenti.

In continuità con gli anni precedenti, metodologie di lavoro ormai consolidate hanno consentito all'ACN di recepire le esigenze delle Amministrazioni e fornire supporto tecnico in tutto il ciclo di vita degli interventi di attuazione, incluso il monitoraggio periodico volto a verificare l'avanzamento progettuale, il raggiungimento dei risultati prefissati e l'utilizzo delle risorse assegnate.

Il 2025, inoltre, è stato per la Strategia nazionale di cybersicurezza un anno di snodo, in cui si è dato avvio all'analisi del livello di maturità del Paese in vista del prossimo aggiornamento dell'attuale quadro strategico, che esaurirà la sua validità nel 2026. Sulla scorta dei risultati raggiunti nel quinquennio precedente, la Strategia futura opererà in continuità con il precedente quadro strategico, anticipando i fattori di cambiamento che interesseranno il settore digitale, lo scenario internazionale e il quadro giuridico in materia di cybersicurezza.

8.1 RILEVAZIONE DEI FABBISOGNI E RISORSE ASSEGNATE

Nel corso del 2025 l'ACN ha avviato la terza rilevazione dei fabbisogni finanziari finalizzata all'attuazione delle misure previste dal Piano di implementazione della Strategia. Tale rilevazione ha riguardato, in via prioritaria, le misure non ancora attuate e le specifiche esigenze rappresentate da alcune Amministrazioni. Inoltre, sono state coinvolte le Regioni e le Province autonome che non avevano preso parte alla precedente rilevazione e le Autorità amministrative indipendenti, per le quali si è voluto assicurare continuità ai progetti già finanziati con risorse a valere sull'Intervento 1.5 "Cybersecurity" del PNRR.

Precedenti DPCM di ripartizione dei Fondi Strategia

DPCM 9 agosto 2023

66,7	39	10
Mln € per il triennio 2023-2025	Interventi sostenuti	Amministrazioni coinvolte

DPCM 8 luglio 2024

347,6	107	39
Mln € per il triennio 2024-2026	Interventi sostenuti	Amministrazioni coinvolte

In continuità con le precedenti rilevazioni, è stata prevista la presentazione di schede progettuali da parte delle Amministrazioni chiamate a contribuire all'attuazione della Strategia. Tali istanze sono state analizzate e valutate tenendo conto della coerenza degli interventi proposti con le misure di riferimento del Piano di implementazione e del contributo degli stessi al rafforzamento della sicurezza cibernetica delle singole Amministrazioni e del sistema Paese più in generale. Si è inteso, infatti, considerare anche il potenziale impatto di tali interventi sul complessivo livello di resilienza della superficie digitale nazionale.

Nello specifico, la rilevazione condotta nel 2025 ha visto il coinvolgimento di 19 Amministrazioni pubbliche (di cui 16 centrali e 3 tra Regioni e Province autonome), che hanno presentato interventi relativi a un totale di 10 misure del Piano di implementazione della Strategia. Nel complesso, sono stati ritenuti idonei al finanziamento 35 interventi.

Su proposta dell'ACN e d'intesa con il Ministero dell'economia e delle finanze, è stato, quindi, adottato il DPCM 4 luglio 2025, che, in relazione al triennio 2025-2027, ha assegnato un totale di 57,6 milioni di euro, di cui 50,6 milioni di euro a valere sul Fondo per l'attuazione della Strategia nazionale di cybersicurezza e 7 milioni di euro a valere sul Fondo per la gestione della cybersicurezza.

Fondi Strategia per il 2025-2027

Fondo per l'attuazione della Strategia nazionale di cybersicurezza

Finanzia gli investimenti volti al conseguimento dell'autonomia tecnologica in ambito digitale, nonché l'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali.

Fondo per la gestione della cybersicurezza

Finanzia le attività di gestione operativa dei progetti volti all'attuazione della Strategia nazionale di cybersicurezza.

L'ACN indirizza, coordina e monitora l'attuazione del Piano di implementazione della Strategia, anche attraverso una periodica rilevazione dei fabbisogni finanziari delle Amministrazioni, utile alla ripartizione dei Fondi Strategia tramite DPCM.

L'attuazione della Strategia è resa possibile non solo dalle risorse messe a disposizione dai citati Fondi, ma anche da ulteriori fonti di finanziamento europee, nonché dalle risorse proprie delle singole Amministrazioni. In quest'ultimo caso, in particolare, si tratta di interventi che le Amministrazioni svolgono nell'ambito delle proprie competenze e che, tuttavia, contribuiscono a perseguire gli obiettivi della Strategia.

8.2 BENEFICIARI DELLE RISORSE

Il DPCM 4 luglio 2025 ha destinato il 91% delle risorse assegnate a Pubbliche Amministrazioni centrali (Figura 1) che operano a presidio di funzioni nevralgiche dello Stato, quali, ad esempio, la giustizia, la politica economica e la sicurezza nazionale. In questo gruppo rientrano anche, per la prima volta, numerose Autorità amministrative indipendenti, con l'obiettivo di rafforzare la cybersicurezza di enti che detengono prerogative essenziali in termini di tutela di diritti fondamentali e di regolazione settoriale. Vi rientra, inoltre, l'ACN, i cui interventi mirano a rafforzare la cybersicurezza di tutto il Paese e, dunque, producono benefici per l'intero ecosistema nazionale.

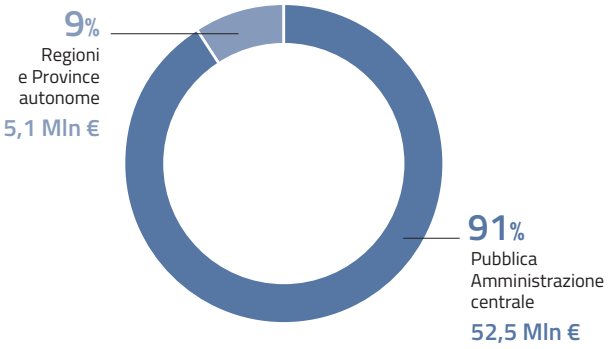


Figura 1 – Distribuzione delle risorse finanziarie tra Amministrazioni centrali e locali

La rilevazione dei fabbisogni 2025 segue la tendenza, già evidente nel 2024, verso una crescente capillarità degli interventi di attuazione della Strategia. Si conferma, infatti, il coinvolgimento delle Pubbliche Amministrazioni locali (per un importo pari al 9% del totale), in particolare di alcune Regioni e della Provincia Autonoma di Trento che non avevano partecipato alle precedenti rilevazioni, facendo sì che l'intero territorio nazionale sia coinvolto nell'attuazione della Strategia.

La distribuzione delle risorse 2025-2027 è ulteriormente approfondita nella Figura 2, che illustra la suddivisione per tipologia di Amministrazione delle risorse assegnate a valere sul Fondo di attuazione della Strategia nazionale di cybersicurezza e sul Fondo per la gestione della cybersicurezza.

