Nuova edizione ottobre 2026

RAPPORTO

Clusit

sulla Cybersecurity
in Italia e nel mondo

2026

SECURITY SUMMIT

Indice

Prefazione 5

Introduzione al Rapporto 8

Panoramica sull'evoluzione del cyber crime in Italia e nel mondo

- Analisi dei principali incidenti cyber del I semestre 2026 11
- Attività e segnalazioni della Polizia Postale e per la Sicurezza Cibernetica nel 1° semestre del 2026 35
- Sicurezza e frodi informatiche in Banca 95

SPECIALE MANUFACTURING

- Analisi dei principali incidenti cyber noti del primo semestre 2026 verso il settore Manufacturing a livello globale e in Italia 105
- Una fotografia sulla cybersecurity degli ambienti OT nelle imprese italiane . . 116

SPECIALE INTELLIGENZA ARTIFICIALE

- AI Act, una normativa particolare 127
- Shadow AI: il rischio invisibile nell'era dell'AI 141

SURVEY

- La maturità cyber delle mPMI italiane dalle evidenze del PID Cyber Check 2025 155
- Cybersecurity nelle imprese modenesi: due anni a confronto, tra progressi organizzativi e ritardi tecnici 166

FOCUS ON 2026

- Il tempo come nuova superficie di attacco 183
- Continuous Authorization: perché l'IAM tradizionale è fallito (e come l'intelligenza artificiale ridefinisce il controllo di accesso) 193
- Cybersecurity sistemica: superare gli strumenti isolati per governare il rischio 201
- Come si legge un certificato ISO/IEC 27001 (e cosa non dice) 209

Glossario 229

Gli autori del Rapporto Clusit 2026 - Edizione di ottobre 255

CLUSIT e Security Summit 270

Copyright © 2026 CLUSIT
Tutti i diritti dell'Opera sono riservati agli Autori e al Clusit.
È vietata la riproduzione anche parziale di quanto pubblicato
senza la preventiva autorizzazione scritta del CLUSIT.

ASTREA

Via Copernico, 38 - 20125 Milano

Prefazione

Come possiamo constatare dai Rapporti Clusit pubblicati negli ultimi anni, lo scenario internazionale è caratterizzato da una crescente pressione cyber, dalla maggiore professionalizzazione della criminalità informatica, che vende attacchi o malware "as a service", e dalla sovrapposizione tra interessi economici, tensioni geopolitiche e operazioni di influenza. Ransomware, furto di credenziali, compromissione della catena di fornitura digitale, attacchi alle infrastrutture critiche e campagne di phishing continuano a rappresentare minacce rilevanti, mentre l'intelligenza artificiale sta modificando sia le capacità degli attaccanti che gli strumenti a disposizione dei difensori.

Per comprendere l'evoluzione del fenomeno è tuttavia necessario distinguere tra numero degli incidenti, gravità degli impatti, numero degli attacchi osservati e capacità di rilevazione. Questi indicatori non è detto che coincidano: un aumento delle segnalazioni può riflettere una maggiore attività criminale, ma anche una migliore capacità di individuare gli eventi e obblighi di notifica più stringenti. Analogamente, un numero relativamente contenuto di incidenti può nascondere eventi di elevata gravità, capaci di compromettere interi settori economici. A livello mondiale, la tendenza degli ultimi anni evidenzia una pressione cyber elevata e una progressiva evoluzione delle modalità operative degli attaccanti. La disponibilità di strumenti facilmente accessibili, la diffusione di servizi criminali acquistabili online e la possibilità di colpire organizzazioni geograficamente distanti hanno abbassato alcune barriere d'ingresso, rendendo possibile condurre campagne articolate anche senza possedere competenze tecniche particolarmente avanzate.

Sono diventati particolarmente rilevanti gli attacchi che sfruttano credenziali rubate, vulnerabilità non corrette, sistemi esposti su Internet e relazioni di fiducia tra organizzazioni. La compromissione di un fornitore tecnologico o di un servizio condiviso può consentire di raggiungere numerosi soggetti attraverso un unico punto di ingresso, amplificando gli effetti dell'incidente.

Un ulteriore elemento è rappresentato dalla crescente dimensione geopolitica delle operazioni informatiche. Gruppi criminali, soggetti riconducibili a Stati e attori che perseguono obiettivi di spionaggio o destabilizzazione possono operare in uno scenario in cui le motivazioni economiche e politiche talvolta si sovrappongono. Le tensioni internazionali contribuiscono inoltre ad aumentare il rischio di attacchi dimostrativi, attività di disturbo e campagne contro istituzioni, imprese strategiche e infrastrutture essenziali.

Tuttavia, dai dati di questo rapporto, che vedono scendere considerevolmente gli attacchi DDOS in Italia rispetto al 2025, parrebbe che il perdurare di alcuni conflitti abbassi l'interesse del pubblico verso attacchi dimostrativi che, quindi, non fanno più notizia e non vengono pubblicati e divulgati.

L'intelligenza artificiale generativa introduce infine un fattore di accelerazione. Può rendere più convincenti i messaggi fraudolenti, facilitare la produzione di contenuti in diverse lingue e sostenere alcune fasi della ricognizione e della preparazione degli attacchi, per non parlare della capacità di produrre malware in tempi brevi e con grande efficienza. Generalmente non si tratta della nascita di minacce completamente nuove, quanto piuttosto di un possibile incremento della velocità, della scala e della personalizzazione di attività già conosciute.

Stiamo anche assistendo a un continuo ampliamento della superficie di attacco con Cloud, dispositivi mobili, lavoro da remoto, Internet of Things, applicazioni e interfacce API, convergenza IT-OT. A questo tema, nel Rapporto, è dedicato uno specifico approfondimento che fotografa la "postura" difensiva delle aziende OT italiane. Anche la supply chain costituisce un fattore di ampliamento della superficie di attacco: una vulnerabilità nei sistemi di un qualunque fornitore costituisce la porta di accesso per scalare altri sistemi. Il recente episodio degli attacchi ai sistemi di refrigerazione di alcune catene di supermercati francesi ne è la testimonianza.

Non si può certamente pensare di riuscire ad azzerare il rischio di essere attaccati ma si può fare molto per minimizzarlo e per aumentare la capacità di ripartire (la resilienza!): prima di tutto insistendo sulla formazione e la creazione di consapevolezza anche tramite esercitazioni dedicate, in modo da ridurre l'incidenza del fattore umano. Avere un piano di valutazione del rischio e delle contromisure è indispensabile. Altrettanto importante è integrare l'intelligenza artificiale nella difesa: l'IA può potenziare i centri operativi di sicurezza (SOC), supportare l'analisi degli incidenti e accelerare la risposta.

Nello stesso tempo, rafforzare la cooperazione migliorerebbe la capacità di risposta collettiva: gli attacchi non rispettano i confini nazionali e possono coinvolgere simultaneamente più organizzazioni e Paesi. La condivisione tempestiva delle informazioni, il coordinamento tra autorità e imprese e la cooperazione internazionale sono indispensabili per anticipare le minacce e limitarne gli effetti.

A questi aspetti si aggiunge la necessità di tradurre gli obblighi normativi in capacità operative concrete. Il quadro europeo, dalla direttiva NIS2 al Cyber Resilience Act, rafforza l'attenzione alla gestione del rischio, alla sicurezza dei prodotti digitali e alla responsabilità degli operatori.

La sfida sarà evitare che la conformità rimanga un adempimento documentale, trasformandola invece in un miglioramento misurabile della sicurezza.

La priorità per il prossimo futuro non dovrebbe quindi essere soltanto ridurre il numero degli attacchi, obiettivo che nessuna organizzazione può garantire autonomamente, ma ridurre la probabilità che un attacco abbia successo e, soprattutto, limitarne gli effetti quando si verifica.

Ciò richiede investimenti continui, una gestione integrata del rischio, tecnologie adeguate, competenze specialistiche e una cultura della sicurezza condivisa. La cybersicurezza deve essere considerata una responsabilità strategica del management e delle istituzioni, non un problema delegabile esclusivamente ai reparti informatici.

In ultima analisi, la capacità di un Paese di proteggere i propri dati, servizi essenziali, infrastrutture e competenze digitali costituisce una componente sempre più importante della sua autonomia tecnologica e della sua resilienza economica e sociale.

Anna Vaccarelli
Presidente Clusit

© Clusit 2026

Introduzione al Rapporto

Il Rapporto inizia come sempre con **una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel primo semestre del 2026**, confrontandoli con i dati raccolti negli anni precedenti.

La panoramica degli attacchi in Italia è poi completata dalle **rilevazioni e segnalazioni della Polizia Postale e per la Sicurezza Cibernetica**, che ci ha fornito dati e informazioni estremamente interessanti su attività ed operazioni svolte nel corso dei primi sei mesi di quest'anno.

Riportiamo inoltre i principali contenuti del Report 2026 "**Sicurezza e Frodi Informatiche in Banca**", che viene realizzato annualmente dal CERTFin e fornisce una fotografia aggiornata del livello di rischio cyber e delle frodi e truffe informatiche nel settore finanziario italiano, che raccoglie i dati segnalati da 35 organizzazioni rappresentative di oltre il 90% del settore.

Segue uno **Speciale Manufacturing**, che presenta un'analisi sulla evoluzione della **Cybersecurity in ambito manifatturiero/industriale**, con i dati di settore tratti dalle ultime rilevazioni Clusit al 30 giugno 2026. Questa analisi è poi completata da una fotografia sulla **cybersecurity degli ambienti OT nelle imprese italiane**, a cura delle Women for Security.

Presentiamo ora uno **Speciale Intelligenza Artificiale**, con due articoli:

- **AI Act, una normativa particolare**, a cura di Giancarlo Butti
- **Shadow AI: il rischio invisibile nell'era dell'AI**, a cura di Federica Maria Rita Livelli.

Seguono due **survey** realizzate entrambe presso le micro, piccole e medie imprese. La prima, dal titolo "**La maturità cyber delle mPMI italiane dalle evidenze del PID Cyber Check**", realizzata su scala nazionale, con uno strumento di autovalutazione promosso da **Unioncamere** e dal sistema delle **Camere di Commercio**, in collaborazione col mondo della ricerca (**IIT-CNR**) e i Competence Center nazionali (**CYBER 4.0** e **START 4.0**). La seconda, giunta alla sua terza edizione, è **una survey sulla Cybersecurity nelle imprese modenesi**. **669 aziende hanno risposto alla survey che è stata realizzata** nel 2026 **dalla Camera di Commercio di Modena** in collaborazione **con l'Università di Modena e Reggio Emilia** e con il Clusit.

È interessante il confronto tra le due iniziative, che esaminano aspetti diversi della stessa problematica.

Questi sono infine i temi trattati nella sezione FOCUS ON:

- **Il tempo come nuova superficie di attacco**, a cura di CrowdStrike
- **Continuous Authorization: Perché l'IAM tradizionale è fallito (e come l'intelligenza artificiale ridefinisce il controllo di accesso)**, a cura di Oplon Networks
- **Cybersecurity sistemica: superare gli strumenti isolati per governare il rischio**, a cura di Cyberoo
- **Come si legge un certificato ISO/IEC 27001 (e cosa non dice)**, a cura di Andrea Cabras.

© Clusit 2026

Analisi dei principali incidenti cyber del I semestre 2026

Volume, frequenza, velocità: le nuove sfide della cyber security

In questo aggiornamento semestrale del Rapporto CLUSIT 2026, giunto al suo quattordicesimo anno di pubblicazione, analizziamo i più gravi incidenti cyber avvenuti a livello globale nell'ultimo semestre, confrontandoli con l'andamento del 2025 e con la serie storica dal 2021.

L'obiettivo è fornire ai lettori una bussola per navigare in uno scenario che, nel corso dell'ultimo semestre, ha mostrato dinamiche di grande discontinuità rispetto agli anni precedenti.

Aumento significativo di volumi e perdite complessive

I dati raccolti nel primo semestre 2026 delineano un quadro di escalation massiva. Nel primo semestre 2026, a parità di risorse e di capacità di analisi dei dati, abbiamo registrato 4.911 incidenti: un numero che non ha precedenti nella storia della nostra pubblicazione.

Si tratta di un incremento inequivocabile: il volume è più che raddoppiato rispetto al semestre precedente (+105%) e ha superato del 71% l'intero primo semestre del 2025.

In termini di frequenza, la media mensile a livello globale è passata dai 171 incidenti del 2021 agli (impressionanti) 819 del semestre in esame: in cinque anni, l'intensità degli attacchi osservati è quasi quintuplicata.

Pur trattandosi di incidenti rilevati da fonti aperte, cioè di attacchi andati "a buon fine" e diventati di dominio pubblico (la "punta dell'iceberg"), il volume degli attacchi cresce in modo più che lineare, il che inevitabilmente fa aumentare il livello delle perdite complessive, anche a parità di severity media dei singoli incidenti.

Il paradosso della trasparenza

Questa crescita non è uniforme, e dai dati emerge un paradosso che richiede un'analisi puntuale: mentre i regimi normativi impongono obblighi di notifica sempre più stringenti, e quindi portano a far emergere un numero sempre maggiore di eventi, la trasparenza tecnica sui dettagli degli attacchi sembra diminuire.

Nel primo semestre 2026, la quota di incidenti per i quali non è stato possibile determinare la tecnica di attacco (c.d. categoria "Undisclosed") basandoci su fonti pubbliche è esplosa, raggiungendo i due terzi del campione totale.

Questo dato suggerisce alcuni possibili scenari, probabilmente non alternativi: una crescente capacità degli attaccanti di compiere attacchi "non standard", che sfuggono alle classificazioni tradizionali, e un limite strutturale nella capacità di risposta e investigazione delle organizzazioni.

Ve ne è anche un terzo: le organizzazioni stanno probabilmente apprendendo la lezione di quanto sia importante avere un approccio alla comunicazione adeguata degli incidenti verso i propri stakeholder, per minimizzarne le conseguenze negative in termini reputazionali ed operativi.

Ciò può significare, nell'interesse delle stesse organizzazioni, favorire una maggiore trasparenza rispetto alle conseguenze attese delle singole violazioni, mantenendo un profilo di maggiore riservatezza su dettagli tecnici che possono prestare il fianco a conseguenze reputazionali, ma anche a futuri attacchi basati sulla rivelazione di informazioni peculiari sui sistemi di sicurezza.

Infine, gioca un ruolo importante anche il fatto che l'obiettivo delle comunicazioni obbligatorie degli incidenti alle Agenzie nazionali e agli Enti Regolatori, previste da normative come Dora, la NIS2 e nel prossimo futuro[1] il Cyber Resilience Act, non necessariamente si trasformano in una maggiore trasparenza verso il grande pubblico. La finalità di tali obblighi, infatti, va dal coordinamento e supporto della risposta agli eventi più gravi, verso vittime accertate o potenziali, alla gestione degli stessi in scenari B2B (con conseguente comunicazione puntuale verso soggetti specifici), cercando in tutti i casi possibili di preservare la reputazione delle vittime. Anche in situazioni maggiormente eclatanti, che non possono sfuggire alla diffusione mediatica, aspetti quali la natura dell'attacco, o la matrice dell'attaccante, quando non utili agli obiettivi di prevenzione e minimizzazione delle conseguenze, sono correttamente mantenuti riservati.

Ai fini del nostro Rapporto, questo ha determinato e determinerà sempre più in futuro una maggiore latenza tra la registrazione dell'incidente e le informazioni di dettaglio su cosa sia avvenuto nello specifico incidente per caratterizzarne origine, tecnica e conseguenze.

[1] L'obbligo di notifica ai sensi del Cyber Resilience Act è in vigore dall'11 Settembre 2026, pertanto non è applicabile all'attuale campione di incidenti.

Resta comunque vero, come ampiamente descritto nell'appendice metodologica, che l'obiettivo di questo documento non è la completezza rispetto a tutti gli incidenti che avvengono nello scenario globale, quanto rappresentare, con una metodologia solida e una base statistica rilevante, le tendenze e i fenomeni macroscopici che possono aiutare le organizzazioni a porre in essere scelte tattiche e strategiche sugli interventi volti a rafforzare la propria postura di sicurezza.

L'ombra dell'IA

Il motore dell'escalation di attacchi registrati nel I semestre 2026 è quasi interamente il Cybercrime, che ha generato il 95,4% del totale degli incidenti. Parallelamente, assistiamo ad un'ennesima mutazione del panorama degli attacchi: se da un lato l'Hacktivism mostra un calo significativo rispetto all'anno precedente, dall'altro stiamo entrando in una nuova fase caratterizzata dal crollo delle barriere di accesso per nuove tipologie di attaccanti, una sorta di "democratizzazione" dell'attività malevola fai-da-te, resa possibile dalla diffusione di modelli AI sempre più performanti anche in questo campo specifico, ormai alla portata di chiunque.

L'ingresso dell'Intelligenza Artificiale nell'arsenale degli attaccanti sta progressivamente cambiando le regole del gioco. L'IA agisce come un moltiplicatore di forza su due fronti distinti ma complementari:

- aumento della sofisticazione: gli attacchi stanno diventando più avanzati, meno prevedibili, capaci di eludere le protezioni tradizionali e di colpire con maggiore efficacia, rendendo la difesa un bersaglio sempre più mobile;
- riduzione della barriera all'ingresso: l'IA permette anche ad attori non esperti di orchestrare attacchi complessi, ed aumenta esponenzialmente il numero di attori malevoli attivi nel cyber-spazio.

Beninteso: l'IA non è ancora il fattore determinante nella crescita che abbiamo osservato nel I semestre 2026. D'altro canto, la preoccupazione sta proprio nel fatto che oggi rileviamo solo una prima, timida, manifestazione dello scenario prossimo venturo, ovvero quello rivelato dall'AI Mythos e dalle sue eredi: il prossimo passo sarà la completa automazione degli attacchi, l'*"agentic hacking"* in cui squadre di AI opereranno di concerto adattando i propri comportamenti e concatenando tecniche differenti e vulnerabilità anche banali (quelle che oggi finiscono immancabilmente nelle "fasi 2" delle attività di remediation) per violare i sistemi informativi delle organizzazioni.

Situazione dell'Italia: inversione di tendenza o tregua momentanea?

In questo scenario, l'Italia nel primo semestre 2026 mostra un profilo peculiare. Sebbene abbiamo registrato una leggera ripresa degli incidenti rispetto al 2025, la nostra quota percentuale rispetto al totale mondiale è scesa al 5%, contro il 9,5% del semestre precedente. Inoltre, la crescita del volume di incidenti in Italia è stata inferiore alla media globale.

Anche la gravità degli attacchi è variata nell'ultimo semestre, benché in senso negativo: in Italia la maggior parte degli incidenti si è spostata dalla categoria "Medium/Low" al livello High, complice la riduzione degli eventi di DDoS e di matrice Hacktivism.

Il fatto che l'Italia sia meno colpita in termini percentuali rispetto alla crescita degli incidenti a livello globale non significa che il Paese sia meno esposto: per esempio il settore del Manufacturing è oggi il principale bersaglio in Italia, confermando come le piccole e medie imprese produttive rimangano il bersaglio più attenzionato da parte di un cybercrime sempre più efficiente e automatizzato.