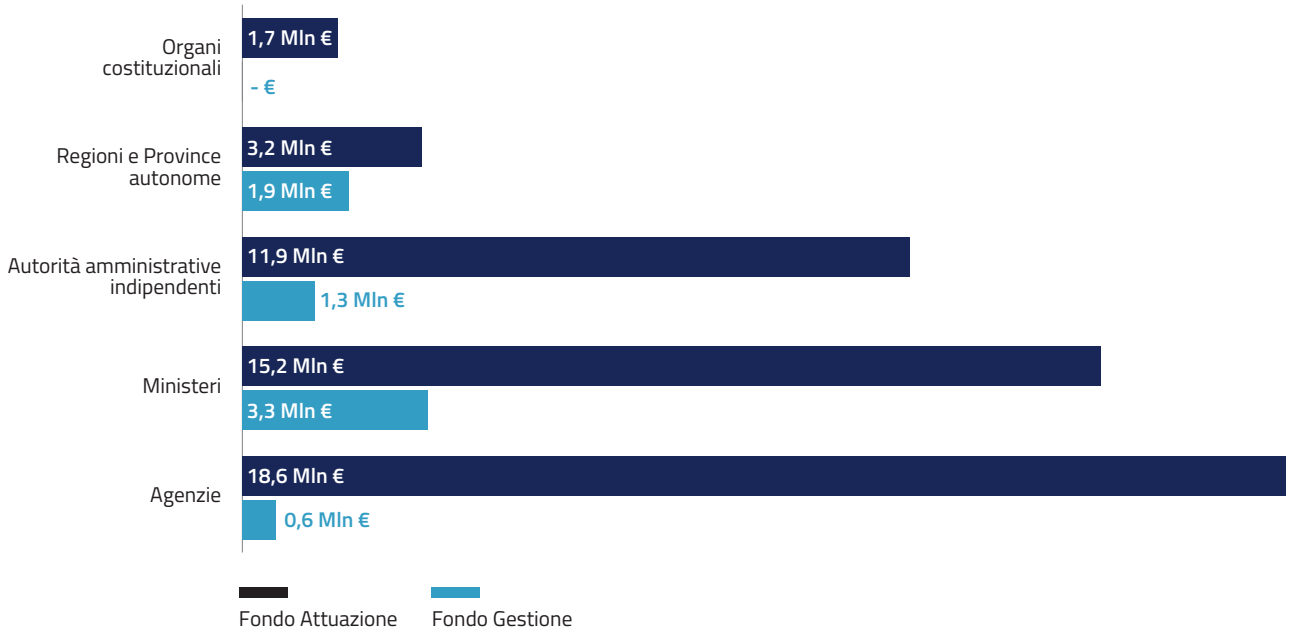


Figura 2 – Distribuzione delle risorse finanziarie per tipologia di Amministrazione beneficiaria

8.3 RISULTATI RAGGIUNTI

Nel 2025 delle 82 misure del Piano di implementazione della Strategia nazionale di cybersicurezza 2022-2026, 60 risultano conseguite e 22 in corso (Figura 3). Tale risultato, reso possibile dalla collaborazione sul piano istituzionale di tutte le Amministrazioni responsabili dell'attuazione della Strategia, conferma la consapevolezza della Pubblica Amministrazione italiana rispetto al tema della cybersicurezza.

Nel 2025 sono stati raccolti i frutti degli interventi avviati negli anni precedenti. Infatti, i numerosi interventi realizzati hanno generato effetti benefici per le Amministrazioni in termini di rafforzamento della postura di cybersicurezza grazie all'impiego degli strumenti tecnologici, all'implementazione di nuovi processi e assetti organizzativi e, non ultima, alla crescita di competenze e consapevolezza sui rischi informatici.

Figura 3 – Stato di implementazione delle misure al 2025

Protezione

In relazione al primo dei tre macro-obiettivi previsti dalla Strategia, la protezione degli *asset* ICT strategici nazionali, nel 2025 sono stati avviati ulteriori interventi nei seguenti ambiti:

- rafforzamento del sistema di scrutinio tecnologico nazionale, grazie all'aggiornamento della strumentazione in uso al Centro di valutazione e certificazione nazionale (Misura #1);
- definizione di una politica nazionale sulla divulgazione coordinata di vulnerabilità e relativa progettazione di una piattaforma informatica per le segnalazioni (Misura #9);
- realizzazione di iniziative di sensibilizzazione per favorire l'applicazione del "Framework Nazionale per la Cybersecurity e la Data Protection" e dei "Controlli essenziali di *cybersecurity*" (Misura #11);
- sviluppo di tecnologie/sistemi di cifratura nazionale in ambito non classificato e creazione di un ecosistema nazionale in tale ambito (Misura #23).

Risposta

Ai fini del raggiungimento del secondo macro-obiettivo, risposta alle minacce, agli incidenti e alle crisi cyber nazionali, nel 2025 sono stati avviati ulteriori interventi per:

- sviluppare le capacità per assicurare una pronta attività di comunicazione istituzionale in caso di incidenti cyber rilevanti o di crisi cibernetica (Misura #28);
- realizzare un programma di qualificazione in materia di *incident response* dei SOC/CERT/CSIRT di un gruppo di aziende selezionate (Misura #36);
- potenziare la rilevazione statistica e l'analisi dei dati relativi ai reati informatici da parte di Forze di polizia e Autorità giudiziaria (Misura #44).

Sviluppo

Quanto al terzo macro-obiettivo, sviluppo consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, sono stati avviati ulteriori interventi in molteplici ambiti:

- supportare l'operatività dei *Digital Innovation Hub* e favorirne le sinergie con il Centro nazionale di coordinamento, con i Centri di competenza ad alta specializzazione e con i Cluster tecnologici (Misura #47);
- promuovere la strutturazione di un ecosistema *quantum* robusto e integrato che consenta di conseguire una significativa autonomia relativamente a prodotti e processi informatici di rilevanza strategica (Misura #48);
- avviare il processo di realizzazione del "Parco nazionale della cybersicurezza" a supporto dello sviluppo del tessuto produttivo nazionale nell'ambito della sicurezza cibernetica (Misura #49);
- promuovere l'internazionalizzazione delle imprese italiane che offrono prodotti e servizi di *cybersecurity* attraverso la partecipazione a fiere internazionali e a programmi di accompagnamento, *scale-up* e *market access* nell'ambito di un Tavolo di coordinamento (Misura #50);
- incoraggiare la creazione di *Product Security Incident Response Team* da parte degli operatori privati (Misura #52);
- avviare nuovi progetti di rafforzamento della cybersicurezza della PA come accompagnamento alla digitalizzazione e all'innovazione (Misura #55).

Fattori abilitanti

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

- attivazione di ITS con percorsi di *cybersecurity* contribuendo a sostenere le specializzazioni produttive della manifattura locale (Misura #60);
- sviluppo di un sistema di certificazione dell'apprendimento e dell'acquisizione di specifiche professionalità (Misura #61);
- erogazione di fondi da dedicare alla formazione professionale nei settori pubblico e privato (Misura #63);
- potenziamento della formazione del personale diplomatico così da rafforzare le capacità di *cyber diplomacy* (Misura #69);
- campagne di sensibilizzazione volte a promuovere le competenze degli utenti e i comportamenti responsabili nello spazio cyber (Misura #71);
- cooperazione internazionale in materia di cybersicurezza con Paesi di interesse strategico per contribuire alla stabilità e alla sicurezza dello spazio cibernetico (Misura #77);
- sostegno al *cyber capacity building* in favore di Paesi esteri (Misura #79).

L'ACN monitora con cadenza quadrimestrale l'andamento dell'attuazione della Strategia nazionale, attraverso il dialogo costante con le Amministrazioni, che verrà ulteriormente rafforzato nel corso del 2026 in vista dell'aggiornamento del quadro strategico. Al riguardo, sarà determinante valutare l'impatto degli sviluppi nell'impianto normativo nazionale ed europeo, l'accresciuto livello di competizione geopolitica e l'imprescindibile esigenza di proteggere le infrastrutture critiche nazionali. Altrettanto importante sarà valutare come l'innovazione tecnologica, e la sua *cybersecurity*, incida sulla competitività dell'economia e sulla sicurezza del Paese. Come in precedenza, il contributo delle Amministrazioni responsabili e l'azione sinergica di istituzioni, industria, accademia e società civile saranno elementi irrinunciabili per il successo della futura Strategia nazionale di cybersicurezza.

Protezione

AREE TEMATICHE	MISURE CONSEGUITE
Scrutinio tecnologico	4 SU 4
Definizione e mantenimento di un quadro giuridico nazionale aggiornato e coerente	6 SU 7
Conoscenza approfondita del quadro della minaccia cibernetica	2 SU 2
Potenziamento capacità cyber della Pubblica Amministrazione	3 SU 3
Sviluppo di capacità di protezione per le infrastrutture nazionali	1 SU 5
Promozione dell'uso della crittografia	1 SU 2
Definizione e implementazione di un piano di contrasto alla disinformazione online	1 SU 1

Risposta

AREE TEMATICHE	MISURE CONSEGUITE
Sistema di gestione crisi nazionale e transnazionale	4 SU 5
Servizi cyber nazionali	3 SU 8
Esercitazioni di cybersicurezza	2 SU 2
Definizione del posizionamento e della procedura nazionale in materia di attribuzione	- SU 1
Contrasto al *cybercrime*	4 SU 4
Capacità di deterrenza in ambito cibernetico	1 SU 1

Sviluppo

AREE TEMATICHE	MISURE CONSEGUITE
Centro nazionale di coordinamento	1 SU 2
Sviluppo di tecnologia nazionale ed europea	- SU 1
Realizzazione di un "Parco nazionale della cybersicurezza"	- SU 1
Sviluppo industriale, tecnologico e della ricerca	2 SU 3
Impulso all'innovazione tecnologica e alla digitalizzazione	5 SU 6

Fattori abilitanti

AREE TEMATICHE	MISURE CONSEGUITE
Formazione	9 SU 12
Promozione della cultura della sicurezza cibernetica	2 SU 3
Cooperazione	8 SU 8
Metriche e *Key Performance Indicators*	1 SU 1

Figura 4 – Misure conseguite per obiettivi e aree tematiche

9

L'Agenzia nel 2025

Il 2025 è stato per l'Agenzia per la cybersicurezza nazionale un anno di consolidamenti progressivi sotto ogni profilo della struttura organizzativa: dal personale alle risorse finanziarie e ai sistemi tecnologici, fino alla comunicazione verso l'esterno. Ciò per sostenere una missione sempre più complessa e centrale per il Paese, in un panorama della minaccia cyber in continua evoluzione.

Con il crescere delle responsabilità affidate all'ACN, è proseguita la ricerca delle migliori professionalità, un impegno che alimenta una comunità di lavoro giovane, competente e appassionata. Parallelamente, è stata posta particolare attenzione al miglioramento e alla semplificazione dei processi interni, cercando soluzioni sempre più funzionali.

La cura nella gestione delle risorse finanziarie è anch'essa parte di questo percorso di evoluzione, anche attraverso un *procurement* attento e coerente con le nuove normative. Allo stesso tempo, le tecnologie a disposizione dell'Agenzia sono state implementate per supportare servizi sempre più vari e avanzati, capaci di rispondere alle numerose sfide correlate alle diverse competenze attribuite all'ACN.

Accanto a tutto questo, si è ampliata la capacità dell'Agenzia di raccontarsi, di far conoscere il proprio lavoro e di coinvolgere un pubblico sempre più vasto, valorizzando i propri canali istituzionali e promuovendo campagne informative e divulgative che contribuiscono a diffondere una cultura della cybersicurezza ormai indispensabile per qualunque utente digitale.

9.1 SVILUPPO DELL'ORGANIZZAZIONE E DELLE PERSONE

Il percorso di progressiva crescita dell'Agenzia è continuato nel 2025 attraverso l'adozione di paradigmi organizzativi, di reclutamento e di sviluppo del personale finalizzati a fronteggiare le nuove sfide poste dall'innovazione tecnologica, dalle modifiche del quadro normativo in materia di cybersicurezza, sia a livello nazionale che dell'Unione europea, nonché dagli ulteriori compiti istituzionali assegnati all'ACN.

Il nuovo assetto organizzativo è stato definito mediante l'inserimento nella struttura operativa dell'Agenzia del Servizio Crittografia anche in relazione all'istituzione del Centro nazionale di crittografia, l'aggiornamento delle funzioni connesse al ruolo di Autorità nazionale di certificazione della cybersicurezza, nonché mediante interventi di soppressione, accorpamento e riorganizzazione dei Servizi e delle Divisioni che hanno ridisegnato l'organigramma dell'Agenzia (Figura 1).