Oltre al presente: la sfida della resilienza come fattore strategico

I segnali che emergono dai dati ci impongono di guardare oltre il semplice conteggio degli incidenti. La complessità tecnologica e l'automazione degli attacchi stanno rendendo il mantenimento di capacità difensive adeguate sempre più costoso da sostenere. Il rischio è quello di una saturazione delle risorse disponibili per i difensori, che rischiano di essere travolti dai nuovi livelli di attività malevola.

A questo riguardo, i dati del semestre appena trascorso evidenziano tre punti di attenzione a livello strategico:

- **la necessità di difese "AI-specifiche"**: le contromisure basate su logiche statiche sono destinate a fallire contro attacchi orchestrati da algoritmi. La difesa deve evolvere verso una capacità di risposta rapida, automatizzata e predittiva, in modo da compensare l'incremento dei volumi (e quindi delle probabilità di subire un incidente) e della velocità degli attacchi, e di conseguenza mitigare le perdite complessive per il Paese;
- **la necessità di gestire il rischio sistemico:** la crescente pressione applicata da queste minacce può rappresentare un rischio sistemico, dal momento che superata una certa soglia di frequenza degli incidenti, alcuni settori (in particolare manifatturiero, governo centrale e locale, infrastrutture critiche, fornitori di servizi ICT) potrebbero ritrovarsi in una condizione di sofferenza costante, con ricadute anche

importanti sul loro buon funzionamento e, di conseguenza, sul sistema economico nazionale;

- **l'urgenza di una governance adattiva e di responsabilità condivise**: in un mondo dove l'attacco è diventato costante e "alla portata di chiunque", la cybersecurity non può più essere considerata un costo di conformità, ma deve diventare il pilastro centrale della continuità operativa delle singole organizzazioni, evolvendo nell'arco di mesi e, allo stesso tempo, una responsabilità collettiva a supporto della resilienza nazionale.

Confidando che questo Rapporto CLUSIT possa offrire strumenti utili per comprendere e affrontare questa nuova, complessa realtà, auguriamo a tutti una buona lettura.

© Clusit 2026

Analisi dei principali incidenti cyber noti a livello mondiale dal 2021 al I semestre 2026

In questa sezione offriamo una panoramica degli incidenti di sicurezza più significativi avvenuti a livello mondiale nel primo semestre 2026, confrontandoli con il semestre precedente, con lo stesso semestre del 2025 e con i dati raccolti dal 2021.

Lo studio si basa sull'analisi di incidenti cyber di pubblico dominio che hanno avuto impatti significativi, sotto il profilo economico, tecnologico, legale e reputazionale, sulle organizzazioni che ne sono state vittime.

Nel periodo in esame, tra gennaio 2021 e giugno 2026, abbiamo censito un totale di 21.034 incidenti, così distribuiti per semestre (Fig. 1).

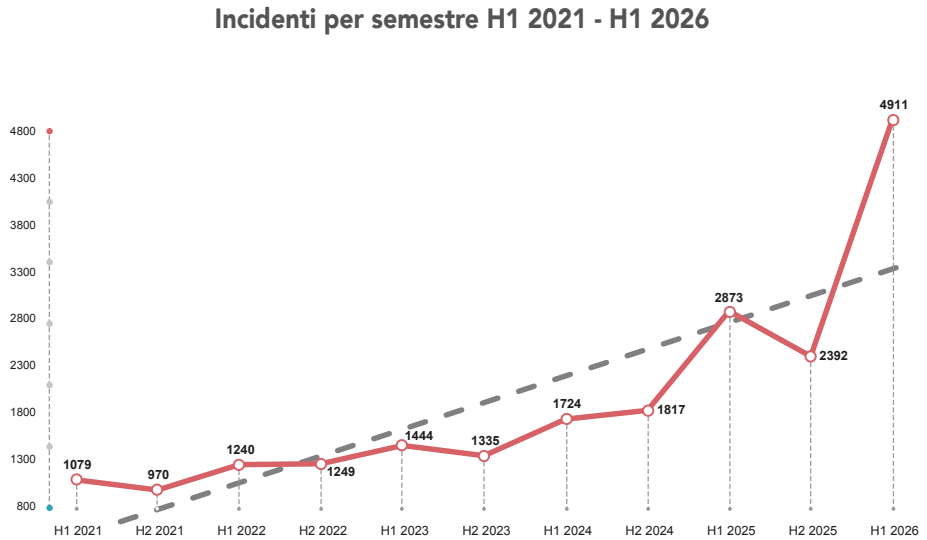


Fig. 1 - Andamento degli incidenti cyber nel periodo 2021 - I sem. 2026

Nel primo semestre 2026 abbiamo registrato 4.911 incidenti: il numero più alto di sempre per un singolo semestre, più del doppio del semestre precedente (2.392, **+105%**) e il 71% in più rispetto al primo semestre 2025 (2.873).
In sei mesi è stato quasi raggiunto il totale dell'intero 2025 (93% dei 5.265 incidenti dell'anno), e gli eventi del semestre rappresentano da soli quasi un quarto (23%) di tutti quelli censiti dal 2021.

Anche la media mensile segna un salto: 819 incidenti al mese, contro i 439 del 2025 e i 171 del 2021, quasi cinque volte tanto in cinque anni. Il mese meno intenso del semestre (febbraio, 684 incidenti) supera il mese peggiore dell'intero 2025 (aprile, 511), e giugno, con 984 incidenti, è il mese con più eventi mai registrato.

Questa crescita va però letta con attenzione. Si concentra interamente negli incidenti per i quali non è stato possibile determinare la tecnica di attacco (Undisclosed), che passano da 943 nel primo semestre 2025 a 3.321, due terzi del campione. Gli incidenti di cui conosciamo la tecnica sono invece in calo (1.590, contro 1.930). Si conferma, e si amplifica, il tema già evidenziato nel Rapporto di marzo: il rafforzamento degli obblighi di notifica verso le Autorità non si traduce in maggiore trasparenza pubblica sui dettagli tecnici dei singoli attacchi, dato che l'obbligo di fornire dettagli alle autorità non comporta che queste rendano poi disponibili queste informazioni, se non in forma aggregata.

Distribuzione degli attaccanti per tipologia

La crescita in volume degli incidenti è trainata quasi esclusivamente dal Cybercrime: con 4.683 incidenti, nel primo semestre 2026 raggiunge il 95,4% del totale (era l'89,3% nel 2025 e l'87,2% nel primo semestre 2025) ed **eguaglia in sei mesi il numero di eventi dell'intero 2025** (4.704).

Information Warfare ed Espionage / Sabotage restano marginali in termini di quota (rispettivamente 1,5% e 1,9%), ma con andamenti diversi: gli incidenti di Information Warfare (73) raddoppiano rispetto al primo semestre 2025 e in sei mesi eguagliano quasi l'intero 2025 (75), mentre quelli di Espionage / Sabotage restano stabili in valore assoluto (93, contro 91 nel primo semestre 2025) e perdono peso sul totale. Sono, come ricordato più volte, le categorie per cui l'attribution è più complessa e il campione più sottostimato (rif. Appendice metodologica).
Il dato più netto del semestre riguarda l'**Hacktivism, in forte calo** (Fig. 2): 62 incidenti, contro i 227 del primo semestre 2025 **(-73%**) e i 307 dell'intero 2025, pari all'1,3% del totale. È una discontinuità rispetto alla crescita costante osservata dal 2022, coerente con il calo degli incidenti DDoS, la tecnica tipica di questa categoria (68 incidenti, contro i 251 del primo semestre 2025). Tra i possibili fattori può incidere la risposta delle forze di polizia[2], così come il minore clamore mediatico ormai

[2] Ad esempio, l'Operation Talent avvenuta a Gennaio ad opera delle forze di polizia tedesche con il supporto dell'Europol (https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world) o l'Operation Endgame, che in modo permanente ormai da tempo con azioni successive (l'ultima a maggio 2026 - https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source) mira a smantellare le principali botnet che colpiscono le organizzazioni europee.

attribuito a questo tipo di incidenti, che ha dirottato l'interesse degli stessi attaccanti su obiettivi diversi, destinati a generare maggiori impatti, ma molto più complessi nell'attuazione (ad esempio, verso le supply chain e i settori, come quello dei trasporti, logistica, ICT, che permettono di generare conseguenze trasversali su più ambiti): saranno i prossimi mesi a dire se si tratta di una tregua momentanea o di un vero e proprio cambio di tendenza.

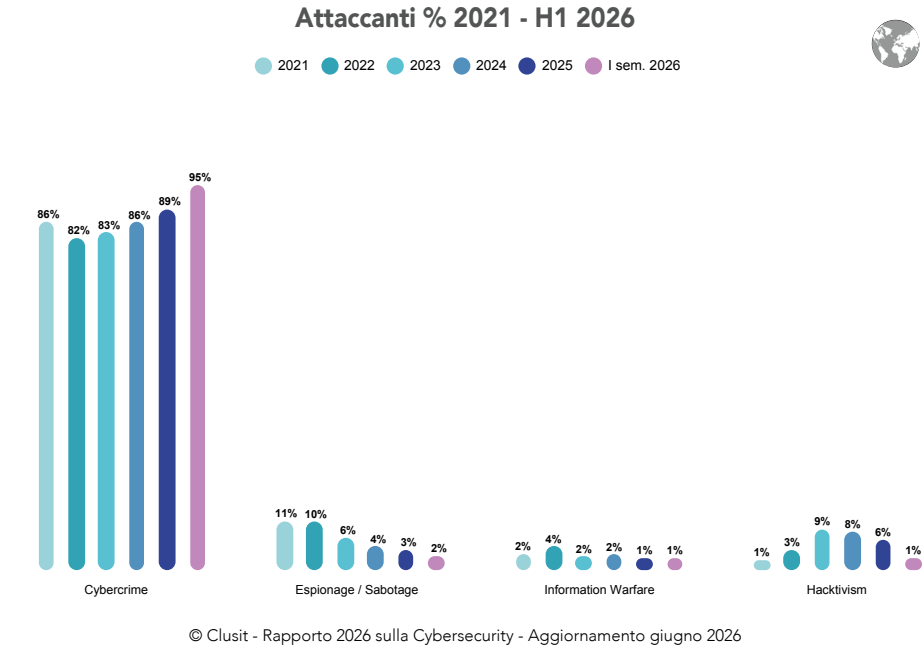


Fig. 2 - La distribuzione percentuale degli attaccanti nel periodo 2021 - I sem. 2026

Distribuzione delle vittime per categoria

Come nella precedente edizione semestrale, accanto alla quota sul totale guardiamo a quanti incidenti ciascun settore ha già accumulato in sei mesi rispetto all'intero anno precedente: è l'indicatore che meglio anticipa quali settori risulteranno più colpiti a fine anno. Nel primo semestre 2026 (**Fig. 3**) la categoria Gov / Mil / LE torna al primo posto della classifica, come non accadeva dal 2021: 751 incidenti, pari al 15,3% del totale, quasi il doppio del primo semestre 2025 (388) e già più dell'intero 2025 (644, +3,1 punti percentuali rispetto al 2025 in soli sei mesi).

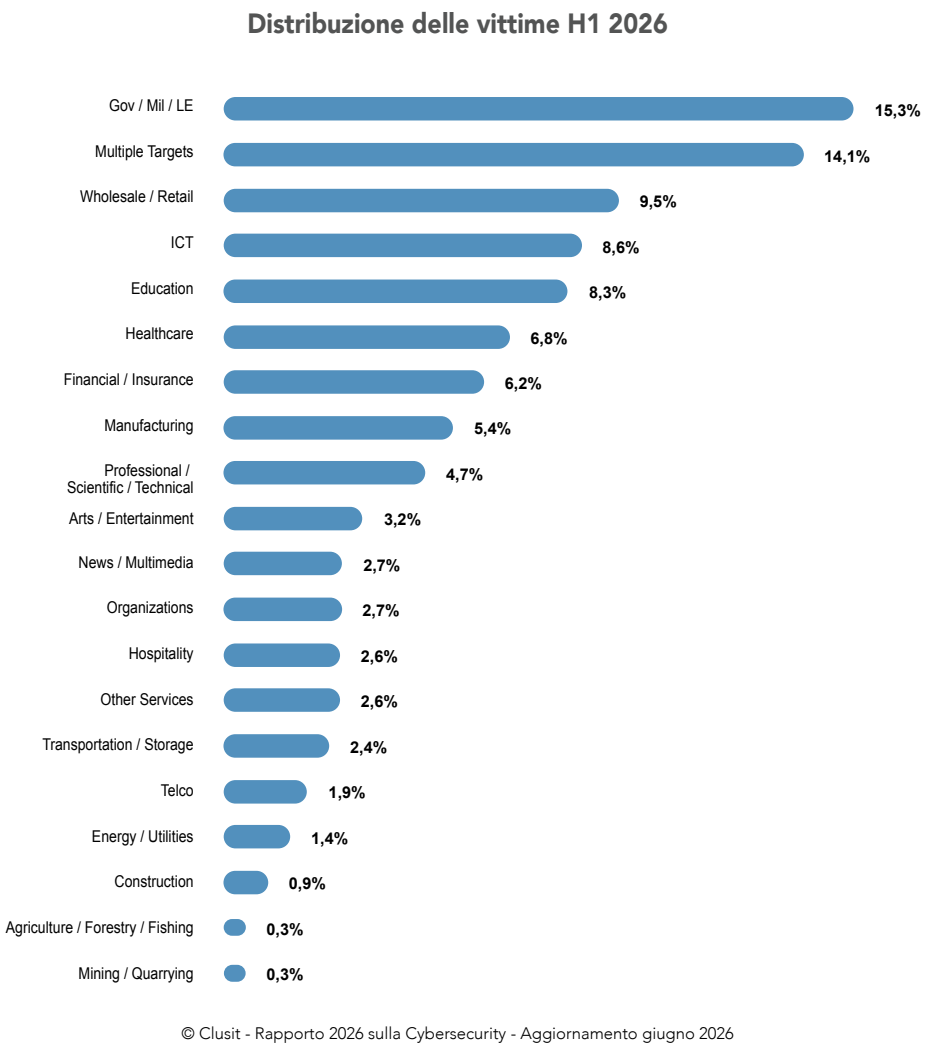


Fig. 3 - Distribuzione della tipologia di vittime nel I sem. 2026

Scendono al secondo posto le campagne che colpiscono più settori contemporaneamente (Multiple Targets): 690 incidenti, in crescita del 20% sul primo semestre 2025, ma con una quota che passa dal 23,5% del 2025 al 14,1%.

La crescita più marcata riguarda Wholesale / Retail, che sale dal nono al terzo posto: 467 incidenti, oltre quattro volte quelli del primo semestre 2025 (101) e più del doppio dell'intero 2025 (206). La quota sul totale passa dal 3,9% al 9,5%.

Segue il settore ICT (422 incidenti, 8,6%), che in sei mesi supera già il totale del 2025 (375): trattandosi di organizzazioni che tipicamente dispongono di competenze specialistiche, e che sono in grado di realizzare economie di scala sulla spesa di cybersecurity, nello scegliere questi bersagli gli attaccanti probabilmente ritengono che il maggiore sforzo nel violare tali soggetti sia ripagato dalla possibilità di colpire contemporaneamente i numerosi clienti che utilizzano i servizi informatici che questi erogano.

Il settore Education (406 incidenti, 8,3%): dopo essere stato nel 2025 l'unico settore della top ten in calo, registra nel semestre l'80% di incidenti in più rispetto all'intero anno precedente.

Il settore Healthcare scende dal terzo al sesto posto: 335 incidenti, stabili rispetto al primo semestre 2025 (337) e pari al 60% dell'intero 2025, con una quota che si riduce dal 10,6% al 6,8%. A diminuire è il peso sul totale, non l'esposizione: il ritmo in valore assoluto è lo stesso dell'anno scorso, e Healthcare resta il settore con la quota più alta di incidenti con impatto Critical o Extreme (58%, contro una media del campione del 24%).

Financial / Insurance (304 incidenti, 6,2%) mantiene una quota sostanzialmente invariata rispetto al 2025 (6,3%) e in sei mesi raggiunge il 92% degli eventi dell'intero anno.

Il Manufacturing perde invece quattro posizioni, dal quarto all'ottavo posto (267 incidenti, 5,4%, contro il 7,6% del 2025), pur crescendo del 25% sul primo semestre 2025.

Professional / Scientific / Technical (233 incidenti, 4,7%) conferma la quota del 2025, mentre entra nella top ten Arts / Entertainment (158, 3,2%), che in sei mesi supera del 36% il totale dell'anno precedente.

Esce invece dalla top ten Transportation / Storage, entrato per la prima volta nel 2025: 117 incidenti, stabili rispetto al primo semestre 2025 ma pari al 60% dell'intero anno, con una quota che scende dal 3,7% al 2,4%.

Tra i settori meno rappresentati, Hospitality (130 incidenti) e Agriculture / Forestry / Fishing (16) superano già in sei mesi il totale del 2025 (rispettivamente 101 e 6).

La classifica del semestre conferma quanto osservato in passato: alcuni settori possono subire impennate improvvise, spesso legate a campagne che sfruttano la loro dipendenza da specifiche soluzioni tecnologiche o da fornitori comuni nella supply chain. Saranno i dati consolidati di fine anno a dire se le crescite di Wholesale / Retail, Education e ICT sono tendenze strutturali o picchi di breve periodo.

Analisi degli incidenti cyber in Italia

In questa sezione scendiamo nel dettaglio della situazione italiana, con una panoramica degli incidenti di sicurezza avvenuti negli scorsi 6 mesi, messi a confronto con l'andamento dal 2021 in poi.
Complessivamente, tra il 2021 e il 2026 il campione ha incluso **1.677** eventi solo nel nostro Paese; nel primo semestre 2026 (**Fig.4**), gli incidenti noti di particolare gravità che hanno coinvolto vittime italiane sono **245. Considerata la crescita del 105% degli incidenti nel mondo, l'Italia realizza "solo" un 8% in più rispetto al semestre precedente**.

Il grafico conferma infatti una riduzione della crescita del numero di incidenti, iniziata a partire dal secondo semestre 2025 (227 incidenti), rispetto alla tendenza preoccupante che avevamo riscontrato a partire dal 2021 e che si era manifestata in modo significativo con il picco rilevato nel primo semestre 2025 (280 incidenti).

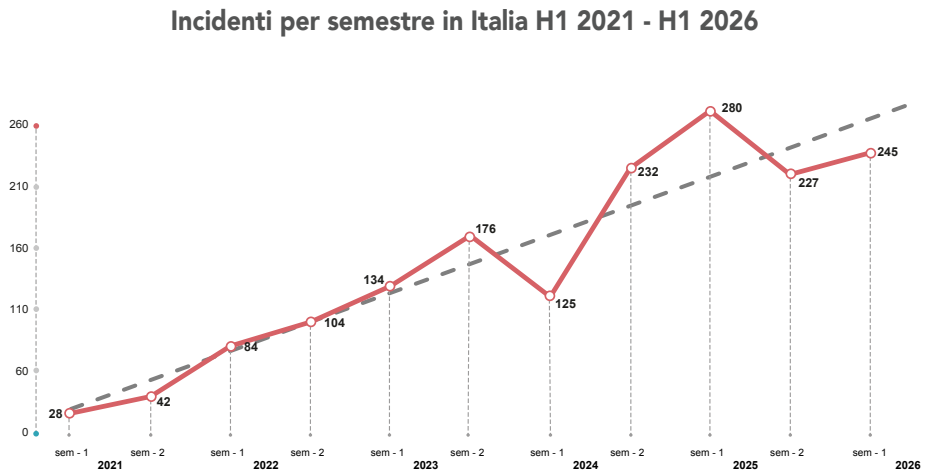


Fig. 4 - Distribuzione degli incidenti in Italia nel periodo I sem. 2021 - I sem. 2026

Nei primi 6 mesi del 2026, **gli attacchi avvenuti con successo contro le realtà del nostro Paese costituiscono il 5% del totale degli eventi rilevati nello stesso periodo a livello mondiale**. Al raddoppiare del numero di incidenti nel mondo, la componente dell'Italia si è circa dimezzata rispetto al secondo semestre 2025 (dove era pari al 9,5%): siamo tornati ai livelli di 5 anni fa, superando di poco il minimo del 3,4% segnato nel 2021.

Attendiamo scaramanticamente il dato dell'intero anno prima di tirare le conclusioni. Se avremo una conferma, **il dato sarebbe compatibile con uno scenario in cui l'aumento dell'attenzione al problema della Cybersecurity inizia a dare i primi riscontri positivi**, e che una parte del gap rispetto al passato sia stato colmato. Questa conferma non andrebbe letta come la fine di un percorso: piuttosto, le organizzazioni che hanno compiuto degli sforzi e che nell'ultimo periodo non hanno subito impatti significativi, **devono guardare al +105% degli incidenti a livello mondiale come una conferma che se i processi, le competenze e la tenuta di strumenti adeguati a proteggere l'organizzazione sono mantenuti costantemente attivi e all'avanguardia, ciò ha un effetto, anche se non visibile, positivo**.

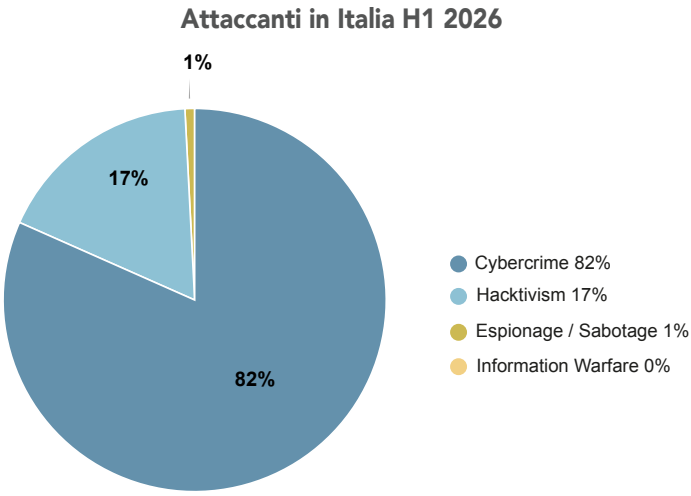
Distribuzione degli attaccanti per tipologia

Come sempre, questa sezione racconta molto delle evoluzioni nel mondo degli attaccanti e aiuta a capire quali fenomeni prevalenti devono essere tenuti sotto attenzione (**Fig.5**), cercando di individuare eventuali peculiarità del nostro Paese.

Tra quelli avvenuti in Italia nei primi 6 mesi del 2026, **la maggioranza degli incidenti noti è afferente alla categoria *Cybercrime*: nel primo semestre 2026, diversamente da quanto avvenuto negli anni precedenti, lo scenario italiano si avvicina a quello globale,** in cui il *Cybercrime* raggiunge quota 96%, mentre in Italia si attesta circa all'82%. L'*Hacktivism* - che nel 2025 aveva raggiungo quota 38,7%, seppure con incidenti di scarso rilievo, - si ferma invece al 17%.

Le ipotesi più plausibili nello spiegare questo cambiamento possono essere tanto una maggiore preparazione delle vittime a maggiore rilievo mediatico, già bersaglio più volte di questo tipo di attacchi negli anni precedenti, sia un progressivo allentamento dell'interesse mediatico nei confronti dei conflitti geopolitici, che genera di conseguenza anche un minore interesse da parte degli attaccanti: dopo 4 anni di conflitto Russia-Ucraina gli attacchi di hacktivism, se non sono plateali, non fanno più notizia.

Infine, in continuità con gli anni precedenti, nel nostro Paese non rilevano in modo significativo gli incidenti nelle categorie *Espionage / Sabotage* o *Information Warfare*.



© Clusit - Rapporto 2026 sulla Cybersecurity - Aggiornamento giugno 2026

Fig. 5 - Attaccanti in Italia nel primo semestre 2026

Distribuzione delle vittime per categoria

La distribuzione delle vittime degli attacchi è l'indicatore che più, negli ultimi anni, permette di analizzare i cambiamenti più significativi nello scenario degli attacchi informatici, tanto rispetto al grado di preparazione delle organizzazioni, tanto in riferimento alle strategie e campagne messe in atto dagli attaccanti.

Nel primo semestre del 2026 in Italia, assistiamo infatti ad una prima variazione di rilievo (**Fig.6**): il settore Manufacturing passa dal secondo posto nel 2025, al primo (è ottavo a livello globale) con un incremento di 6 punti percentuali, e il settore Governativo / Militare / Law Enforcement scende dal primo posto nel 2025 al terzo nel primo semestre 2026, con un crollo della percentuale dal 28,4% all'11%.
Questo dato è coerente con il dato relativo alla riduzione degli incidenti causati dall'Hacktivism (Fig.5), il cui bersaglio preferenziale sono proprio la Pubblica Amministrazione e le strutture governative, vista la natura dimostrativa di queste operazioni.
Il fatto che sia sensibilmente diminuito potrebbe essere imputato a una combinazione di tre fattori:

- che le pubbliche amministrazioni, soprattutto le più grandi e più soggette a questo fenomeno, abbiano migliorato procedure e dispositivi di difesa, e ciò è compatibile anche con il quadro di enforcement introdotto dal combinato disposto di dispositivi normativi quali la Legge 90 del 2024 e la NIS2;

- che sempre più spesso l'operatività dei servizi, in caso di attacchi finalizzati al diniego del servizio, venga ripristinata in poche ore: ciò anche grazie alla recente attivazione degli obblighi di segnalazione al CSIRT Nazionale presso l'Agenzia per la Cybersicurezza Nazionale (ACN);
- per i soggetti NIS2, che favorisce un quadro di coordinamento e la possibilità di ottenere un supporto specialistico da parte delle vittime, unitamente all'azione di segnalazione che la stessa ACN compie verso i soggetti in perimetro NIS2 rispetto alle vulnerabilità più gravi e alle campagne di attacco in corso;
- che le fonti pubbliche (tra cui molte testate) danno sempre meno evidenza a notizie di questo genere, ritenute ormai di minore interesse.

Ovviamente, queste ipotesi dovranno essere validate dai dati completi del 2026, seppure diversi fenomeni mostrano già elementi di continuità con i trend rilevati negli anni precedenti.
Ad esempio, il fatto che il settore Manufacturing occupi il primo posto, passando da 11,7% (dato annuale 2025) al 18,4% nei primi sei mesi del 2026, è purtroppo la fotografia di un interesse consolidato negli ultimi anni dei cybercriminali, sussistono complessi ecosistemi di fornitura costituiti anche da medie e piccole imprese. Da notare che **l'incidenza delle vittime italiane su quelle a livello globale, in questo settore, è del 17%**.

Al secondo posto (come accade nel mondo), quasi a pari merito con la prima posizione, ritroviamo le campagne generalizzate su settori diversi (Multiple Targets, 18% del totale).

Si è già detto del settore pubblico, a cui seguono a pari merito il settore ICT e Wholesale/Retail (8,6%). Il settore *ICT* in particolare registra un aumento di 4,4 punti percentuali rispetto alla rilevazione 2025 e una scalata di ben tre posizioni nella classifica: come accade livello mondiale, è evidente l'interesse degli attaccanti di generare un forte impatto a cascata sulle organizzazioni andando a colpire i fornitori di servizi digitali. La forte attenzione che le normative negli ultimi anni hanno posto sulle modalità di scelta delle terze parti in relazione ai rischi, e la relativa definizione di presidi di protezione nell'ambito delle singole forniture, trova concreta giustificazione nell'incremento degli incidenti su questo settore.

Continuando a registrare una crescita statisticamente rilevante di incidenti anno su anno, Wholesale / Retail scala di un'altra posizione la classifica rispetto al 2025: l'interesse verso questo settore è progressivamente crescente da parte degli attaccanti, e ciò potrebbe non escludere un ulteriore livello di escalation come in passato è avvenuto su altri settori.

Tra i rimanenti settori, rileva *Arts / Entertainment* che subisce un notevole incremento, passando da 1,2% a 2,9%: questa "impennata" fa pensare che le difese in questo settore siano particolarmente basse, rendendolo appetibile per i cybercriminali.

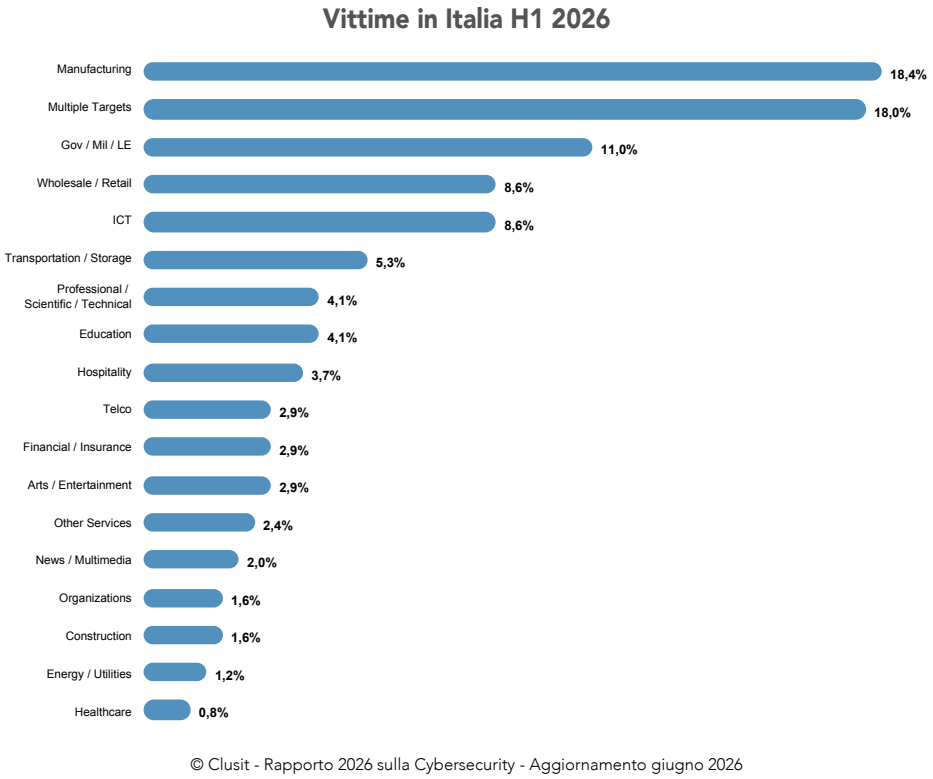


Fig. 6 - Distribuzione delle vittime in Italia I sem. 2026

Questi dati definiscono un quadro ancora preoccupante della capacità di protezione sia delle organizzazioni pubbliche sia delle imprese: è evidente che le tecniche di difesa introdotte non sono all'altezza di quelle degli attaccanti e che la presenza di vulnerabilità rende questi obiettivi particolarmente appetibili per gli hacker. È una tendenza da seguire con molta attenzione, che rischia di peggiorare ulteriormente nel prossimo futuro: le tecniche di attacco sono infatti sempre più sofisticate, anche grazie all'utilizzo di Intelligenza Artificiale, ed è necessario che anche le contromisure adottate dalle organizzazioni si adeguino al livello tecnologico degli attaccanti.

Non mancano però le buone notizie: Energy / Utilities vede dimezzato il valore percentuale degli incidenti in questo settore passando da 2,4% dell'anno 2025 all'1,2% del primo semestre 2026, e a confronto con i dati dell'intero 2025, si segnala un'ulteriore diminuzione degli incidenti rivolti al settore *Healthcare* che risulta ultimo in classifica.

Quest'ultimo è un segnale estremamente positivo, benché vada letto con prudenza, in quanto il confronto con altri report nazionali e internazionali disegna un quadro ancora incerto[3]. Se anche nel secondo semestre trovassimo un ulteriore riscontro positivo, potremmo spiegare il fenomeno con la corrispondenza con l'attuazione delle iniziative sostenute tramite PNRR in ambito Pubblico, con la pressione di normative come la NIS2, nonché dall'attenzione accesa sul settore a livello mondiale causata dai picchi di incidenti avvenuti a cavallo tra il periodo pre-COVID-19 e gli anni immediatamente successivi. Come avvenuto in passato nel settore finanziario, dove i dati di questo Rapporto hanno riscontrato nei grandi numeri gli effetti benefici dell'attuazione delle normative sulla cybersecurity (PSD, DORA, …), ulteriori casi in cui sia evidente un rapporto di causalità tra i meccanismi che sostengono la spesa in cybersecurity e l'abbassamento degli incidenti complessivi su interi settori o filiere, impone di fare riflessioni sulle modalità con le quali perseguire le direttrici strategiche di sviluppo del digitale nel prossimo futuro, nel nostro paese. D'altro canto, è corretto anche domandarsi se gli obiettivi di rafforzamento della cybersecurity in Italia possano ancora essere raggiunti a colpi di normative, e non grazie ad un salto di qualità del livello di consapevolezza delle singole organizzazioni.

Distribuzione delle tecniche di attacco

Anche l'analisi delle tecniche di attacco aiuta a comprendere le cause sottostanti l'elevata crescita degli incidenti subiti dalle nostre imprese e istituzioni.

Come evidenziato dalla **Fig.7**, la distribuzione delle tecniche di attacco è abbastanza diversa da quella del 2025. È il Malware che (ri)conquista il primo posto con il 43%, dal 22,7% del 2025, ripristinando un quadro, nel nostro paese, maggiormente coerente con il dato internazionale degli ultimi anni. Il dato maggiormente negativo è costituito dal fatto che, in valore assoluto, nel primo semestre 2026 gli incidenti di questa tipologia costituiscono più del 90% degli eventi registrati in tutto il 2025.

[3] L'Operational Summary dell'Agenzia per Cybersicurezza Nazionale indica il settore ai primi posti, mentre l'ENISA Threat Landscape 2026 conferma sul territorio europeo una generalizzata riduzione degli incidenti verso il settore sanitario, se si escludono i dati provenienti dalle segnalazioni obbligatorie NIS2 che – lo ricordiamo – non afferiscono necessariamente ad incidenti con impatti corrispondenti alla scala di Severity elevata usata per il nostro Rapporto.

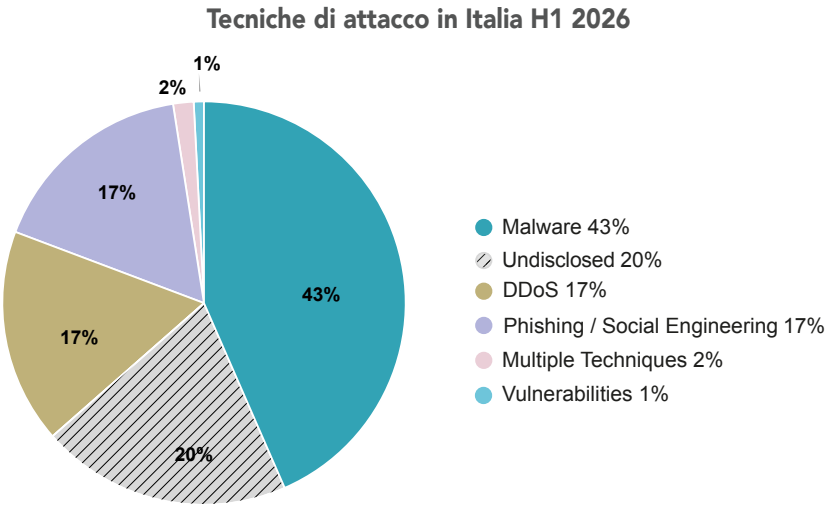


Fig. 7 - Tecniche di attacco in Italia I sem. 2026

Il DDoS scende dal 38,5% al 17%, praticamente dimezzandosi: questo dato è coerente con la diminuzione del fenomeno dell'Hacktivism e degli incidenti subiti dalla Pubblica Amministrazione, che è la vittima preferita per gli attacchi dimostrativi, e trova riscontro anche sui dati raccolti dal CSIRT Nazionale (che sul proprio campione di segnalazioni identifica una flessione anche più ampia). Delle ragioni di questo calo ne abbiamo ragionato nel paragrafo precedente.

Al secondo posto, a pari merito, sale il phishing (17%) confermandosi come una tecnica di successo dal punto di vista degli attaccanti, che sfruttano una volta di più il "fattore umano". Non si tratta solo di guadagnare posizioni: nel solo primo semestre 2026 si sono verificati i 2/3 degli incidenti di tutto il 2025, che fa temere per una crescita ancor più significativa sul resto dell'anno. Tale dato per il nostro paese riflette un quadro coerente con quello europeo[4], dove lo sfruttamento del fattore umano è causa principale di penetrazione e di innesco anche delle altre tecniche classificate in questo Rapporto.

Completano il campione gli incidenti basati su Multiple Techniques, la cui incidenza resta pressoché invariata rispetto al 2025, e gli incidenti basati su vulnerabilità –

[4] Enisa Threat Report 2026: https://www.enisa.europa.eu/sites/default/files/2026-09/ENISA%20Threat%20Landscape%202026_Final.pdf

spesso note – che si fermano all'1% con un drastico abbassamento rispetto all'anno precedente.
Gli eventi *Undisclosed* (ovvero quelli per i quali le tecniche utilizzate non sono di pubblico dominio) raggiungono il 20% del totale del campione.

Guardando al trend degli ultimi anni (**Fig.8**), balza all'occhio la curva di progressione degli attacchi di Phishing/Social Engineering, che al contrario di quanto accade per le altre tecniche di attacco, risulta lineare e sempre crescente, priva di picchi o crolli.