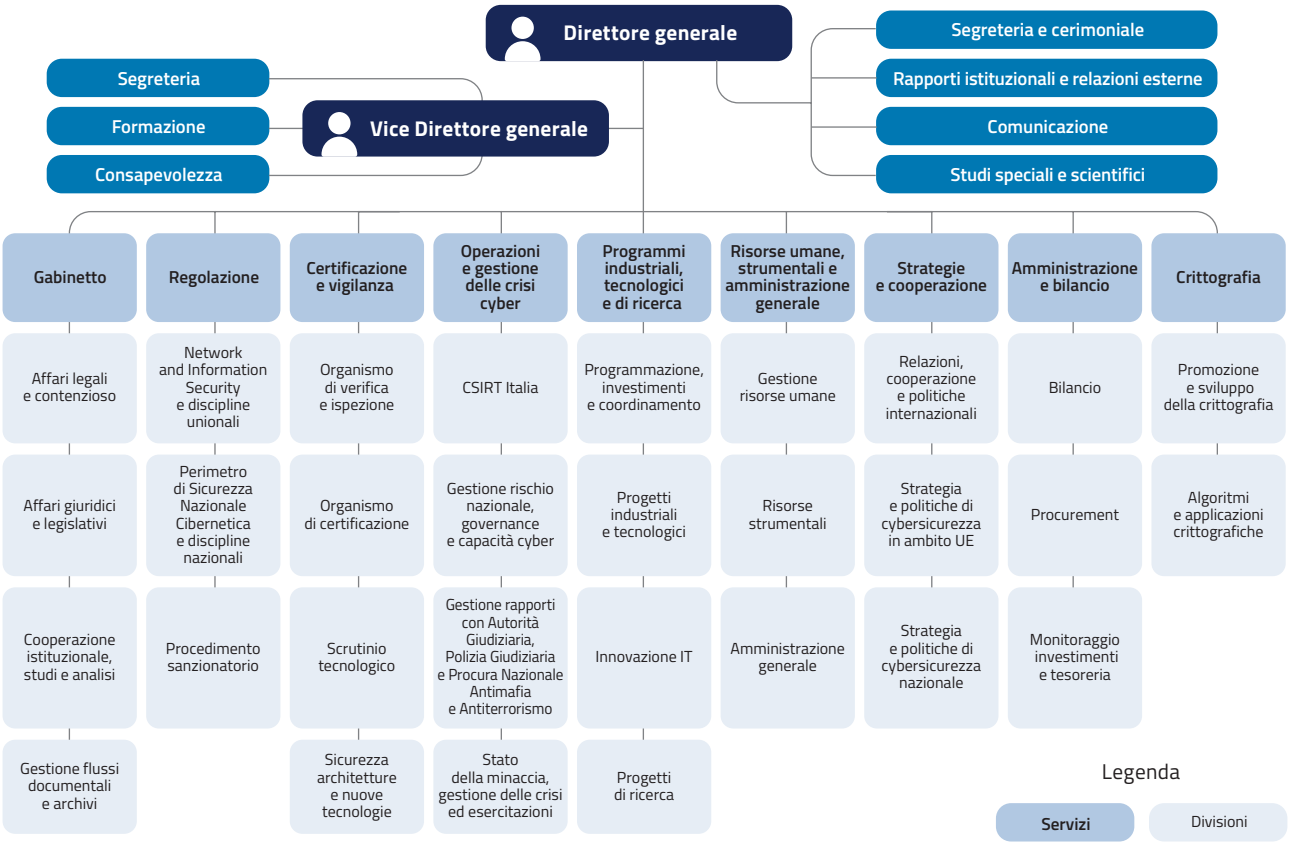


Figura 1 – Organigramma ACN al 31.12.2025

Parallelamente, alla luce delle nuove funzioni in materia di crittografia e tenuto conto degli sviluppi connessi al carattere trasversale e multidisciplinare della cybersicurezza e delle tecnologie innovative, si è proceduto ad aggiornare il Piano strategico ACN 2024-2026.

FOCUS

Il Piano strategico ACN 2024-2026

Il Piano è il documento unico di programmazione, governance e coordinamento dell'Agenzia, in cui i 5 obiettivi strategici assumono rilievo trasversale. Il Piano raccoglie sia le finalità istituzionali e la missione pubblica dell'ACN, sia l'organizzazione e gli obiettivi da perseguire, garantendo coerenza con le risorse disponibili e puntando all'efficientamento e alla semplificazione dell'azione amministrativa. Il Piano è anche un utile strumento per monitorare progressivamente i risultati e per realizzare il massimo allineamento tra obiettivi e contributi individuali del personale. Per il triennio 2024-2026, l'ACN ha orientato la propria azione verso la creazione di valore pubblico, sostenendo il processo di ammodernamento delle infrastrutture, rafforzando la resilienza cibernetica del Paese, riducendone le vulnerabilità e aumentando l'autonomia e l'indipendenza tecnologica.

5 OBIETTIVI

Protezione degli *asset* strategici nazionali

Risposta alle minacce, agli incidenti e alle crisi cyber nazionali e transnazionali

Sviluppo sicuro delle tecnologie digitali

Rafforzamento della cooperazione in materia di cybersicurezza

Essere un centro di eccellenza con un'organizzazione a geometrie variabili

Il costante processo di innovazione strategica, organizzativa e funzionale dell'ACN ha interessato anche il reclutamento del personale e lo sviluppo delle competenze e delle professionalità. La crescita della capacità operativa dell'Agenzia è stata accompagnata dalla rideterminazione della dotazione organica complessiva, culminata con l'adozione del DPCM del 29 settembre 2025, che ha previsto un incremento progressivo del personale fino a raggiungere un massimo di 669 unità di personale dal 2026. Tale rideterminazione è principalmente riconducibile agli effetti degli interventi normativi che hanno affidato maggiori compiti all'Agenzia, in particolare il D.Lgs. n. 138/2024 di recepimento della Direttiva NIS2 che ha tenuto in considerazione l'esigenza di disporre di ulteriori risorse per poter far fronte ai maggiori compiti derivanti dalla nuova disciplina.

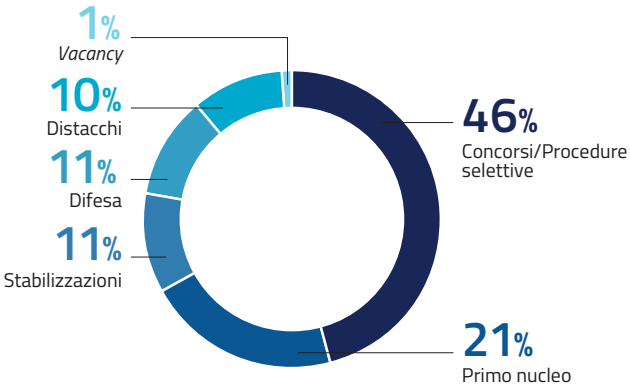


Figura 2 – Personale ACN al 31.12.2025

Gli istituti previsti dalla normativa per il reclutamento del personale hanno consentito all'ACN di impiegare, al 31 dicembre 2025, un totale di 422 unità, oltre al Direttore generale. La Figura 2 schematizza i vari canali per l'impiego presso l'Agenzia.

L'incremento di personale rispetto al 2024 è stato caratterizzato da particolare dinamicità, sia sotto il profilo dell'impiego dei diversi canali di reclutamento a disposizione, sia sotto quello dell'avvio delle procedure interne di valorizzazione delle professionalità.

In primo luogo, tenuto conto dell'elevato livello di competenza professionale richiesto in settori competitivi e soggetti a fenomeni di rapida obsolescenza delle competenze come quello della cybersicurezza, si è proceduto all'immissione in ruolo di 75 risorse, selezionate mediante concorsi pubblici. Oltre ad attingere dalle graduatorie delle procedure concorsuali concluse nel 2024, nel corso del 2025, ne sono state avviate altre 4 per l'assunzione di personale con diversi profili professionali.