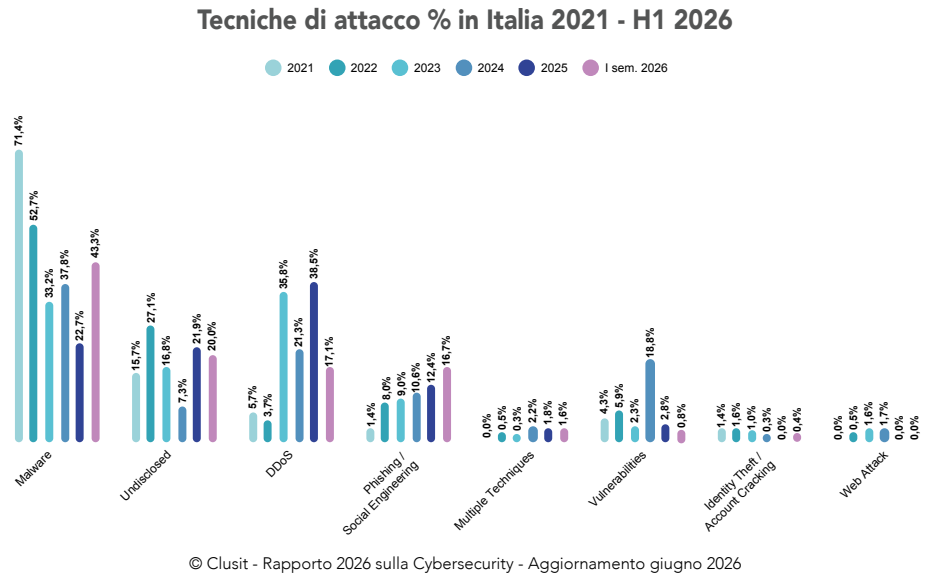


Fig. 8 - Tecniche di attacco % in Italia nel periodo 2021 - I sem. 2026

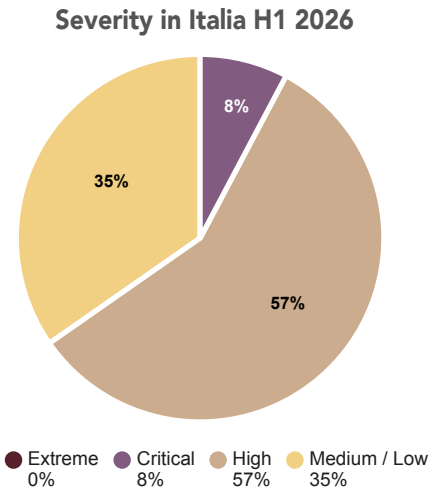
Questa è la chiara manifestazione di un fenomeno strutturale, in cui agiscono in modo complementare e armonico i due fattori che sono prevalenti dietro ad ogni incidente informatico: la pressione degli attaccanti (minaccia) e la capacità di difesa delle vittime (vulnerabilità). In questo ambito specifico, dove l'incidenza degli strumenti di prevenzione è comunque limitata dall'azione umana che resta al centro tanto della capacità di difendersi che dell'azione malevola, è evidente come ancora oggi l'aumento della pressione degli attacchi non sia controbilanciato da un'equivalente azione rivolta alle persone per renderle maggiormente consapevoli dei rischi connessi con l'uso degli strumenti informatici. Ciò non vuol dire che gli sforzi in questa direzione non siano cresciuti: se così non fosse, probabilmente questa categoria

sarebbe oggi a livelli nettamente superiori a tutte le altre. D'altro canto, guardando alle organizzazioni, è bene ricordare che basta anche una bassissima percentuale di persone ("una persona", in realtà) non adeguatamente formate o sensibilizzate, per rendere possibile un incidente anche di grave portata.

L'andamento storico delle altre tecniche dipende in generale da due aspetti diversi: da un lato, sicuramente, incidono le variazioni di pressione della minaccia, come già discusso ad esempio per quanto riguarda il fenomeno dell'Hacktivism a livello mondiale e riguardo al settore Pubblico. Dall'altro, guardando alle tecniche di attacco prevalenti, come Malware e DDoS negli ultimi anni, l'incidenza percentuale è condizionata anche dal dimensionamento complessivo del campione, che negli ultimi anni per il nostro paese ha subito cambiamenti piuttosto repentini, con percentuali di crescita a due digit.

Analisi della "Severity" degli incidenti

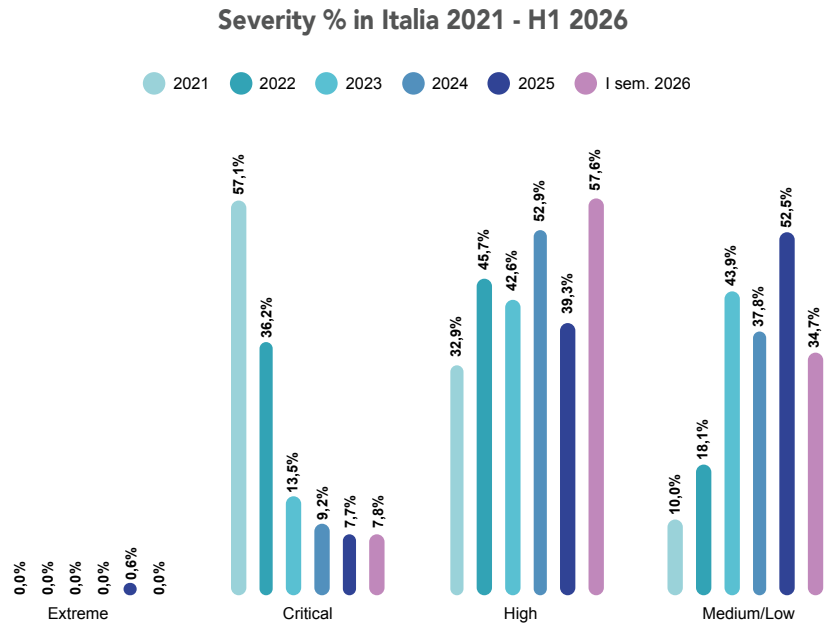
Dal punto di vista della *Severity*, il dato italiano (**Fig.9**) è lievemente peggiorativo rispetto alle altre dimensioni precedentemente analizzate, benché in modo coerente con le variazioni registrate sulle tecniche di attacco e sulla tipologia di attaccanti.



© Clusit - Rapporto 2026 sulla Cybersecurity - Aggiornamento giugno 2026

Fig. 9 - Severity degli incidenti in Italia I sem. 2026

Se infatti la quota di *severity* Critical mantiene una soglia molto bassa di incidenti (8% del campione) gli incidenti con impatto High salgono (**Fig.10**) quasi di 20 punti percentuali raggiungendo quota 57% del totale, riducendo conseguentemente la componente di eventi con impatto Medium/Low, al 35% (-18 p.p.). Come detto precedentemente, questo quadro è coerente con i cambiamenti descritti nei paragrafi precedenti per il nostro paese: si riducono gli incidenti dimostrativi, tipicamente a basso impatto, mentre risale la quota di incidenti di matrice cybercriminale, che nel perseguire i propri obiettivi determina mediamente conseguenze più significative per le vittime.
La buona notizia è che il nostro paese mantiene una componente di incidenti con impatto medio o basso quasi tre volte superiore rispetto al dato globale 2025. Se questa tendenza si manterrà stabile, potrà essere spiegata con una crescente capacità, da parte delle organizzazioni del nostro paese, di attuare misure procedurali, tecniche e organizzative di tipo reattivo, atte a contenere e ridurre, per quanto possibile, le conseguenze dei singoli incidenti.



© Clusit - Rapporto 2026 sulla Cybersecurity - Aggiornamento giugno 2026

Fig. 10 - Severity degli incidenti in Italia nel periodo 2021 - I sem. 2026

D'altro canto, il grafico in Fig.10 impone una certa prudenza: l'unico fenomeno confermato e ormai stabile dal 2024 resta la bassa incidenza degli eventi a impatto critico, mentre gli incidenti con conseguenze High o Medium/Low continuano ad alternarsi anno su anno con variazioni dell'ordine dei 20 punti percentuali.

Appendice metodologica

Le decisioni in ambito cybersecurity sono basate principalmente su analisi dei rischi, legate anche a valutazioni di scenario. Che si tratti di attivare o non attivare un servizio, implementare o non implementare un controllo, accettare o non accettare un rischio, a fine giornata il manager dovrà aver preso una decisione, e lo farà con i dati che ha a disposizione. Non decidere è comunque una decisione, di solito la peggiore, e un lusso che il manager non si può permettere. Quello che possiamo fare, come Clusit, è fornirgli i migliori dati che possiamo raccogliere, insieme agli strumenti per valutarne la qualità ed i limiti. Negli ultimi anni, il gruppo di lavoro sta adeguando la metodologia all'evoluzione del contesto, per tenere conto di nuove tecniche, diversi impatti e fattori che nel tempo variano di rilevanza, pur cercando di mantenere la confrontabilità dei dati anno su anno.

L'analisi dei principali incidenti cyber noti a livello globale si scontra necessariamente con la disponibilità di un campione parziale e non necessariamente rappresentativo dello scenario complessivo di rischio di attacco, che deve comunque essere valutato nel contesto specifico in cui opera una singola organizzazione. Per valutare il valore dei dati raccolti e delle analisi effettuate, è necessario chiedersi prima di tutto quali siano le modalità di raccolta e di analisi, e quali quindi i limiti dei risultati ottenuti.

I dati riportati si riferiscono ad incidenti riportati in fonti di informazione pubbliche. Da quando, nel 2011, è iniziata questa attività, il numero di fonti utilizzato è molto aumentato, e le modalità di ripulitura dei dati, ad esempio dalle duplicazioni, sono migliorate. L'utilizzo di fonti pubbliche introduce comunque un *bias* rispetto alla totalità degli incidenti occorsi e, quindi, all'esposizione ai rischi. In questa sezione cerchiamo di dare una maggiore visibilità a questi possibili bias, in modo che se ne possa tenere conto. Per contro, quando un incidente arriva ad essere pubblicato sulle fonti analizzate, di solito le caratteristiche descritte risultano essere abbastanza affidabili. Quando non lo sono, normalmente le parti interessate tendono a pubblicare o chiedere la pubblicazione di informazioni corrette.

Gli incidenti analizzati rappresentano certamente un campione significativo di quelli resi pubblici dalle fonti principali. Fra quelli resi pubblici, rimangono quindi esclusi incidenti riportati ad esempio da testate minori, locali o di Paesi del mondo poco co-

perti dall'analisi. Nel corso degli anni, è aumentata l'attenzione alla copertura più ampia delle fonti italiane anche minori. In questo senso, possiamo avere quindi un bias verso la rappresentatività dei paesi occidentali maggiormente presenti (ad esempio, gli Stati Uniti) e verso l'Italia. Questo aspetto, se correttamente gestito, può essere più di aiuto che di svantaggio per i manager italiani.

Fra gli incidenti noti pubblicamente, rimangono esclusi quelli che non hanno avuto una rilevanza tale da essere inclusi nelle fonti analizzate. Si tratta per lo più di incidenti di lieve entità, o che interessano aziende di minori dimensioni e che non hanno particolarità tali da renderli di interesse per le fonti principali. Possono essere, ad esempio, attacchi malware di minore entità che, per chi deve gestire la sicurezza di un'organizzazione, probabilmente aggiungono poco rispetto alla valutazione della necessità di adottare una baseline di misure di sicurezza che è ormai da considerare indispensabile. Anche fra quelli riportati nelle fonti analizzate, possono essere esclusi incidenti che sono di impatto particolarmente basso, e che sono arrivati ad essere pubblicati magari per fattori fortuiti.

Ci sono poi incidenti che, pur essendo divenuti noti in contesti circoscritti, non hanno raggiunto le fonti pubbliche. Anche dove vi siano obblighi di notifica, infatti, questo non vuole dire che tutti gli incidenti siano notificati (dipende da caratteristiche dell'incidente e dalla normativa locale e di settore); soprattutto, le autorità in generale non rendono pubblici gli incidenti notificati. Lo stesso per vale per le denunce alle autorità di polizia, alle assicurazioni, e per i dati raccolti dai fornitori di connettività e di servizi di gestione incidenti. Si tratta di dati interessanti, ma in generale disponibili solo a questi soggetti, e quindi molto frammentati. Alcuni li pubblicano a loro volta sotto forma di statistiche. Il Clusit collabora con le autorità ed organizzazioni interessate a pubblicare questi dati all'interno del Rapporto, ma i dati rappresentano comunque viste diverse e più verticali su specifici ambiti, e quindi non sono integrati in questa analisi, ma pubblicati in altre parti del Rapporto, dando loro anche la giusta e specifica visibilità.

Nel campione di questa analisi sono certamente meglio rappresentati gli incidenti realizzati per finalità cyber criminali o di hacktivism, che quindi spesso si manifestano con danni e disservizi evidenti, rispetto a quelli derivanti da attività di cyber espionage, che tendono ad essere condotti con grande cautela e poco rumore, e pertanto emergono più difficilmente. Questo può essere un limite importante da considerare: gli attacchi che colpiscono la riservatezza dei dati sono sicuramente sotto rappresentati perché, a meno che gli attaccanti per qualche motivo pubblichino l'informazione, le stesse organizzazioni colpite potrebbero non averne evidenza. Si tratta di *known unknown* rispetto ai quali è difficile avere dati statisticamente significativi.

Anche venendone a conoscenza, le organizzazioni colpite potrebbero avere interesse a non darne evidenza a nessuno. Un tema analogo è legato alle attività di information warfare, che possono essere condotte con altrettanta cautela, anche per non esporre gli strumenti utilizzati[5].

In questi casi, una delle parti potrebbe avere interesse a dare evidenza dell'attacco per motivi di propaganda, ma può essere difficile validare la veridicità di quanto affermato. Dove non vi siano sufficienti conferme sulle caratteristiche dell'attacco, o addirittura sul fatto stesso che l'attacco sia avvenuto, l'attacco non viene incluso nell'analisi.

Nel complesso, quindi, possiamo considerare i dati di questa analisi rappresentativi della maggior parte degli attacchi di grandi dimensioni, con una sottostima difficile da quantificare in termini di attacchi banali o di lieve entità, e di attacchi, come quelli di cyber espionage, che possono facilmente non essere né rilevati né pubblicizzati.
In termini numerici, il campione analizzato è ormai piuttosto consistente, e si può quindi considerare rappresentativo di quanto reso pubblico. Le analisi fatte sul campione stesso danno quindi una rappresentazione chiara di quanto si sa, e possono essere utilizzate dai manager per avere quel quadro della situazione complessiva a livello globale che è sempre più necessario per definire le strategie di un'organizzazione in tema di cyber security.

Un'ultima nota riguarda le variazioni anno su anno. Quelli che analizziamo non sono fenomeni fisici, che hanno una certa regolarità e sui quali variazioni percentuali anche piccole possono, in alcuni casi, essere indicative di tendenze importanti. Qui parliamo di fenomeni influenzati da un numero enorme di parametri. Il fatto stesso che, in talune situazioni, da anno ad anno le variazioni percentuali relative siano tutto sommato limitate per la maggior parte dei valori, seppure in un contesto di generale aumento, depone a favore della qualità complessiva dei risultati, e dà anzi maggior valore alle variazioni più evidenti ed ampie. È quindi utile focalizzarsi su queste ultime e sull'andamento complessivo, piuttosto che su piccole fluttuazioni annuali. Per questo, nella nostra metodologia abbiamo aumentato l'attenzione ai fenomeni più significativi, riducendo la disamina di singole variazioni meno rilevanti.

[5] Salvo quando vengano esposti per errore, come nel caso di Stuxnet.

Attività e segnalazioni della Polizia Postale e per la Sicurezza Cibernetica nel 1° semestre del 2026

Innovazione tecnologica, valore umano e presidio territoriale a tutela dell'ecosistema digitale

La dimensione digitale costituisce una componente sempre più integrata della nostra quotidianità e uno degli spazi principali della vita sociale, economica e istituzionale del Paese. Le relazioni, i servizi e le attività che quotidianamente attraversano la rete si intrecciano strettamente con la realtà fisica, in un ambiente in continua evoluzione, in cui le interazioni fisiche e cibernetiche si integrano in modo naturale. In questo contesto, Il Servizio Polizia Postale e per la Sicurezza Cibernetica, insieme alle sue articolazioni territoriali, è chiamato ad assicurare una presenza costante, autorevole e rassicurante, capace di coniugare l'analisi attenta dei fenomeni con un approccio organizzativo flessibile e di adattarsi rapidamente ai mutamenti tecnologici e alle nuove forme di minaccia.

L'accelerazione dell'innovazione digitale, e in particolare la diffusione dell'Intelligenza Artificiale Generativa, offre prospettive di sviluppo straordinarie ma impone anche una costante capacità di aggiornamento. Le medesime tecnologie che favoriscono crescita, efficienza e progresso possono infatti essere sfruttate in ambiti illeciti, ad esempio per rendere più sofisticate attività fraudolente, campagne di disinformazione o tentativi di ingegneria sociale. Per affrontare efficacemente tali sfide e preservare il giusto equilibrio in questo continuo cambiamento, la Specialità sta integrando progressivamente strumenti avanzati di analisi e supporto investigativo nei propri processi operativi e di *digital forensics*. L'intento è di supportare l'attività degli operatori valorizzando le nuove tecnologie, senza mai prescindere dal controllo umano e dal rigoroso rispetto dei principi etici e normativi definiti a livello europeo.

L'efficacia di questa evoluzione tecnologica dipende inevitabilmente dal valore delle persone che la governano. In questa prospettiva, un passaggio strutturale e vitale per la Specialità si è concretizzato l'11 giugno scorso presso il Centro di Addestramento di Cesena, con il giuramento dei 195 allievi del 9° corso di formazione per Vice Ispettori Tecnici della Polizia di Stato, settore di impiego sicurezza cibernetica. Queste figure professionali, formate per coniugare la solida impostazione investigativa della polizia giudiziaria con competenze tecnico-ingegneristiche e informatiche mirate, hanno rafforzato con nuove competenze le Divisioni del Servizio Polizia Postale, i 18 Centri Operativi per la Sicurezza Cibernetica e le 82 Sezioni Operative per la Sicurezza Cibernetica distribuite sul territorio nazionale. Un apporto di elevato profilo

tecnico, che rimanda al senso profondo del nostro servizio, sintetizzato dal Capo della Polizia, Direttore Generale della Pubblica Sicurezza, Prefetto Vittorio Pisani, in occasione della stessa cerimonia: «Dietro un'identità digitale vi è sempre un essere umano».

Il consolidamento delle risorse umane si intreccia strettamente con i traguardi storici che definiscono l'identità profonda del Servizio Polizia Postale. Quest'anno, infatti, celebriamo i vent'anni di operatività di due presidi strategici per la transizione digitale del Paese: il Centro Nazionale per il Contrasto della Pedopornografia Online (C.N.C.P.O.) e il Commissariato di P.S. Online, strutture che nel tempo hanno saputo evolversi insieme alla rete e alle esigenze dei cittadini.

Nati nel 2006, questi due presidi continuano ad adeguare la propria azione ai profondi mutamenti della rete. Il C.N.C.P.O. rappresenta il punto di riferimento nazionale nel contrasto allo sfruttamento sessuale dei minori in rete, assicurando una tutela ininterrotta e orientando costantemente le proprie indagini per far fronte al passaggio dalle prime piattaforme di condivisione di materiale multimediale ai più complessi ambienti anonimizzati, proteggendo le fasce più vulnerabili della società. Parallelamente, il Commissariato di P.S. Online traduce ogni giorno il principio di prossimità nello spazio virtuale, agendo come punto di ascolto trasparente e offrendo informazione, orientamento preventivo e supporto ai cittadini. Quando necessario, coordina in tempo reale delicati interventi di soccorso sul territorio in situazioni di particolare fragilità emotiva o pericolo personale.