Le procedure concorsuali avviate nel 2025

24
Coordinatori
con orientamento archivistico e per la prevenzione e gestione di incidenti informatici

27
Assistenti
con orientamento nelle discipline amministrative, economiche, ICT e in impiantistica meccanica ed elettrica

90
Esperti
con orientamento tecnico scientifico per l'assunzione di 10 differenti profili in ambiti STEM

17
Coordinatori
con orientamento nelle discipline giuridico-economiche e tecnico-scientifiche, appartenenti alle categorie protette

Inoltre, a seguito di apposita selezione a evidenza pubblica, è stata assunta a tempo determinato, con contratto di diritto privato (*vacancy*), una figura dirigenziale in possesso di alta e particolare specializzazione nel campo dell'*Information Security*. Quanto alle altre professionalità già impiegate in Agenzia tramite *vacancy*, si è svolta la procedura selettiva prevista dal D.L. n. 19/2024, che ha consentito l'ingresso nel ruolo di 11 dipendenti di livello non dirigenziale.

Infine, si è proceduto anche con l'espletamento del primo concorso interno che ha permesso di valorizzare la professionalità acquisita in servizio di 8 unità che sono

progredite dall'Area operativa all'Area manageriale e alte professionalità.

Un ulteriore canale per completare la strutturazione dell'Agenzia è rappresentato dagli istituti del distacco, comando, fuori ruolo o altre analoghe posizioni, che sono stati disposti per 16 nuove unità, anche grazie a specifiche intese con altri enti e istituzioni pubbliche. A ciò si aggiunge l'impiego, ai sensi del DPCM 24 luglio 2024, di personale del Ministero della difesa per un totale di ulteriori 25 militari di vari ruoli e gradi previa individuazione di specifici profili di interesse collaborativamente identificati da Agenzia e Dicastero.

Inoltre, in attuazione della Convenzione fra l'Agenzia e il MAECI sottoscritta nel 2025 e all'adozione della disciplina giuridica ed economica per il personale assegnato quale addetto per la cybersicurezza presso le Rappresentanze diplomatiche e gli uffici consolari, sono state attivate due posizioni, rispettivamente presso l'Ambasciata d'Italia a Washington e presso la Rappresentanza Permanente d'Italia presso l'Unione europea.

L'Agenzia, anche grazie agli ingressi del 2025, continua a disporre di un capitale umano particolarmente giovane e qualificato. L'età media del personale dipendente è di circa 43 anni (quella dei 75 nuovi assunti tramite concorso è di 35 anni), con un andamento decrescente rispetto al momento di istituzione dell'Agenzia. Per quanto attiene ai titoli di studio, si evince una netta prevalenza di personale laureato (79%), di cui circa il 71% in possesso di almeno una laurea magistrale (Figura 3).

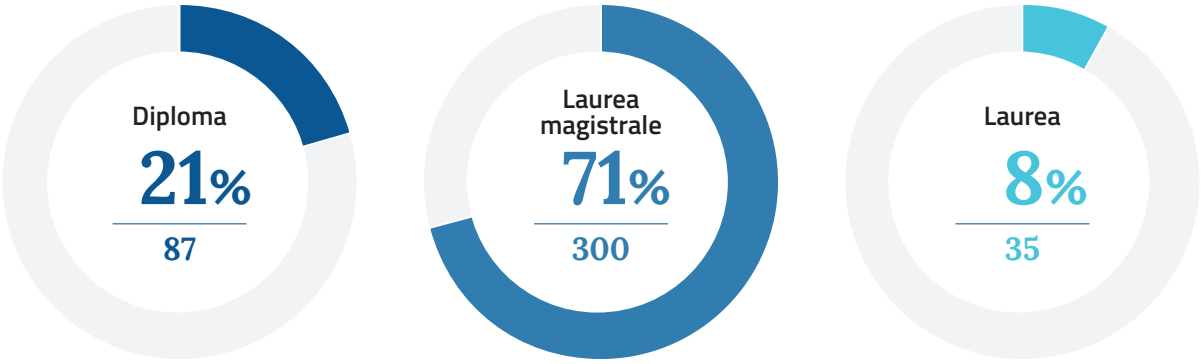


Figura 3 – Titoli di studio del personale ACN al 31.12.2025

L'ACN si è avvalsa, inoltre, nell'ambito del contingente di esperti in possesso di specifica ed elevata competenza nel campo dell'ICT, di due professionisti per la realizzazione di progetti su processi di trasformazione tecnologica nonché di comunicazione e disseminazione.

In un'ottica di progressivo rafforzamento del capitale umano dell'Agenzia, sono proseguite le iniziative formative già avviate nel precedente anno e sono stati avviati mirati percorsi per l'aggiornamento delle competenze tecnico-specialistiche, manageriali e linguistiche, anche mediante le collaborazioni con il mondo universitario e istituzionale (Banca d'Italia, Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri, SNA e FormezPA). Particolare attenzione è stata rivolta alla materia dei contratti pubblici, anche al fine di dare attuazione alle disposizioni che prescrivono specifici obblighi di formazione finalizzati al raggiungimento dei requisiti rilevanti per la qualificazione dell'Agenzia come stazione appaltante.

FOCUS

La sicurezza sul lavoro in ACN

Nel 2025 un intervento normativo in materia di sicurezza sui luoghi di lavoro (D.L. n. 159/2025) ha riconosciuto e valorizzato la specificità istituzionale e funzionale dell'Agenzia, quale soggetto chiamato a svolgere compiti di rilievo strategico nel presidio della sicurezza nazionale nello spazio cibernetico. Nel modificare il Testo unico sulla sicurezza sul lavoro, si consente all'Agenzia di dotarsi di una disciplina ad hoc in materia per adattarla alle proprie peculiari esigenze organizzative e operative, preservando al contempo i livelli di tutela dei lavoratori. La specifica modulazione dell'applicazione della normativa in materia sarà disciplinata da un regolamento approvato con decreto del Presidente del Consiglio dei ministri, su proposta dell'ACN, sentiti i Ministri del lavoro e delle politiche sociali e della salute, previo parere del COPASIR.

9.2 PROGRAMMAZIONE ECONOMICO-FINANZIARIA E *PROCUREMENT*

L'Agenzia, in virtù dell'autonomia finanziaria e contabile riconosciutale dal decreto-legge istitutivo, assicura una corretta gestione delle risorse assegnatele e, attraverso i propri documenti di bilancio, una rappresentazione veritiera, corretta e trasparente della propria situazione economica, finanziaria e patrimoniale. In tale ottica, l'Agenzia predispone i bilanci, sia previsionali che consuntivi, conformi ai principi contabili civilistici, da sottoporre al parere del CIC prima della loro approvazione con DPCM.