La capacità di far fronte a uno spettro così ampio di responsabilità — che spazia dalla tutela delle infrastrutture critiche alla protezione delle persone più fragili — poggia sull'attività continua dei Centri e delle Sezioni Operative sul territorio e sul lavoro armonico e complementare delle cinque Divisioni che compongono il Servizio Polizia Postale e per la Sicurezza Cibernetica. I contributi che seguono offrono una lettura delle rispettive aree di competenza operativa, restituendo il senso di un impegno corale e quotidiano. Pur operando in ambiti differenti, le cinque Divisioni concorrono in modo integrato al perseguimento di un obiettivo comune: garantire la sicurezza dell'ecosistema digitale e la tutela dei cittadini, delle istituzioni e delle infrastrutture strategiche del Paese, preservando quel rapporto di fiducia tra persone, tecnologia e istituzioni che rappresenta una condizione essenziale per lo sviluppo della società digitale.

La Prima Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica

Nel primo semestre dell'anno 2026 la Prima Divisione del Servizio, confermando il suo ruolo di governance strategica e di raccordo tra le divisioni operative e le articolazioni territoriali della Polizia Postale e per la Sicurezza Cibernetica, ha tracciato le linee di indirizzo, pianificazione e coordinamento dell'azione della Specialità. I settori nei quali è articolata concorrono con attività più prettamente amministrative alla sicurezza nello spazio digitale, attraverso la cura dei rapporti con le istituzioni, con gli organismi internazionali e gli enti pubblici e privati, massimizzando l'efficacia delle attività di cooperazione in materia *cyber*, sia a livello nazionale che internazionale, la gestione delle risorse umane attuali e la pianificazione delle esigenze future e la formazione specialistica e professionalizzante del personale. Assume particolare rilievo, inoltre, l'attività di prevenzione attuata attraverso le iniziative di sensibilizzazione rivolte ai cittadini per la diffusione della massima consapevolezza e sicurezza nella navigazione online, che si esplica anche mediante il Commissariato di P.S. online, sito ufficiale della Polizia Postale accessibile all'indirizzo www.commissariatodips.it.

Si tratta di un portale che offre un servizio continuo e accessibile a chiunque e che consente di segnalare reati riscontrati in rete, situazioni di disagio e di pericolo, dubbi e circostanze sospette relative a reati informatici. Allo stesso tempo, svolge un ruolo attivo nella prevenzione dei fenomeni criminali che nascono e si diffondono sul web: l'analisi delle segnalazioni ricevute consente di evidenziare le fenomenologie criminose attuali più frequenti per la pubblicazione di alert, approfondimenti e consigli di sicurezza ai fini della massima diffusione tra gli utenti del web, per evitare che altri internauti possano cadere nelle trappole insite nella rete.

Nel corso del primo semestre 2026 sono stati numerosi gli utenti che si sono rivolti alla Polizia Postale tramite la piattaforma, oltre 57.000 segnalazioni e quasi 14.000 richieste di informazioni pervenute, che hanno evidenziato contenuti riferibili principalmente a problematiche di *phishing*, relative all'utilizzo dei *social network* e ad attacchi *hacker*. La facilità di accesso e la popolarità del sito sono testimoniate da oltre 5 milioni di visite e più di 56 milioni di pagine consultate.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Il potenziamento delle capacità professionali delle risorse umane necessarie ad affrontare le sfide sempre nuove imposte dall'evoluzione tecnologica, in particolare di quelle connesse all'utilizzo dell'Intelligenza artificiale, si conferma uno degli elementi chiave del contrasto al *cybercrime*. Prosegue in tal senso l'impegno della Polizia Postale in formazione di alto livello specialistico, anche in collaborazione con il mondo accademico e con gli Istituti Tecnici Superiori, attraverso la stipula di protocolli d'intesa. Il corso per Vice Ispettori Tecnici nel settore di impiego della sicurezza cibernetica, in corso di svolgimento a Cesena da settembre 2025 e concluso nel giugno 2026, ha provveduto, altresì, a formare nuove risorse di elevata professionalità da immettere nei ruoli della Polizia di Stato, nelle quali saranno concentrate le prerogative investigative e tecniche necessarie per potersi agevolmente muovere all'interno dell'investigazione cibernetica.

In ambito internazionale, la Divisione è molto attiva: numerose delegazioni straniere, interessate alle metodiche dell'attività di contrasto e prevenzione poste in essere nella *cybersecurity* dalla Polizia italiana, sono state ospitate presso gli uffici del Servizio e dei Centri di eccellenza.

Nell'ambito dell'attività di prevenzione la Specialità, oltre al monitoraggio continuo della rete, è stata impegnata costantemente in campagne di sensibilizzazione e di educazione al corretto uso delle tecnologie, al fine di diffondere una cultura della sicurezza digitale e accrescere la resilienza dei cittadini, soprattutto quelli più fragili, nei confronti delle insidie del web.

Tra le iniziative più significative si menziona la campagna itinerante di educazione digitale "*Una vita da Social*", dedicata ai giovani studenti e affiancata negli ultimi tempi dalla versione "*boomer edition*", rivolta agli adulti presso i propri luoghi di lavoro. A bordo del *truck* che contraddistingue l'iniziativa e presso istituti - scolastici e non - su tutto il territorio nazionale, sono state incontrate dagli operatori della Specialità, nel corso del semestre, numerose scolaresche e cittadini, promuovendo, soprattutto tra i più giovani, un uso consapevole delle tecnologie e dei *social media*.

Altra iniziativa simbolo della Polizia Postale è *#cuoriconnessi*, realizzata in collaborazione con Unieuro e finalizzata a promuovere comportamenti responsabili nell'ambiente digitale, anche attraverso la narrazione di storie ed esperienze di giovani protagonisti, tratte dall'omonima collana editoriale e da contenuti tematici disponibili online. Il momento di maggiore visibilità della campagna coincide con il *Safer Internet Day*, la giornata internazionale per la sicurezza in rete. Il 10 febbraio 2026, in occasione del decimo anniversario, l'evento nazionale si è svolto presso l'Auditorium Parco della Musica Ennio Morricone di Roma, con la partecipazione di oltre 1.200 studenti in presenza e più di 230.000 collegati in diretta streaming.

A partire dal mese di febbraio 2026, l'attività di prevenzione si è ulteriormente arricchita con "*InsospettABILI – sviluppiamo abilità contro le frodi online*", iniziativa presentata a Sanremo e dedicata alla prevenzione delle frodi digitali. Il progetto propone un percorso interattivo ed esperienziale che, attraverso totem multimediali, una web-app dedicata, quiz e attività ludico-educative, coinvolge direttamente gli utenti nella simulazione di situazioni riconducibili alle principali tecniche utilizzate dai truffatori, favorendo lo sviluppo di abilità concrete per riconoscerle e prevenirle.

Il significativo interesse e l'ampia partecipazione di pubblico registrati in occasione dell'esordio a Sanremo hanno trovato ulteriore conferma nelle successive iniziative, tanto che il percorso è stato riproposto a Roma, dal 10 al 13 aprile 2026, presso la Galleria Alberto Sordi, nell'ambito delle celebrazioni per il 174° Anniversario della fondazione della Polizia di Stato. In tale occasione, il progetto è stato illustrato alla presenza del Presidente della Repubblica e del Capo della Polizia – Direttore Generale della Pubblica Sicurezza, ricevendo particolare attenzione per l'innovativo approccio adottato nella prevenzione delle frodi.

Nell'ambito delle attività di educazione digitale, sensibilizzazione e prevenzione dei rischi e delle insidie del cyberspazio, la Polizia Postale partecipa al progetto *"Cinema e Diritto"*, realizzato in collaborazione con l'Università degli Studi di Salerno e Giffoni, con l'obiettivo di avvicinare le giovani generazioni ai temi della legalità e dell'uso consapevole delle tecnologie digitali attraverso il linguaggio cinematografico.

Nel marzo 2026 il progetto ha confermato la propria dimensione internazionale con una tappa a Tirana, in Albania, nel corso della quale è stato proiettato il cortometraggio *"(IM)PERFETTA"*, realizzato nell'ambito della collaborazione della Polizia di Stato con Rai Cinema e *One More Pictures*. Il corto ha offerto lo spunto per un momento di confronto con i giovani sui temi del rapporto tra vita reale e dimensione virtuale, dell'accettazione di sé e del proprio corpo e dei rischi connessi all'esposizione sui social, rafforzando il messaggio di prevenzione e consapevolezza digitale portato dalla Polizia di Stato anche oltre i confini nazionali.

Complessivamente, le attività del Servizio Polizia Postale al 30 giugno 2026 hanno coinvolto 2.363 scuole, 282.708 studenti, 20.957 docenti e 9.525 genitori, oltre a ulteriori 31.513 partecipanti tra studenti, insegnanti e famiglie nei numerosi seminari e convegni dedicati alla cultura della sicurezza online.

La Seconda Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica

La protezione della persona negli ambienti digitali è l'obiettivo primario nell'ambito delle competenze della Seconda Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica, chiamata a intervenire nei contesti in cui le tecnologie possono diventare strumenti di abuso e sfruttamento delle vulnerabilità individuali di giovani vittime.

L'attività della Divisione si estende in un ampio raggio di azione che va dal monitoraggio costante della rete, nell'ambito dell'attività di prevenzione, al contrasto delle condotte criminali con particolare attenzione alla produzione e alla circolazione di materiale pedopornografico, nell'ambito delle attività investigative, nonché al riconoscimento e allo studio delle dinamiche attraverso cui si manifestano comportamenti abusanti e predatori.

Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.)

L'esperienza quotidiana dei più giovani si svolge sempre più all'interno di ecosistemi digitali nei quali social network, applicazioni di messaggistica e altri canali di comunicazione assumono un ruolo centrale nella costruzione dei rapporti personali. Questi strumenti ampliano le possibilità di apprendimento e socializzazione, ma espongono bambini e adolescenti a situazioni che possono comprometterne i diritti e la sicurezza. Per la Polizia di Stato, la salvaguardia dei minori costituisce pertanto un impegno prioritario, da attuare attraverso l'analisi dei nuovi fattori di rischio, l'adozione di soluzioni tecnologiche avanzate e il continuo adeguamento delle modalità di intervento alle trasformazioni della comunicazione.

La risposta istituzionale ai reati di sfruttamento sessuale dei minori commessi attraverso internet fa capo al Servizio Polizia Postale, struttura del Ministero dell'Interno cui la disciplina istitutiva del Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) attribuisce competenze esclusive in materia[1]. Il Centro esercita le funzioni di prevenzione e repressione dello sfruttamento sessuale dei minori in rete e raccoglie le segnalazioni provenienti da autorità italiane ed estere, soggetti pubblici e privati[2].

Tra le minacce presenti negli spazi virtuali figurano le condotte di adulti che avvicinano i minori con finalità di adescamento (*grooming*) o li persuadono a realizzare e condividere contenuti intimi. Tali dinamiche possono coinvolgere le vittime a forme di sfruttamento e abuso, alla diffusione non consensuale di immagini sessualmente esplicite (*revenge porn*) e al ricatto a sfondo sessuale (*sextortion*). L'ambito di azione comprende anche il contrasto al bullismo e alla sua dimensione digitale; le interazioni tra coetanei possono assumere carattere lesivo: umiliazioni, vessazioni e comportamenti molesti trovano spazio, tra l'altro, negli ambienti di gioco in rete, dando luogo a episodi di cyberbullismo. Completano questo scenario i rischi per la riservatezza dei dati personali e le frodi, incluse quelle basate sulla simulazione di un legame affettivo (*romance scam*), nonché l'attenzione verso comportamenti emergenti tra i ragazzi, come le *challenge*: prove veicolate dai social che possono comportare conseguenze pericolose per chi vi prende parte.

---

[1] La Legge 6 febbraio 2006 n. 38, all'art.14 bis istituisce il (C.N.C.P.O), con compiti di raccolta delle segnalazioni riguardanti la diffusione di materiale concernente l'utilizzo sessuale dei minori, provenienti da organi di polizia anche stranieri e da soggetti pubblici e privati impegnati nella lotta alla pornografia minorile.

[2] Il quadro delle attribuzioni della Specialità è stato ampliato dal decreto del Ministro dell'Interno del 15 agosto 2017, mentre le leggi n. 71/2017 e n. 70/2024 hanno rafforzato il sistema di tutela rispetto al bullismo e al cyberbullismo.

Un'ulteriore area di attenzione riguarda le comunità online che possono offrire ai ragazzi occasioni di ascolto e sostegno reciproco, ma anche diventare luoghi in cui si condividono vissuti di disagio psicologico, condotte autolesive e problematiche legate ai disturbi alimentari. La facile accessibilità ai contenuti e l'assenza di ostacoli efficaci all'accesso, può favorire un'esplorazione precoce della sessualità e l'ingresso in gruppi chiusi dove circolano immagini di ogni genere, incluse rappresentazioni di violenza estrema, note come materiale "gore".

Tra i rischi più allarmanti del contesto digitale emerge il coinvolgimento dei minori in gruppi che celebrano la violenza e incoraggiano comportamenti emulativi. L'adesione a queste comunità può alimentare percorsi di radicalizzazione, nei quali il desiderio di riconoscimento e appartenenza si intreccia con fantasie di vendetta, fino a favorire propositi di aggressione contro la scuola, gli insegnanti e i compagni.

Il C.N.C.P.O., pertanto, con l'attività investigativa espletata con operatori specializzati e il coordinamento operativo delle indagini sul territorio nazionale attraverso i 18 Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) e le 82 Sezioni Operative (S.O.S.C.), assicura il raccordo informativo e il supporto alle attività territoriali. La natura transfrontaliera dei reati di sfruttamento sessuale dei minori online richiede una cooperazione costante tra le autorità investigative dei diversi Paesi, affinché gli elementi raccolti nei singoli contesti nazionali possano concorrere alla ricostruzione degli abusi e all'individuazione dei responsabili. In questo quadro, il C.N.C.P.O., quale organo centrale, cura i rapporti a livello internazionale con le forze di polizia estere, mediante la condivisione delle informazioni con Europol e Interpol e coordina le attività degli Uffici della Specialità nell'ambito delle indagini di rilievo internazionale. Lo scambio informativo permette di mettere in relazione le evidenze acquisite all'estero con quelle emerse sul territorio italiano, assicurando continuità e coerenza all'azione investigativa.

L'Unità di Analisi del Crimine Informatico (UACI) è una struttura specialistica della Polizia Postale e per la Sicurezza Cibernetica. Il suo compito principale è quello di affiancare l'azione investigativa tecnologica del C.N.C.P.O., unendo le competenze delle scienze sociali e della psicologia per la tutela dei minori online da ogni forma di aggressione tecnomediata.

La collaborazione tra istituzioni rappresenta un ulteriore elemento di questo sistema. Il confronto interistituzionale si sviluppa mediante la partecipazione al Safer Internet Center Italy, in collaborazione con il Ministero dell'Istruzione e del Merito, all'Osservatorio Nazionale per l'Infanzia e l'Adolescenza, all'Osservatorio per la Prevenzione e il Contrasto della Pedofilia e della Pornografia Minorile, promosso dal Dipartimento

per le Politiche della famiglia della Presidenza del Consiglio dei ministri e al Tavolo Tecnico per la prevenzione e il contrasto del bullismo e cyberbullismo ai sensi della L.71/2017 come modificata dalla L.n.70/2024.

Il C.N.C.P.O partecipa inoltre al Gruppo di Lavoro sulle Sfide e Opportunità del Gaming, istituito dal Dipartimento per la Trasformazione Digitale e al Group Network for the Prevention of Child Sexual abuse- della Commissione Europea.

Queste sedi istituzionali consentono di mettere a confronto competenze diverse, necessarie per interpretare fenomeni complessi e sviluppare risposte condivise multilivello. La collaborazione sui temi della prevenzione e il contrasto dell'abuso e dello sfruttamento sessuale dei minori con la partecipazione del C.N.C.P.O ha consentito la redazione dell'attuale Piano Nazionale per gli anni 2025- 2027.

La tutela dei soggetti più vulnerabili passa anche attraverso il coinvolgimento delle realtà impegnate nella protezione dell'infanzia. In questa prospettiva, il C.N.C.P.O. ha potenziato le collaborazioni con le organizzazioni impegnate nella protezione dei minori, attraverso protocolli e forme di partenariato pubblico-privato. Tra queste figurano Telefono Azzurro, Save the Children, Terre des Hommes, Operation Underground Railroad Rescue, National Center for Missing & Exploited Children, Child Rescue Coalition (C.R.C.) e l'Associazione Meter.

Sul piano europeo, il Centro ha partecipato, per conto del Ministero dell'Interno, ai lavori sulla proposta di regolamento per la prevenzione e il contrasto dell'abuso sessuale sui minori. I contributi tecnici, basati sull'esperienza investigativa, hanno riguardato anche le misure di rilevazione dei contenuti illeciti da parte dei fornitori di servizi, nella ricerca di un equilibrio tra protezione dei minori, riservatezza delle comunicazioni ed esigenze operative di contrasto.

L'impegno internazionale ha compreso inoltre i lavori del G7 nell'ambito dell'*High Tech Crimes Sub-Group* e del *Law Enforcement Practitioners*, oltre alla partecipazione alla *Victim Identification Task Force*, dedicata all'identificazione di vittime e autori, e alla *High Value Targets Task Force*, rivolta all'individuazione dei soggetti attivi nelle comunità pedofile del *dark web*. Il confronto sulle tecniche sotto copertura e sulle prassi investigative si è sviluppato anche attraverso il *Global Covert Internet Investigations Meeting*.

Significativo è l'impegno profuso dell'articolazione per l'attualizzazione delle metodologie investigative con corsi specialistici dedicati agli operatori di settore e la ricerca di innovative tecnologie idonee a velocizzare i processi del lavoro in particolare degli operatori impegnati della categorizzazione del materiale di pedopornografia.

È stata avviata all'inizio del 2026 la **progettualità, denominata CYPHER**, nell'ambito del programma Nazionale ISF 2021-2027, per la realizzazione di una infrastruttura tecnologica collocata su più nodi sul territorio Nazionale con l'uso di software specialistico per velocizzare ed automatizzare il lavoro degli operatori di visualizzazione e categorizzazione del materiale di pedopornografia con formazione ed aggiornamento del personale. Le numerose segnalazioni ricevute quotidianamente attraverso diversi canali costituiscono una base informativa essenziale per l'avvio e lo sviluppo delle indagini. La valutazione degli elementi raccolti e i successivi approfondimenti investigativi nel primo trimestre del 2026 hanno consentito di individuare i soggetti coinvolti confermando il ruolo centrale dell'analisi delle segnalazioni nel tradurre le informazioni disponibili in interventi concreti di contrasto allo sfruttamento sessuale dei minori online.