Il 14 maggio 2025 è stato adottato il bilancio d'esercizio 2024 (bilancio consuntivo) che ha registrato un utile di 24.360.893 euro, il quale è stato destinato al finanziamento di una riserva di patrimonio netto per la copertura delle future spese di investimento funzionali a potenziare l'efficacia dell'operatività dell'ACN. Nel corso del 2025 sono stati, altresì, predisposti i provvedimenti di assestamento del bilancio 2025 (revisione del budget economico), nonché di adozione del bilancio preventivo 2026 (budget economico). La lettura di tali documenti consente di avere una rappresentazione complessiva della dimensione economica e finanziaria dell'Agenzia e della sua evoluzione.

Lo stanziamento annuale dell'ACN, che le fornisce i mezzi finanziari strutturali per svolgere ordinariamente i propri compiti istituzionali, è costituito dalla sua dotazione ordinaria (stabilita dal D.L. n. 82/2021) come rimodulata dalle autorizzazioni di spesa intervenute successivamente con specifiche disposizioni normative. Al riguardo, la Figura 4 rappresenta la misura dello stanziamento annuale prevista a legislazione vigente (da ultimo con legge di bilancio 2026) nel quadriennio 2025-2028, dove si delinea la progressiva crescita delle risorse finanziarie, che si completa nell'annualità 2027, in parallelo con la crescita strutturale dell'ACN in termini di funzioni e compiti affidati.

Figura 4 – Risorse finanziare assegnate all'ACN

Alle citate risorse di natura strutturale si aggiungono ulteriori voci di finanziamento di respiro pluriennale volte a sostenere, principalmente, le progettualità di investimento dell'Agenzia e del sistema Paese nel suo complesso. Tra queste rientrano, in particolare, i finanziamenti, del valore di 623 milioni di euro, dell'Investimento 1.5 "Cybersecurity" del PNRR che l'Agenzia, in qualità di soggetto attuatore, gestisce mediante la realizzazione di linee di intervento sia condotte direttamente, sia portate avanti da soggetti terzi, principalmente PA, cui vengono trasferite le risorse messe a disposizione dal PNRR fino al 2026 (vedasi Capitolo 5). Altra leva finanziaria fondamentale, e con un orizzonte temporale più ampio, è costituita dai Fondi Strategia, ossia i fondi istituiti per supportare l'attuazione alla Strategia nazionale di cybersicurezza e soddisfare le esigenze di sicurezza cibernetica delle Amministrazioni Pubbliche e dell'ACN, come più ampiamente descritto nel Capitolo 8.

Tra le entrate dell'Agenzia possono, infine, annoverarsi i corrispettivi per i servizi di certificazione e accreditamento resi in favore di soggetti pubblici e privati che, nel 2025, hanno registrato un incremento rispetto all'anno precedente, nonché i finanziamenti correlati alla partecipazione dell'Agenzia a progetti dell'Unione europea o nazionali.

Sul fronte della spesa, una parte delle risorse finanziarie destinate al funzionamento dell'Agenzia è stata dedicata al raggiungimento dell'obiettivo, considerato primario, della crescita di competenze e specifiche professionalità mediante le attività di reclutamento di personale. Al riguardo, si è assicurata la sostenibilità finanziaria della spesa per il personale fornendo proiezioni decennali dell'evoluzione degli oneri relativi alla crescita in termini numerici e di carriera del personale dell'Agenzia.

Si è, inoltre, proceduto ad avviare alcuni interventi specifici sull'immobile acquistato nel 2024 per l'assolvimento di peculiari attività previste dal mandato istituzionale dell'ACN, adeguando gli spazi per poter accogliere i laboratori di certificazione del CVCN, una sala situazioni per lo CSIRT Italia, nonché spazi e infrastrutture per la trattazione delle informazioni, comprese quelle classificate.

Con riferimento alle attività di *procurement*, nel corso del 2025 l'Agenzia ha nuovamente attivato la procedura di iscrizione nell'Elenco delle stazioni appaltanti qualificate dell'ANAC, ottenendo la qualificazione ordinaria nel livello massimo nel settore servizi e forniture "SF1" per la durata di un anno. Sono state, inoltre, predisposte e concluse oltre 60 procedure, tra cui affidamenti diretti e adesioni a Convenzioni e Accordi quadro Consip, nonché ulteriori 9 procedure sopra la soglia di rilevanza europea, aperte e negoziate (Figura 5).

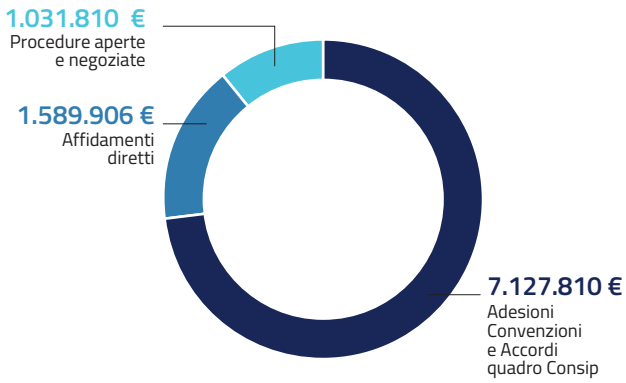


Figura 5 – Importi delle procedure di acquisizione del 2025

L'ACN ha, inoltre, espletato ulteriori procedure di gara per la stipula di contratti di appalti di lavori, servizi e forniture per le proprie attività finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico, come previsto dalla specifica normativa in materia di tale tipologia di appalti dell'Agenzia (DPCM n. 166/2022).

A dimostrazione della maggiore strutturazione e complessità dell'azione portata avanti, nel 2025 l'Agenzia si è confrontata con procedure con le quali non si era ancora cimentata. Ne è un esempio l'avvio di un partenariato strategico con la Fondazione Med-Or che ha permesso all'ACN di ottenere un finanziamento da parte del MAECI per la realizzazione del progetto *CyberBridge*, illustrato nel Capitolo 7. L'ACN ha anche avviato una procedura aperta finalizzata alla stipula di un Accordo quadro per lo sviluppo della piattaforma di formazione e sensibilizzazione online E-Academy (anche su questo vedasi Capitolo 7).

Infine, nell'ottica di digitalizzare quanto più possibile i processi operativi, l'Agenzia ha adottato un applicativo di

gestione che, favorendo la semplificazione e la trasparenza delle attività di *procurement*, consente il costante monitoraggio della spesa, il tracciamento delle procedure di affidamento e del ciclo di vita dei contratti.

9.3 IL SUPPORTO TECNOLOGICO ALL'ATTIVITÀ ISTITUZIONALE

Sempre nel corso del 2025, l'Agenzia ha portato avanti il percorso di consolidamento ed evoluzione dei propri sistemi tecnologici, che hanno accompagnato l'attuazione di nuovi obblighi regolatori e l'incremento delle capacità di coordinamento e vigilanza, contribuendo a rendere più efficiente l'azione istituzionale.

In particolare, nel quadro dell'attuazione nazionale della Direttiva NIS2, la piattaforma messa a disposizione dall'ACN nel 2024 continua a rappresentare lo strumento centrale per la gestione digitale degli adempimenti richiesti ai soggetti NIS, assicurando uniformità nella raccolta dei dati e nella comunicazione con l'Autorità competente (vedasi Capitolo 1).

La piattaforma è stata progressivamente rafforzata per sostenere il rispetto degli obblighi previsti dalla nuova normativa. In linea con il principio di *compliance* continuativa, il sistema è stato potenziato per includere il servizio dedicato all'aggiornamento annuale delle informazioni, consentendo ai soggetti NIS di mantenere allineati, attraverso un'unica interfaccia web, i dati anagrafici, le informazioni di contatto e le eventuali variazioni intervenute nel tempo.

Il sistema è stato ulteriormente sviluppato prevedendo l'attivazione di una procedura telematica dedicata alla designazione del referente CSIRT e dei relativi sostituti, rafforzando così il modello di interlocuzione operativa tra i soggetti NIS e il CSIRT Italia. In prospettiva dell'avvio degli obblighi di notifica degli incidenti di sicurezza a partire da gennaio 2026, è stata predisposta l'evoluzione della piattaforma per l'integrazione del servizio dedicato all'invio delle segnalazioni NIS, concentrando le funzionalità relative alla NIS su un unico canale ufficiale e strutturato per la trasmissione di tali informazioni verso l'Agenzia.

Nel loro complesso, queste evoluzioni hanno consentito di rendere più tracciabile e affidabile il presidio del quadro regolatorio NIS, semplificando gli adempimenti per i soggetti coinvolti e rafforzando la capacità dell'ACN di svolgere efficacemente le proprie attività istituzionali.

L'ACN, nei primi mesi del 2025, ha inoltre completato gli ultimi adeguamenti della piattaforma relativa al Catalogo delle infrastrutture digitali e dei servizi *cloud* per consentire la completa implementazione del Regolamento *cloud*, con particolare riferimento alle funzionalità offerte alle Pubbliche Amministrazioni e all'avvio del censimento sugli utilizzatori delle infrastrutture digitali e dei servizi *cloud* nel rispetto delle prescrizioni previste dalla normativa. Questi interventi hanno consolidato la capacità dell'Agenzia di supportare le PA nell'adozione di infrastrutture digitali e servizi *cloud* affidabili e conformi ai requisiti normativi, contribuendo alla creazione di un ambiente digitale più efficiente e coerente con le esigenze istituzionali.

Inoltre, l'evoluzione del Portale servizi ha permesso di ampliare e strutturare le modalità di accesso ai servizi digitali dell'Agenzia, introducendo nuove funzionalità di registrazione e gestione degli utenti. In particolare, è stata abilitata la registrazione per gli utenti delle Pubbliche Amministrazioni in ambito *cloud* e sono state predisposte le funzionalità di accesso e fruizione dei servizi dedicati all'NCC, a supporto dei processi di accreditamento e interazione con gli *stakeholder* nazionali.

Grazie a questi interventi, il Portale ha consolidato il proprio ruolo di punto unico di accesso ai servizi istituzionali dell'Agenzia, migliorandone l'accessibilità complessiva. Oggi accedono al Portale oltre 77.000 utenti e più di 32.000 organizzazioni, a testimonianza della crescente diffusione e rilevanza dei servizi digitali offerti. Si tratta di numeri estremamente significativi considerando che nel 2024 vi erano circa 4.500 utenti e 3.000 organizzazioni registrate sul Portale servizi ACN.

Portale servizi ACN

+77.000
utenti

+32.000
organizzazioni

L'Agenzia sta, inoltre, proseguendo nel percorso di rafforzamento del sistema di gestione documentale quale infrastruttura abilitante dell'azione amministrativa, funzionale non solo al rispetto degli obblighi normativi, ma anche al miglioramento della qualità dei processi decisionali e della capacità di assicurare trasparenza, efficienza e *accountability* nei confronti dei portatori d'interesse istituzionali e della collettività. In tale contesto, nel 2025 è stata significativamente potenziata l'attività di digitalizzazione e gestione documentale, con il trattamento strutturato di volumi fino a circa 1 milione di documenti.

9.4 COMUNICAZIONE

Una comunicazione efficace costituisce un *driver* strategico per il posizionamento e l'operatività dell'Agenzia, in quanto abilita la diffusione tempestiva e autorevole delle iniziative istituzionali, rafforza la credibilità dell'azione pubblica e contribuisce a orientare gli *stakeholder* verso comportamenti consapevoli in materia di sicurezza cibernetica. In un ecosistema digitale caratterizzato da minacce crescenti e da una loro costante evoluzione, la capacità dell'ACN di comunicare in modo integrato e multicanale contribuisce a incrementare la resilienza del Paese.

In tale prospettiva, la strategia di comunicazione si è sviluppata lungo quattro direttrici sinergiche: l'aggiornamento continuo del sito istituzionale, inteso come *repository* ufficiale, affidabile e sempre accessibile di documenti, avvisi, linee guida e iniziative; la presenza attiva sulle piattaforme social, quale leva di ingaggio diretto e amplificazione delle informazioni di pubblico interesse; il consolidamento delle relazioni con organi di stampa e media e la diffusione di campagne di comunicazione, per assicurare un racconto chiaro, coerente e ad ampio spettro delle molteplici attività dell'ACN.

Nel 2025, il sito web istituzionale ha totalizzato 2,1 milioni di visite. Le sezioni del sito più visitate sono state quelle relative al "CSIRT Italia", alla "NIS", alle "Domande frequenti", nonché quella "Lavora con noi". Il sito web dell'Agenzia è stato costantemente aggiornato con la pubblicazione di circa 170 notizie ottimizzate per la ricerca sul web. La maggior parte delle visite è avvenuta tramite motore di ricerca.

Il sito web ACN nel 2025

www.acn.gov.it

4 minuti 5 secondi	2,8	5.242.635	67.451
Durata media di una visita	Azioni per visita	Pagine viste	Download

I canali social istituzionali dell'ACN – LinkedIn e YouTube – hanno registrato una crescita costante e sostenuta. Le metriche registrate (impressioni, reazioni e condivisioni) evidenziano un livello significativo di attenzione e partecipazione, con picchi associati a iniziative ad alto valore strategico. Il profilo LinkedIn, in particolare, ha superato nel 2025 i 100.000 *follower* e, tra i post che hanno generato maggior traffico e interazioni, si segnalano quelli relativi all'accrescimento del capitale umano dell'Agenzia, nello specifico i concorsi pubblici per l'assunzione di nuove risorse. Parallelamente, un altro importante segmento di *engagement* ha riguardato la diffusione delle informazioni chiave relative alla fase attuativa della normativa NIS, con focus sugli obblighi in capo ai soggetti essenziali e importanti, tema percepito come prioritario da imprese e operatori di settore.