L'evoluzione delle modalità con cui si realizza lo sfruttamento sessuale dei minori in rete impone un costante adeguamento della risposta investigativa. In questo scenario, il Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) svolge un ruolo centrale nella tutela delle vittime e nell'individuazione delle condotte illecite, affiancando all'attività di indagine un impegno continuo sul versante della prevenzione. Social network, servizi di messaggistica e circuiti meno accessibili, come le darknet, presentano infatti modalità di contatto e diffusione dei contenuti che richiedono competenze specialistiche e una costante collaborazione internazionale.

La strategia investigativa ha privilegiato le situazioni di maggiore gravità, concentrando le risorse sui soggetti coinvolti in condotte reiterate, organizzate o particolarmente lesive. La valutazione preliminare delle segnalazioni ha permesso di definire le priorità di intervento e di indirizzare gli approfondimenti verso i principali punti di connessione delle reti criminali. Particolare impegno è stato dedicato all'identificazione degli autori che operano dietro identità anonime e utilizzano sistemi cifrati o altri strumenti di occultamento.

In questo contesto si collocano le operazioni sotto copertura condotte nel *Deep Web* e nel *Dark Web*, avvalendosi delle possibilità offerte dalla normativa. Il C.N.C.P.O. ha assicurato agli uffici territoriali assistenza tecnica e investigativa, mantenendo il raccordo con le agenzie estere per la condivisione delle informazioni, il confronto sulle prassi operative e la conduzione delle attività internazionali.

Alla ricerca degli autori si affianca l'impegno prioritario per l'identificazione delle vittime. Un'unità dedicata esamina e gestisce i file multimediali secondo gli standard internazionali, utilizzando la banca dati I.C.S.E. (*International Child Sexual Exploitation Database*) di Interpol. Il confronto con il materiale e le informazioni inseriti dalle

forze di polizia dei diversi Paesi permette di ricercare collegamenti tra le indagini ed elementi utili al riconoscimento dei minori. Ulteriori approfondimenti riguardano la componente finanziaria del fenomeno, sulla base delle informazioni trasmesse dall'Unità di Informazione Finanziaria della Banca d'Italia su operazioni sospette potenzialmente riconducibili al commercio online di materiale pedopornografico.

CNCPO	Primo Semestre 2025	Primo Semestre 2026
Casi trattati	1.383	1.508
Persone arrestate	148	95
Persone denunciate	648	400
Perquisizioni	604	458
Siti in Black List	2.821	2.907
Siti visionati	7.826	5.201

© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Il confronto tra il primo semestre del 2025 e il 2026 restituisce un quadro di crescente impegno operativo: i casi trattati sono passati da 1.383 a 1.508 (+9%). L'incremento documenta il maggior numero di situazioni affrontate e, pur non consentendo da solo di misurare l'effettiva diffusione del fenomeno, conferma la rilevanza dell'azione di contrasto. Di questi 1.508 casi, 937 hanno avuto origine da segnalazioni pervenute attraverso il circuito del National Center for Missing & Exploited Children (N.C.M.E.C.), che costituisce una fonte rilevante per l'avvio degli accertamenti. L'attività ha interessato sia la detenzione, la commercializzazione e la diffusione di materiale di abuso sessuale su minori, insieme alle condotte di istigazione alla pedofilia, sia l'adescamento e le fattispecie correlate. Pur potendo emergere nelle medesime indagini, questi ambiti richiedono percorsi di analisi e modalità di accertamento differenti.

I risultati operativi comprendono 95 arresti e 400 denunce in stato di libertà, per un totale di 495 soggetti individuati. A sostegno della raccolta della prova sono state eseguite 458 perquisizioni locali e informatiche, con il coinvolgimento dei 18 Centri

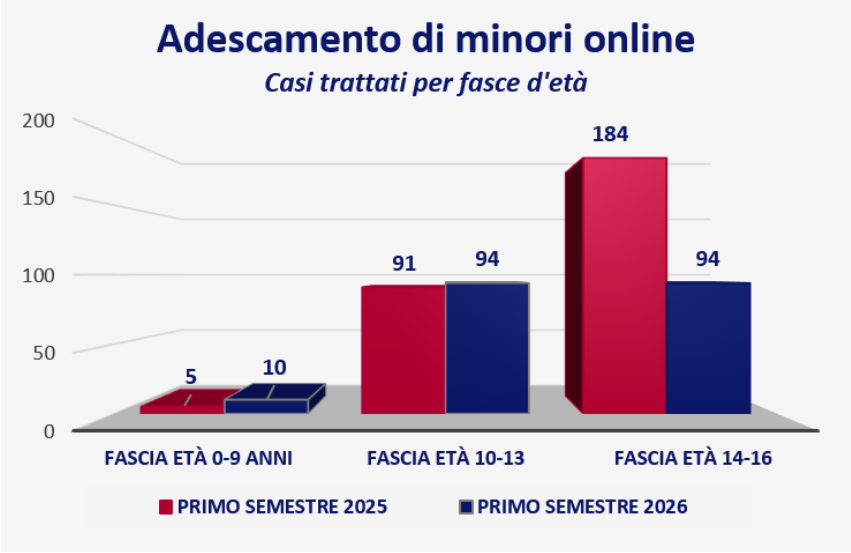
Operativi per la Sicurezza Cibernetica e delle 82 Sezioni Operative. Questi interventi hanno consentito di acquisire elementi utili ai procedimenti giudiziari e di intervenire sulla disponibilità e sulla circolazione dei contenuti illeciti, con l'obiettivo di interrompere le condotte di abuso e proteggere i minori coinvolti.

Sul versante della prevenzione, il C.N.C.P.O. svolge un'attività sistematica di osservazione degli ambienti digitali, alla quale si affianca la gestione della Black List. I siti, segnalati per la presenza di materiale di abuso sessuale su minori (*Child Sexual Abuse Material*, C.S.A.M.), agli Internet Service Provider affinché ne inibiscano l'accesso ha portato all'inserimento di 2.907 siti nell'elenco destinato al blocco dell'accesso, contribuendo a ostacolare la diffusione dei contenuti. L'impiego di tecnologie avanzate e la collaborazione con le autorità estere sostengono questo lavoro di analisi, che permette di individuare nuove minacce e circuiti di distribuzione dei materiali illeciti. La sorveglianza della rete integra così l'attività investigativa, contribuendo a limitare la circolazione dei contenuti di abuso e a rafforzare la protezione dei minori.

Adescamento online

L'adescamento online si sviluppa negli spazi digitali frequentati, in età sempre più precoce, da bambini e adolescenti: social network, applicazioni di messaggistica e ambienti di gioco online. In questi contesti, gli adulti con finalità di abuso adattano il proprio linguaggio e le modalità di interazione alle abitudini dei più giovani, costruendo rapporti di fiducia attraverso forme di manipolazione affettiva. Il legame così instaurato può essere utilizzato per indurre i minori a produrre e condividere immagini o video sessuali, fino a ottenere incontri di persona.

La gradualità di queste dinamiche e la difficoltà di riconoscerne tempestivamente la finalità abusante rendono il fenomeno particolarmente insidioso. Il contrasto all'adescamento costituisce pertanto una priorità per il C.N.C.P.O., che affianca alla prevenzione interventi investigativi specializzati, orientati a individuare i segnali di pericolo, interrompere le condotte e proteggere i minori coinvolti.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

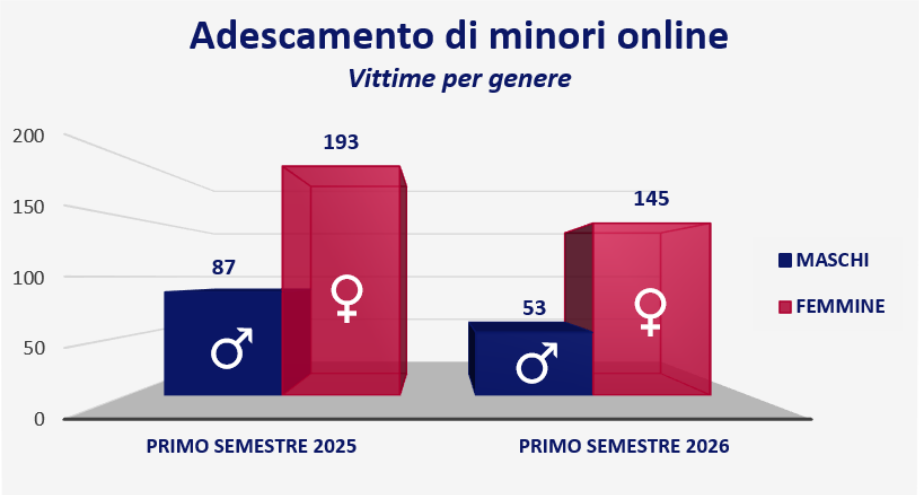
Un'analisi approfondita dei dati mostra come il rischio non sia distribuito in modo uniforme tra le diverse fasce d'età e in base al genere delle giovani vittime. Se è vero che i bambini tra 0 e 9 anni rappresentano ancora una quota relativamente minore di vittime, con 5 casi nel primo semestre 2025 rispetto ai 10 casi del primo semestre 2026, è altrettanto vero che si tratta di una tipologia di vittime particolarmente fragili per le quali un approccio sessuale precoce e tecnomediato può costituirsi come trauma concreto con potenzialità dannose piuttosto elevate.

Spesso è nei luoghi virtuali del gioco che gli adescatori "avvicinano" le loro vittime, sfruttando l'entusiasmo di vincere una partita nel gioco online preferito, nascondendosi dietro profili falsi di sedicenti coetanei.

La fascia d'età 10-13 anni registra 91 casi nel primo semestre 2025 e 94 casi nel primo semestre 2026. In questa fase dello sviluppo i minori iniziano a esplorare il mondo digitale in maniera più autonoma utilizzando i social media e le chat per stringere nuove amicizie. Gli adescatori sfruttano questa apertura per avvicinarsi alle vittime, fingendo di condividere interessi comuni e instaurando un rapporto basato su fiducia e manipolazione. È in questo contesto che la Polizia Postale ha rafforzato le proprie strategie di prevenzione, promuovendo campagne di sensibilizzazione rivolte sia ai

ragazzi che ai genitori, affinché possano riconoscere segnali di pericolo e adottare comportamenti più sicuri online.

Per la fascia d'età 14-16 anni si evidenziano 184 casi nel primo semestre 2025 e 94 casi nel primo semestre 2026. Durante la fase adolescenziale, si osserva un incremento significativo sia nell'uso delle tecnologie di rete sia nel livello di esposizione ai rischi digitali. Sebbene un'adeguata alfabetizzazione digitale dovrebbe favorire una maggiore consapevolezza dei pericoli online, le complesse dinamiche di relazionalità virtuale e i meccanismi di dipendenza dai social media determinano un'elevata vulnerabilità nei giovani. Tale condizione li espone a condotte a rischio e fenomeni vittimizzanti, tra cui il *sexting*, la condivisione non consensuale di materiale intimo, nonché episodi di minaccia e ricatto informatico. Gli adescatori mirano a minori di questa età consapevoli della loro naturale curiosità per la seduzione, la sessualità e l'interazione libera, consapevoli di quanto i ragazzi si sentano sicuri in un dominio, quello digitale, in cui credono di muoversi con maggiore dimestichezza, minore esposizione corporea senza particolari controlli. In questo contesto, il Centro Nazionale per il Contrasto alla Pedopornografia Online ha intensificato le proprie attività investigative, adottando tecniche avanzate di monitoraggio del deep e dark web, collaborando con le principali piattaforme digitali per segnalare e rimuovere contenuti illeciti e rafforzando la cooperazione con le forze dell'ordine internazionali per identificare e fermare i responsabili di questi crimini.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

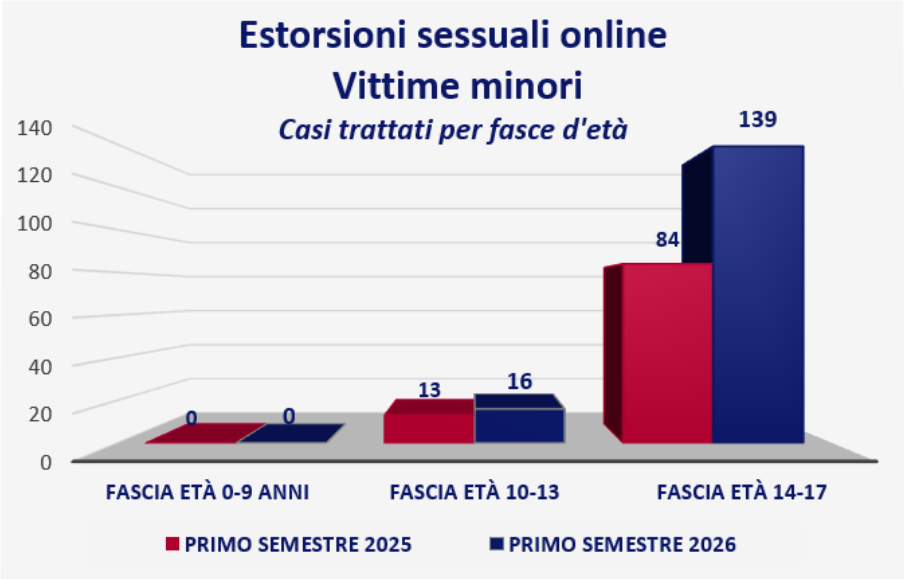
Dal punto di vista della composizione per genere, l'analisi comparativa tra i primi semestri del 2025 e del 2026 riconferma una marcata sproporzione di genere, con la componente femminile che continua a rappresentare la maggioranza assoluta della coorte considerata (oltre il 70% nel 2026).

Il fenomeno dell'adescamento online rappresenta una delle minacce allo sviluppo di bambini e adolescenti più subdole e mutevoli; influenzato continuamente dai cambiamenti sociali nell'uso delle tecnologie da parte delle famiglie, l'adescamento oggi interessa, come potenziale rischio, bambini sempre più piccoli e impone uno sforzo di progettazione di iniziative di prevenzione e sensibilizzazione sempre più complesso. In questo l'attività di analisi dei dati, studio dei casi e valutazione del rischio svolta dall'Uaci consente di progettare e realizzare in sinergia iniziative di sensibilizzazione attagliate sulle caratteristiche contingenti del fenomeno, aumentando l'efficacia dell'opera di sensibilizzazione messa in atto dagli operatori della Polizia Postale, su tutto il territorio nazionale, a partire dalla Scuola Primaria e sino alla maggiore età degli studenti.

Sextortion – Vittime minori

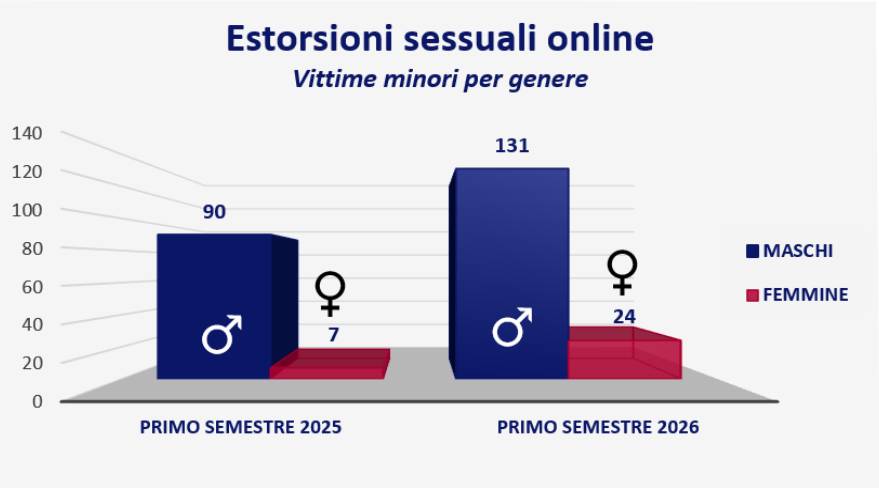
Nel primo semestre del 2026, la sextortion, ossia il ricatto sessuale online, ha assunto un rilievo particolarmente significativo, analizzabile attraverso un incremento del 60% dei casi trattati. Questo aumento richiama l'attenzione su una minaccia che intreccia sfruttamento sessuale, coercizione psicologica e richieste estorsive, con conseguenze potenzialmente gravi per le vittime. Le condotte possono essere messe in atto da singoli autori o da organizzazioni criminali, che fanno leva sulle fragilità psicologiche e sociali dei ragazzi, sulla loro curiosità e sulla fiducia riposta nelle relazioni. Il contatto avviene spesso attraverso profili falsi o identità simulate, con cui viene costruito un rapporto apparentemente rassicurante e confidenziale. La sensazione di discrezione e anonimato offerta dall'ambiente digitale può ridurre la percezione del pericolo, portando i minori a sottovalutare le conseguenze della condivisione di contenuti personali con sconosciuti. Attraverso l'inganno, la seduzione, la manipolazione emotiva o la pressione psicologica, gli autori inducono quindi le vittime a produrre e inviare immagini o video intimi, che diventano lo strumento del ricatto: la minaccia di divulgarli a familiari, amici o compagni di scuola viene utilizzata per ottenere denaro, ulteriori materiali sessuali, favori personali o altre utilità. La relazione inizialmente percepita come sicura si trasforma così in una condizione di soggezione, nella quale il timore dell'esposizione alimenta la pressione sul minore. La vergogna e il senso di isolamento possono impedire al minore di chiedere aiuto o denunciare, prolungando la sua esposizione al ricatto: cedere alle richieste, anziché porre fine alle minacce, può incoraggiare ulteriori pretese da parte dell'autore.

Il C.N.C.P.O. contrasta questa forma di abuso attraverso un'azione integrata, che unisce le indagini per identificare i responsabili e ricostruire i flussi digitali e finanziari dell'estorsione, agli interventi per rimuovere tempestivamente i contenuti illeciti e interrompere il ricatto, affiancando a tali attività iniziative di sensibilizzazione rivolte ai minori e alle famiglie, per aiutarli a riconoscere i segnali di rischio e chiedere aiuto, e percorsi di sostegno alle vittime, finalizzati a contenere le conseguenze psicologiche dell'abuso e favorirne il recupero.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

L'analisi dei dati relativi al primo semestre 2025 e 2026 mostra un incremento nel numero complessivo dei casi trattati, da 97 a 155 (+60%). Un'analisi dettagliata delle fasce d'età delle vittime evidenzia come la minaccia della sextortion colpisca principalmente gli adolescenti tra i 14 e i 17 anni, con 84 casi nel primo semestre 2025 e 139 nel primo semestre 2026. Questa stabilità nei numeri conferma come gli adolescenti, per la loro tendenza ad affidare le esplorazioni sentimentali ai servizi del web, social network e messaggistica in primis, siano più esposti a questa tipologia di attacchi dai quali credono di sapersi difendere perché portatori di un'abitudine d'uso della tecnologia che diventa prassi consolidata.



© 2026 - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Si evidenzia un aumento di 3 casi nella fascia 10-13, per un totale di 13 casi nel primo semestre 2025 e di 16 casi nel primo semestre 2026. Anche se il numero complessivo è più contenuto rispetto agli adolescenti più grandi, questa categoria è particolarmente vulnerabile perché meno consapevole dei pericoli del web e più incline a fidarsi degli interlocutori online. I casi trattati in questa fascia evidenziano una dinamica ricorrente: le vittime vengono spinte con l'inganno a produrre immagini sessualmente esplicite, spesso senza rendersi conto delle implicazioni e successivamente vengono minacciate per ottenere ulteriore materiale. Nella fascia di età 0-9 anni non sono stati riscontrati casi.

Sotto il profilo della distribuzione di genere, si riconferma una prevalenza sistemica della componente maschile (superiore all'84%), con un leggero incremento progressivo nel contingente femminile, passato da 7 a 24 casi. Il Centro lavora in sinergia con Ong e con il Portale istituzionale www.commissariatodips.it per la gestione dei casi di rischio per minori. Le segnalazioni che coinvolgono minori che si rivolgono per richiedere aiuto ad enti esterni e alla Polizia Postale vengono analizzate e gestite con il supporto specialistico dei funzionari psicologi dell'Unità di Analisi del Crimine Informatico (U.A.C.I.). Alle vittime e alle famiglie viene così fornito aiuto immediato in casi di cyberbullismo, adescamento e sextortion in particolare. Il C.N.C.P.O. si impegna per l'identificazione e la denuncia dei responsabili ma offre accoglienza alle vittime e alle loro famiglie fornendo strumenti concreti per affrontare le conseguenze emotive

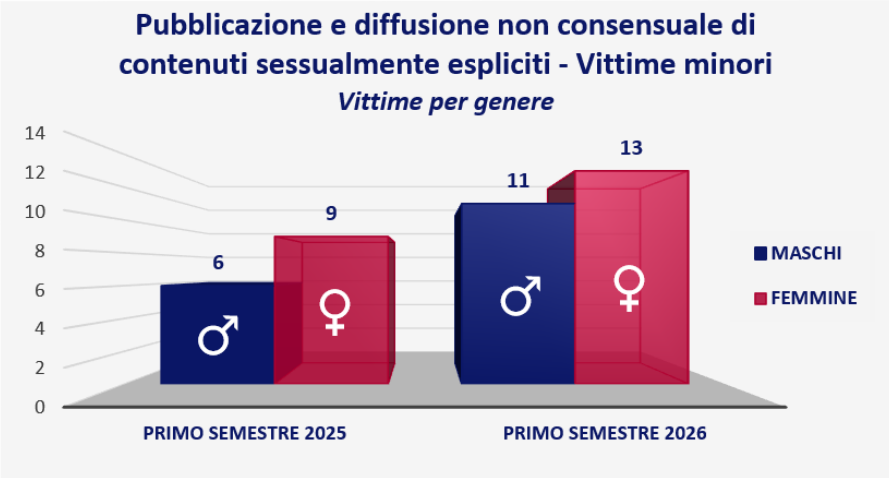
del reato e riprendere il controllo della propria vita. Il contrasto delle sextortion con vittime minorenni continua a rappresentare uno dei target strategici del Centro Nazionale per il Contrasto alla Pedopornografia Online.

Diffusione illecita di immagini o video sessualmente espliciti (612 ter c.p.) – Vittime minori

La diffusione non consensuale di immagini intime, comunemente indicata come *revenge porn*, coinvolge, in ambito minorile, soprattutto preadolescenti e adolescenti, in una fase della crescita in cui le relazioni affettive e la costruzione dell'identità si intrecciano sempre più con la presenza online. L'abuso può maturare dopo la fine di una relazione sentimentale, nei conflitti tra coetanei o in situazioni di adescamento e trova nei social network e nelle applicazioni di messaggistica canali di propagazione rapida, che rendono difficile contenere la circolazione dei materiali e ne amplificano l'impatto sulle vittime. Le immagini possono essere state condivise inizialmente in un rapporto di fiducia oppure ottenute attraverso inganni e pressioni psicologiche, senza che il minore abbia piena consapevolezza del loro possibile utilizzo successivo.

La minaccia di pubblicazione e la divulgazione effettiva possono diventare strumenti di vendetta, controllo o umiliazione, anche all'interno del gruppo dei pari, con conseguenze sulla reputazione, sulle relazioni e sul benessere emotivo della persona coinvolta. Il contrasto al fenomeno integra l'attività investigativa con la prevenzione e l'educazione alla responsabilità digitale. Gli accertamenti si avvalgono di strumenti tecnologici per seguire la circolazione dei file, ricostruire i passaggi di condivisione e identificare i responsabili, anche quando utilizzano profili anonimi o account temporanei. Parallelamente, la collaborazione con scuole, enti pubblici e famiglie sostiene iniziative volte ad aiutare i ragazzi a comprendere i rischi della condivisione di contenuti intimi, rispettare il consenso e la riservatezza altrui, riconoscere le condotte abusive e conoscere i canali attraverso cui chiedere aiuto.

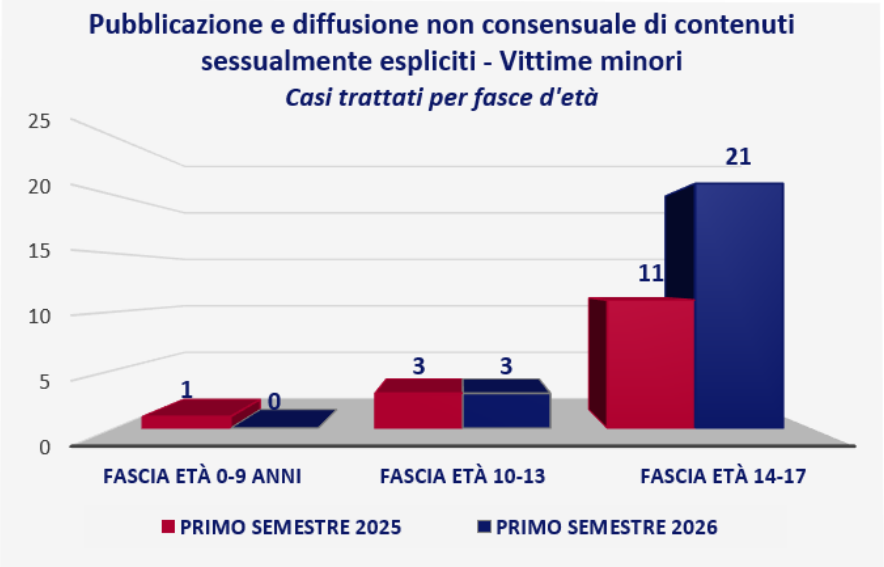
L'analisi dei dati relativi al primo semestre 2025 e 2026 evidenzia un aumento dei casi trattati, passando da 15 nel 2025 a 24 nel 2026, con una crescita del 60%. Questo incremento indica una maggiore diffusione del fenomeno, ma al tempo stesso testimonia l'efficacia del lavoro del C.N.C.P.O., che attraverso monitoraggi sempre più capillari e una crescente sensibilizzazione ha portato a un aumento delle denunce e degli interventi.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Il dato maggiormente in crescita risulta essere quello relativo alla fascia d'età 14-17 anni. Questo incremento evidenzia come anche i più giovani siano esposti al rischio di subire forme di violenza sessuale digitale. Spesso questi casi coinvolgono situazioni in cui i minori vengono indotti con l'inganno o la manipolazione psicologica a condividere immagini intime, senza comprendere appieno le conseguenze di tale azione. L'incremento dei casi in questa fascia d'età ha suggerito un potenziamento delle attività di sensibilizzazione, affinché bambini e preadolescenti siano adeguatamente informati sui pericoli legati alla condivisione di immagini personali in rete.

Gli adolescenti sono spesso vittime di *revenge porn* in contesti di relazioni sentimentali finite male, vendette personali o dinamiche di pressione tra pari. L'abuso si manifesta con la minaccia o la diffusione di immagini intime al fine di esercitare un controllo sulla vittima, danneggiarne la reputazione o ricattarla emotivamente.



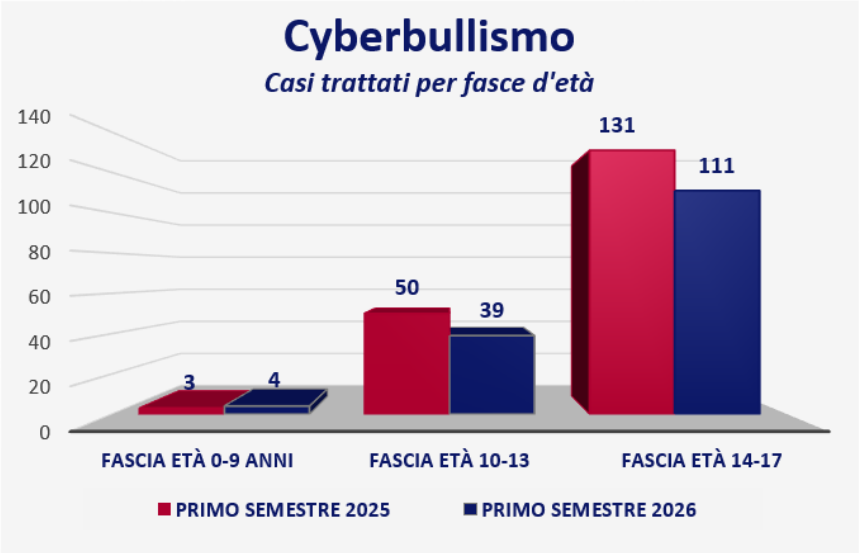
© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Il C.N.C.P.O. interviene con tempestività per identificare i responsabili e bloccare la diffusione dei materiali, collaborando con le principali piattaforme digitali per la rimozione dei contenuti e attivando procedure di supporto psicologico per le vittime, che spesso subiscono gravi ripercussioni emotive e sociali.

Cyberbullismo

Il cyberbullismo compromette la sicurezza e il benessere dei minori attraverso minacce, insulti, diffamazioni, divulgazione di contenuti privati e altre forme di aggressione psicologica. Queste condotte trovano spazio nei social network, nelle piattaforme di comunicazione e nelle chat dei videogiochi online, dove la rapidità della condivisione e l'ampiezza del pubblico possono accrescere l'esposizione e la sofferenza delle vittime.

Il C.N.C.P.O. e gli uffici della Polizia Postale intervengono per individuare gli autori, interrompere le condotte lesive e proteggere i ragazzi coinvolti, affiancando all'attività investigativa iniziative di prevenzione e sensibilizzazione. L'obiettivo è favorire il riconoscimento tempestivo degli abusi e promuovere modalità di relazione fondate sul rispetto della persona e sulla responsabilità nell'utilizzo degli strumenti digitali.



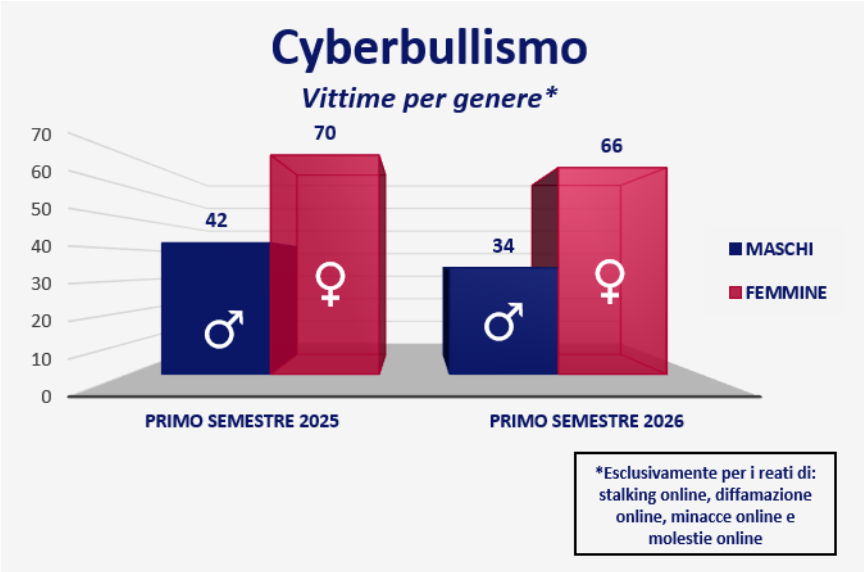
© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

In questo percorso si inserisce il quadro normativo delineato dalla legge n. 71/2017 e ampliato dalla legge n. 70/2024, che rafforza la prevenzione e il contrasto del bullismo e del cyberbullismo, valorizzando gli interventi educativi e rieducativi e il coinvolgimento di scuole e famiglie. Le misure di tutela, insieme agli strumenti per richiedere la rimozione dei contenuti lesivi, concorrono a una risposta che integra protezione delle vittime, responsabilizzazione degli autori e prevenzione della reiterazione dei comportamenti.

L'analisi dei dati relativi al primo semestre 2025 e primo semestre 2026 evidenzia una flessione contenuta nei casi trattati che sono passati da 184 nel 2025 a 154 nel 2026 (-16%). Sebbene il *cyberbullismo* colpisca prevalentemente gli adolescenti, i dati mostrano che nessuna fascia d'età è esente da questo fenomeno; nella fascia 0-9 anni si registrano 3 casi nel primo semestre 2025 e 4 casi nel primo semestre 2026. Questo dato, sebbene numericamente contenuto evidenzia che episodi di prevaricazione digitale possono verificarsi anche tra i più piccoli, spesso in ambienti di gioco *online* o attraverso piattaforme di messaggistica utilizzate senza una piena consapevolezza dei rischi. Nella fascia 10-13 anni si osserva una flessione del 22% con 50 casi registrati nel primo semestre 2025 rispetto ai 39 casi registrati nel primo semestre 2026. In questa fase della crescita, la ricerca di approvazione sociale e l'appartenenza al gruppo diventano fondamentali, e proprio per questo il *cyberbullismo* può avere

conseguenze psicologiche devastanti. Spesso gli atti di prevaricazione si verificano attraverso gruppi di messaggistica privata, dove le vittime vengono isolate, umiliate o sottoposte a pressioni psicologiche che possono portare a conseguenze gravi, come ansia, depressione e perdita di autostima. La fascia 14-17 anni si conferma la più colpita, registrando tuttavia una flessione nei casi da 131 nel primo semestre 2025 a 111 nel primo semestre 2026. Gli adolescenti che vivono una parte sempre più significativa della loro vita online sono particolarmente esposti a forme di *cyberbullismo* che possono includere la diffusione non consensuale di immagini intime, minacce, insulti e fenomeni di esclusione sociale virtuale. In questa fascia d'età, il *cyberbullismo* può intrecciarsi con altre dinamiche digitali pericolose, come il *revenge porn*, la *sextortion* l'adescamento *online*. La rapidità con cui i contenuti possono essere diffusi in rete rende ancora più difficile per le vittime gestire le conseguenze di questi attacchi, portando in alcuni casi a veri e propri stati di profonda sofferenza psichica.

Dal punto di vista della distribuzione di genere, si conferma una persistente sproporzione a carico della componente femminile, che continua a rappresentare circa i due terzi della popolazione in esame.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

L'attività del C.N.C.P.O. nel contrasto al *cyberbullismo* si sviluppa su più livelli. L'aspetto investigativo gioca un ruolo centrale: l'identificazione degli autori, spesso coetanei delle vittime, richiede tecniche di analisi forense e un monitoraggio attento dei canali digitali utilizzati per diffondere contenuti offensivi o minacciosi. Parallelamente, la collaborazione con scuole, istituzioni e associazioni è essenziale per la prevenzione. Le campagne di sensibilizzazione, rivolte sia ai minori che alle loro famiglie mirano a educare all'uso responsabile dei *social media* e a fornire strumenti per difendersi da atti di bullismo digitale.

Nel primo semestre 2026, gli Uffici territoriali della Specialità hanno condotto, sotto il coordinamento del C.N.C.P.O., numerose indagini, alcune delle quali avviate grazie alle segnalazioni acquisite attraverso i canali di cooperazione internazionale e sviluppate anche mediante attività sotto copertura online; tra le operazioni di maggiore rilievo si segnalano le seguenti:

Operazione C.O.S.C. Torino (gennaio 2026)

L'indagine sotto copertura del C.N.C.P.O., durata oltre due anni, ha consentito di identificare due soggetti promotori di un gruppo Telegram dedicato allo scambio di materiale pedopornografico arrestati a Brescia e Torino. I successivi approfondimenti del C.O.S.C. Piemonte e Valle d'Aosta, mediante tecniche di deanonimizzazione, hanno ricostruito la rete di contatti degli indagati e individuato ulteriori quattro soggetti coinvolti nello scambio di materiale illecito. Le perquisizioni disposte dalla Procura di Torino hanno portato a tre arresti in flagranza.

Operazione "Light Bridge" (gennaio 2026)

L'indagine sotto copertura avviata dal C.N.C.P.O. e sviluppata con il C.O.S.C. di Milano, coordinata dalla Procura di Milano con la collaborazione di H.S.I. ed Europol, ha individuato una rete dedita al *Live Distant Child Abuse*, ossia abusi sessuali su minori commissionati a pagamento commessa a distanza tramite videochiamata. L'infiltrazione in comunità ristrette e la deanonimizzazione degli utenti hanno rivelato un sistema di accordi e pagamenti attraverso cui i "buyer" concordavano tempi e modalità delle violenze con intermediari fisicamente presenti accanto alle vittime, detti "trafficker" o "vendor", e le dirigevano in diretta. I compensi, denominati *tips*, venivano trasferiti tramite servizi internazionali di pagamento per importi contenuti, allo scopo di eludere i controlli economico-finanziari. L'operazione ha portato a due arresti in flagranza per detenzione di ingente quantità e quattro denunciati in stato di libertà.

La cooperazione internazionale con l'organizzazione *Child Rescue Coalition*, curata dal C.N.C.P.O. ha sostenuto lo sviluppo di significative indagini sul territorio nazionale che, condotte dagli Uffici della Specialità, hanno portato nel primo semestre del 2026 all'arresto di 28 persone e alla denuncia in stato di libertà di 14 soggetti.

In particolare, sotto la direzione delle Procure di Torino, Firenze e Napoli sono state condotte:

- Operazione "*Viridis*" (marzo 2026): 3 arresti in flagranza e 5 denunce in stato di libertà, con il rinvenimento di ingenti quantità di materiale pedopornografico, anche di natura violenta e raffigurante bambini in tenera età, e il sequestro di numerosi dispositivi informatici.
- Operazione "*Net Sweeping*" (maggio 2026): 8 perquisizioni, concluse con 6 arresti in flagranza e 2 denunce in stato di libertà, e il rinvenimento di decine di migliaia di file pedopornografici, anche relativi a bambini in tenera età.
- Operazione "*Ganymede*" (giugno 2026): 11 perquisizioni tra Campania e Basilicata, con 8 arresti in flagranza, 2 denunce in stato di libertà e il rinvenimento di ingenti quantità di materiale pedopornografico.

Operazione "Mad Hatter" (aprile 2026)

L'indagine sotto copertura condotta dal C.N.C.P.O. dal 2024, sotto il coordinamento della Procura di Roma, ha consentito di infiltrare ambienti virtuali criminali e monitorare canali transnazionali di distribuzione di materiale pedopornografico, anche raffigurante minori in tenera età e prodotto mediante intelligenza artificiale. Le informazioni acquisite con il contributo dell'FBI e i successivi accertamenti hanno portato all'esecuzione di 9 perquisizioni, concluse con 2 arresti e 7 denunce in stato di libertà per detenzione e divulgazione del materiale illecito.