Per quanto riguarda il rapporto con i media tradizionali, oltre alle attività quotidiane di ufficio stampa, è stata avviata a ottobre 2025, in coincidenza con il mese europeo della cybersicurezza, una campagna di posizionamento e di informazione radio. All'interno del programma "Il pomeriggio di Radio 1" è stato trasmesso uno spazio dedicato alla sicurezza digitale di 12 puntate con interviste nelle quali il personale dell'ACN ha illustrato le principali funzioni dell'Agenzia, i progetti nazionali e internazionali, le opportunità che l'ACN offre per supportare le imprese, oltre a fornire consigli pratici di *cyber hygiene*. Inoltre, la proiezione sui media e gli organi di stampa, anche relativamente a iniziative e progetti, ha visto oltre 2.600 citazioni su agenzie di stampa, testate giornalistiche e media, più di 200 interviste ai Vertici dell'Agenzia, quasi 4.000 articoli dedicati, di cui oltre 2.400 su testate digitali e oltre 1.500 sulla carta stampata.

Sito web

Visite: 2,1 milioni (+218%)

News: 170

Social

LinkedIn:
6 milioni di visualizzazioni
112.000 *follower* (+40%)

YouTube:
+69% iscritti
1,2 milioni di visualizzazioni

Media

Citazioni stampa: 2.600

Articoli: 4.000

Interviste ai Vertici: 200

L'Agenzia, inoltre, in collaborazione con il Dipartimento della funzione pubblica e il Dipartimento per l'informazione e l'editoria della Presidenza del Consiglio dei ministri, ha realizzato una campagna di comunicazione integrata relativa al Vademecum di buone pratiche di *cybersecurity* di base per i dipendenti della PA (vedasi Capitolo 7), diffondendo uno spot radio-televisivo che ha avuto centinaia di passaggi televisivi e radiofonici sulle reti RAI.

Infine, il rafforzamento dell'immagine istituzionale dell'Agenzia si è consolidato parallelamente attraverso una crescente riconoscibilità nel panorama istituzionale, imprenditoriale e della ricerca. Tale rafforzamento è avvenuto, come visto, mediante la partecipazione a eventi strategici e la promozione di iniziative qualificate, anche attraverso la concessione del patrocinio a progetti di rilievo. Queste attività hanno contribuito a valorizzare l'identità dell'ACN come *asset* comunicativo, rafforzando la sua presenza nel dibattito pubblico e posizionandola come punto di riferimento nazionale in materia di cybersicurezza.

10

Lista degli acronimi

A

AgID: Agenzia per l'Italia digitale

AISCAT: Associazione italiana società concessionarie autostrade e trafori

AISE: Agenzia informazioni e sicurezza esterna

AISI: Agenzia informazioni e sicurezza interna

ANAC: Autorità nazionale anticorruzione

ANCI: Associazione nazionale dei Comuni italiani

ANSSI: Agenzia nazionale per la sicurezza dei sistemi informativi della Francia

ANVUR: Agenzia nazionale di valutazione del sistema universitario e della ricerca

APT: *Advanced Persistent Threat*

B

BOM: *Bill of Materials*

BSI: Ufficio federale per la sicurezza informatica della Germania

C

CAD: Codice dell'Amministrazione digitale

CADA: *Cloud and AI Development Act*

CBM: *Confidence-Building Measure*

CBOM: *Cryptographic Bill of Materials*

CCB: Centro per la cybersicurezza del Belgio

CCRA: *Common Criteria Recognition Arrangement*

CER: *Critical Entities Resilience Directive*

CERT: *Computer Emergency Response Team*

CIC: Comitato interministeriale per la cybersicurezza

CIN: *Cyber Innovation Network*

CINI: Consorzio nazionale interuniversitario per l'informatica

CISA: Agenzia per la cybersicurezza e la sicurezza delle infrastrutture degli Stati Uniti

COMINT: Comitato interministeriale per le politiche relative allo spazio e alla ricerca aerospaziale

CONSOB: Commissione nazionale per le società e la borsa

COPASIR: Comitato parlamentare per la sicurezza della Repubblica

CRA: *Cyber Resilience Act*

CRI: *Counter Ransomware Initiative*

CSA: *Cybersecurity Act*

CSIRT: *Computer Security Incident Response Team*

CSoA: *Cyber Solidarity Act*

CTS: Comitato tecnico-scientifico

CV: Centri di valutazione

CVCN: Centro di valutazione e certificazione nazionale

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

CVE: *Common Vulnerabilities and Exposures*

CVSS: *Common Vulnerabilities Scoring System*

D

DDoS: *Distributed Denial of Service*

DEP: *Digital Europe Programme*

DFIR: *Digital Forensic Incident Response*

DIS: Dipartimento delle informazioni per la sicurezza

DORA: *Digital Operational Resilience Act*

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

E

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

ECCG: *European Cybersecurity Certification Group*

ECF: *European Competitiveness Fund* – Fondo europeo per la competitività

ECSC: *European Cybersecurity Challenge*

EDT: *Emerging Disruptive 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*

EUSA: *EU Space Act*

G

GDPR: *General Data Protection Regulation* – Regolamento generale sulla protezione dei dati

GPAI: *General-Purpose Artificial Intelligence* – Intelligenza artificiale per scopi generali

H

HPC: *High Performance Computing*

HWPCI: *Horizontal Working Party on Cyber Issues*

I

IA: Intelligenza artificiale

IaaS: *Infrastructure-as-a-Service*

ICE: Agenzia per la promozione all'estero e l'internazionalizzazione delle imprese italiane

ICS: *Industrial Control Systems*

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

INCIBE: Istituto nazionale di cybersicurezza della Spagna

IoC: *Indicator of Compromise* – Indicatore di compromissione

IoT: *Internet of Things*

IPCR: *Integrated Political Crisis Response*

IPZS: Istituto poligrafico e zecca dello Stato

ISAC: *Information Sharing and Analysis Centre*

ITS: Istituti tecnologici superiori

IVASS: Istituto per la vigilanza sulle assicurazioni

L

LAP: Laboratori accreditati di prova

LVS: Laboratori per la 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

MIT: Ministero delle infrastrutture e dei trasporti

MUR: Ministero dell'università e della ricerca

N

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

NCS: Nucleo per la cybersicurezza

NIS: *Network and Information Systems*

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

NISP: Nucleo interministeriale situazione e pianificazione

O

OCSE: Organizzazione per la cooperazione e lo sviluppo economico

OCSI: Organismo di certificazione della sicurezza informatica

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

OT: *Operational Technology*

P

PA: Pubblica Amministrazione

PaaS: *Platform-as-a-Service*

PMI: Piccole e medie imprese

PNRR: Piano nazionale di ripresa e resilienza

PQC: *Post-Quantum Cryptography*

PSNC: Perimetro di sicurezza nazionale cibernetica

Q

QKD: *Quantum Key Distribution*

R

ROSI: *Return on Security Investment*

S

SaaS: *Software-as-a-Service*

SBOM: *Software Bill of Materials*

SCADA: *Supervisory Control And Data Acquisition*

SNA: Scuola nazionale dell'Amministrazione

SOC: *Security Operations Center*

V

VLAP: Valutatori dei Laboratori accreditati di prova