Operazione "Lux contra tenebras" (Maggio 2026)

L'indagine del C.O.S.C. Veneto, condotta con il coordinamento del C.N.C.P.O., ha consentito di identificare attraverso il monitoraggio della rete e l'analisi delle tracce digitali, tre soggetti residenti nelle province di Venezia, Vicenza e Brescia, coinvolti nello scambio online di materiale pedopornografico. Le perquisizioni hanno portato all'arresto in flagranza di 2 soggetti e alla denuncia in stato di libertà di un indagato per detenzione e diffusione di materiale illecito.

L'Unità di Analisi del Crimine Informatico

L'*Unità di Analisi del Crimine Informatico- UACI* è un'*équipe* di funzionari psicologi della Polizia di Stato che integra le competenze di natura sociopsicologica con l'attività di prevenzione e contrasto dei reati online, con particolare riguardo a quelli che coinvolgono minori e vittime vulnerabili.

L'Uaci ha partecipato all'esecuzione di disposizioni dell'Autorità Giudiziaria a carico di autori di reati sessuali e di violenza di genere (perquisizioni domiciliari, interrogatori) e ha condotto ascolti di vittime vulnerabili (S.I.T., audizioni protette, ispezioni fisiche, interrogatori di minorenni autori di reato, etc), assicurando la massima protezione psicoemotiva dal rischio di vittimizzazione secondaria e la massimizzazione dell'attività di raccolta delle prove (15 audizioni/sit di minori vittime di reato, 4 interrogatori di minori autori di reato).

Nel corso dell'anno l'Uaci ha gestito 106 richieste di aiuto provenienti da bambini e ragazzi che si sono rivolti al portale istituzionale, alle hotline nazionali e a ONG attive nella protezione dei minori, in casi di sextortion, cyberbullismo, pedopornografia e violenza di genere online.

Nei primi 6 mesi del 2026 l'Unità ha provveduto **all'ascolto e al supporto specialistico del personale esposto a materiale ad alto impatto emotivo** (pedopornografia, immagini violente, esecuzioni, etc.) con 38 colloqui individuali, 1 debriefing per evento critico, 1 seminario di protezione psicologica, all'interno di progetti tesi ad evitare lo stress cumulativo e la traumatizzazione vicaria, in un'ottica di valorizzazione della risorsa specializzata della Polizia Postale.

Nei primi mesi del 2026, è stata realizzata una **formazione specifica dedicata al personale impiegato nella prevenzione e nel contrasto del cyberterrorismo**, al fine di orientare meglio le attività investigative, dopo il verificarsi di diversi episodi che hanno coinvolto minori radicalizzati online.

Nei primi mesi del 2026 l'Uaci **ha inoltre partecipato a diversi meeting internazionali**, finalizzati a strutturare reti di collaborazione in riferimento ai temi della prevenzione del cybercrime tra i più giovani (Progetto InterCOP di Europol) e dello sviluppo di competenze di leadership nelle forze dell'ordine (SFPR 2026 Foro de Expertos / Expert Meeting sulla leadership, organizzato dalla Guardia Civil Spagnola e la John Moorres University di Liverpool).

Nei primi mesi del 2026 l'Uaci ha curato la sottoscrizione di un **Protocollo di collaborazione con la Federazione Italiana Medici Pediatri** (Fimp), in riferimento al quale sono state strutturate diverse attività preventive congiunte (dalla realizzazione di po-

ster informativi all'avvio di uno studio sulla percezione e i comportamenti dei genitori in materia di rischio online per i minori).

L'Uaci ha partecipato inoltre ai lavori preparatori degli output dei Piani Nazionali definiti dagli **Osservatori Nazionali per la prevenzione e il contrasto della pedofilia e pornografia minorile, del Cyberbullismo e dal Comitato consultivo interistituzionale per l'alfabetizzazione mediatica e digitale.**

Primo Semestre 2026 - Reati contro la persona
Rilevazione nazionale

I 5.020 casi trattati e le 687 persone indagate restituiscono la dimensione dell'impegno della Polizia Postale nel contrasto ai reati contro la persona commessi in rete, dalla diffamazione agli atti persecutori, dalla diffusione non consensuale di immagini intime alla sextortion, fino alle condotte di odio e alla sostituzione di persona.

CATEGORIA	CASI TRATTATI	PERSONE INDAGATE
Sostituzione di Persona	1.555	41
Diffamazione Online	1.447	362
Sextortion	682	53
Illecito Trattamento Dati	357	10
Minacce Online	331	60
Molestie Online	240	38
Diffusione non consensuale di immagini e video a contenuto sessualmente esplicito (Revenge Porn)	187	69
Stalking Online	110	41
Propositi Suicidari	50	4
Fenomeno Hate Speech	61	9
TOTALE COMPLESSIVO	5.020	687

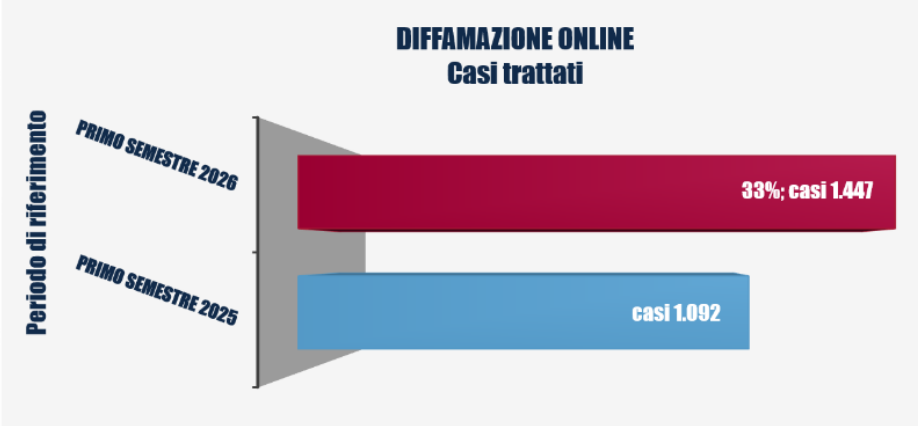
© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Tra i fenomeni emergenti assume particolare rilievo la proliferazione di siti e spazi digitali dedicati alla pubblicazione e allo scambio di materiale intimo senza il consenso delle persone ritratte. La crescente visibilità di questi circuiti evidenzia una modalità di abuso in cui la condivisione tra utenti moltiplica le occasioni di esposizione delle vittime e rende più difficile contenere la circolazione delle immagini. Il contrasto richiede pertanto un monitoraggio costante, finalizzato a individuare gli ambienti di diffusione e i soggetti coinvolti.

L'impiego dell'intelligenza artificiale per creare falsi contenuti pornografici (*deepfake*) ha ulteriormente ampliato le possibilità di abuso, coinvolgendo anche esponenti del giornalismo, dello spettacolo e della politica. Le indagini hanno portato all'avvio di procedimenti penali e al sequestro di infrastrutture digitali, evidenziando la necessità di adeguare costantemente gli strumenti investigativi per contenere la diffusione dei contenuti e tutelare le persone coinvolte. Nel primo semestre del 2026 i casi trattati risultano pari a 5.020 rispetto ai 4.590 del primo semestre del 2025 (+9%). Il dato relativo agli arresti si mantiene sostanzialmente invariato (da 8 a 10), mentre si registra un incremento sia nelle denunce in stato di libertà (+11%) che nelle perquisizioni, passate da 136 nel primo semestre del 2025 a 141 nel primo semestre del 2026 (+4%).

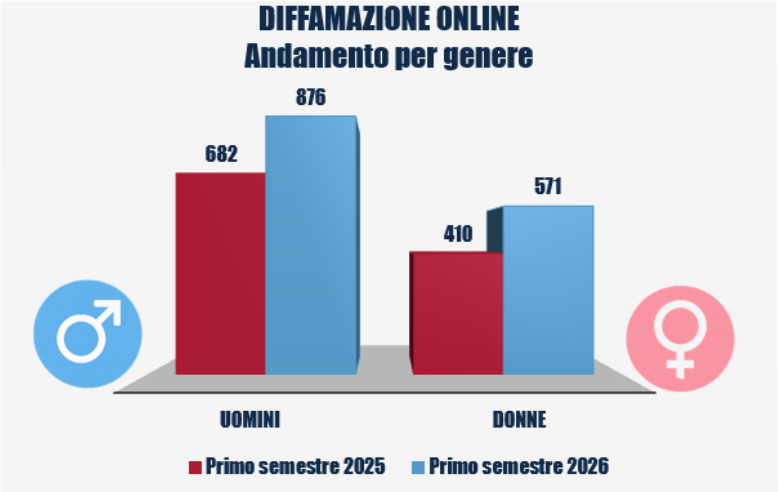
Diffamazione online

Un peso significativo riguarda anche la **diffamazione** online, con 1.447 casi trattati e 362 persone indagate. La rapidità con cui messaggi e pubblicazioni raggiungono un vasto pubblico amplifica il danno alla reputazione e può prolungarne gli effetti nel tempo.



© 2026 - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

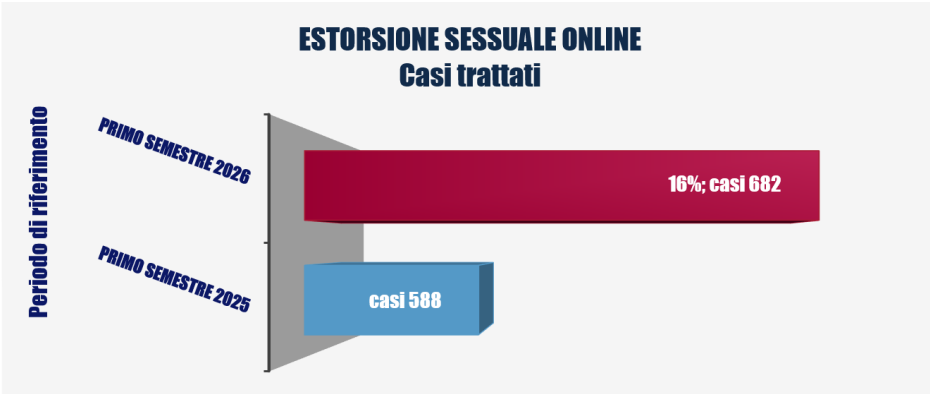
Le indagini, svolte anche in collaborazione con i gestori delle piattaforme, sono state orientate all'identificazione degli autori e alla rimozione dei contenuti lesivi.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Estorsioni sessuali online

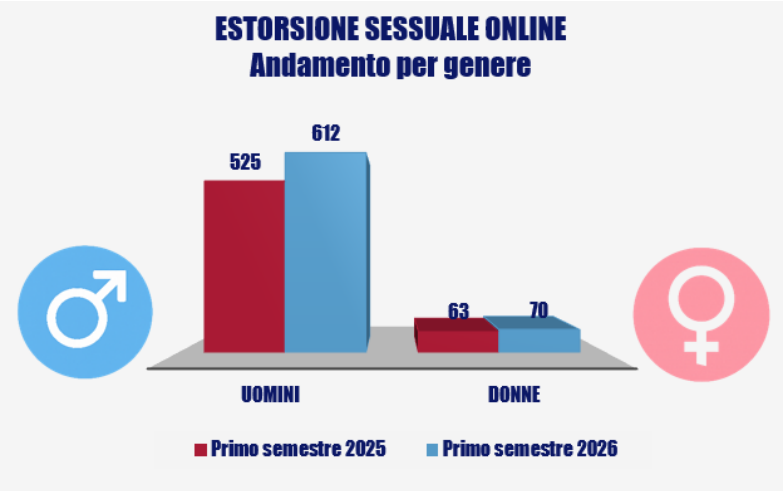
Tra i vari reati trattati emerge quello della *sextortion*. L'analisi dei dati relativi al primo semestre del 2025 e del 2026 evidenzia un incremento nei casi trattati, unitamente al consolidamento di una marcata prevalenza di genere. Nell'arco temporale considerato, il totale complessivo dei casi trattati registra un incremento del 16%, passando da 588 a 682 episodi rilevati.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Sotto il profilo della distribuzione della popolazione offesa in base al sesso, i dati mostrano una sproporzione netta e costante nel tempo, con una prevalente incidenza a carico dei soggetti maschili. Nel primo periodo di osservazione, gli uomini rappresentavano l'89% del totale delle vittime (pari a 525 casi), a fronte di una quota femminile fermatasi all'11% (63 casi). Nel periodo successivo, tale strutturale polarizzazione si è ulteriormente accentuata: la percentuale di vittime di sesso maschile è salita al 90% del totale (612 casi), mentre la componente femminile è scesa al 10% (70 casi).

L'aumento dei volumi totali è stato trainato in misura pressoché esclusiva dalla crescita dei casi a danno di soggetti maschili, aumentati in valore assoluto di 87 unità a fronte di una variazione contenuta della componente femminile. Tale quadro conferma come la sextortion continui a configurarsi nell'ecosistema digitale come un fenomeno criminologico a prevalente connotazione maschile.



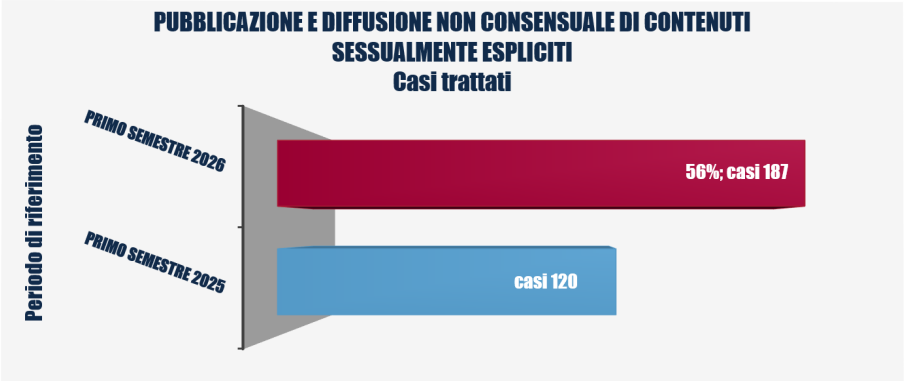
© 2026 - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Sotto una prospettiva di analisi dei reati di genere, tale evidenza, pur riferendosi a un contesto in cui la vittimizzazione femminile non è prevalente, assume rilievo interpretativo. Gli uomini potrebbero essere individuati come bersagli privilegiati nei casi di sextortion in ragione di una possibile maggiore propensione all'interazione digitale a sfondo sessuale ma, dall'altro lato, la dimensione culturale gioca un ruolo determinante. La presenza di possibili stereotipi di genere — la sessualità maschile viene spesso rappresentata in termini di virilità e controllo — rende per l'uomo particolarmente lesiva e umiliante l'eventuale diffusione di materiale intimo, minacciando non

solo la sfera privata e sociale. Inoltre, la reticenza alla denuncia da parte delle vittime maschili, dovuta al timore del giudizio sociale o della difficoltà di riconoscersi nel ruolo della vittima, contribuisce a consolidare l'apparente prevalenza statistica del fenomeno in questa direzione. In altri termini, la sextortion non è un reato "maschile" in senso stretto, ma un fenomeno in cui la differente esposizione e rappresentazione dei ruoli di genere incide sulla selezione delle vittime.

Diffusione illecita di immagini o video sessualmente espliciti

Nel primo semestre del 2026, la diffusione non consensuale di immagini e video sessualmente espliciti ha rappresentato uno dei fenomeni di maggiore rilievo tra i reati online contro la persona. Le numerose segnalazioni ricevute dal Commissariato di P.S. Online e dagli Uffici territoriali hanno riguardato la circolazione di materiale intimo su social network, servizi di messaggistica e siti dedicati, con gravi ripercussioni sulla riservatezza, sulla reputazione e sulla dignità delle vittime.

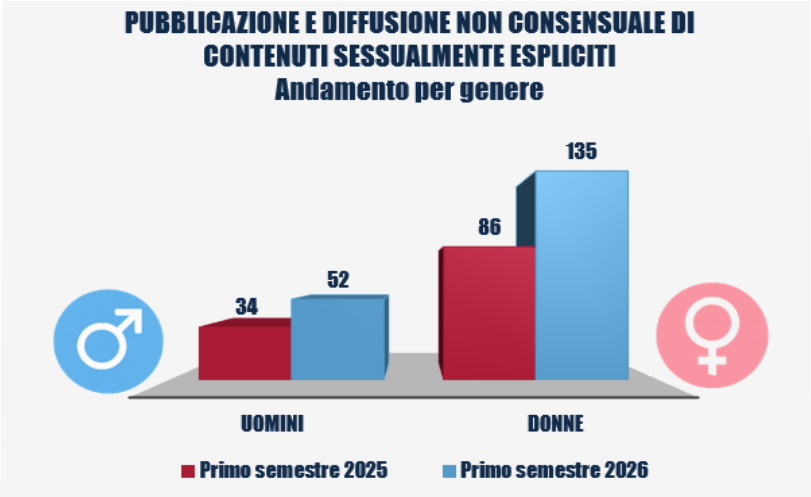


© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Le indagini hanno evidenziato modalità di condivisione sempre più organizzate, soprattutto all'interno di forum e comunità chiuse o parzialmente accessibili. In questi spazi, le immagini vengono spesso associate a informazioni che rendono riconoscibili le persone ritratte e accompagnate da commenti sessualizzati e denigratori. La partecipazione degli utenti e la ripetuta pubblicazione dei materiali prolungano l'offesa e ne rendono difficile il contenimento.

Un ulteriore elemento di criticità è emerso dall'impiego dell'intelligenza artificiale per alterare fotografie e creare falsi contenuti pornografici. Sono stati individuati siti che utilizzavano a questo scopo immagini di esponenti del giornalismo, dello spettacolo

e della politica; gli accertamenti hanno portato all'avvio di procedimenti penali e al sequestro preventivo delle infrastrutture digitali coinvolte.



© 2026 - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

La convergenza tra condivisione organizzata, esposizione dei dati personali e manipolazione delle immagini richiede un continuo adeguamento degli strumenti investigativi e normativi a tutela delle vittime. Dal confronto tra il primo semestre dello scorso anno e il medesimo periodo dell'anno in corso, emerge un forte incremento del fenomeno, pur mantenendosi invece inalterata la proporzione tra i generi.

Il dato generale registra una crescita consistente, passando da 120 a 187 vittime totali, pari a un aumento percentuale del +56%. Nonostante l'aumento dei casi, il rapporto tra le componenti di genere rimane perfettamente identico tra i due periodi osservati. Le donne costituiscono costantemente il 72% della platea complessiva (+49 casi), mentre la componente maschile si attesta stabilmente al 28% (+18 casi).

Un aspetto che merita particolare attenzione riguarda i propositi suicidari, con 50 casi trattati e 4 soggetti indagati. Il ruolo delle forze dell'ordine in questi episodi è stato fondamentale per intervenire in tempo, fornendo supporto psicologico e assistenza. L'attività di monitoraggio delle segnalazioni e la collaborazione con i servizi di emergenza hanno permesso di intervenire tempestivamente e mettere in sicurezza diversi soggetti.

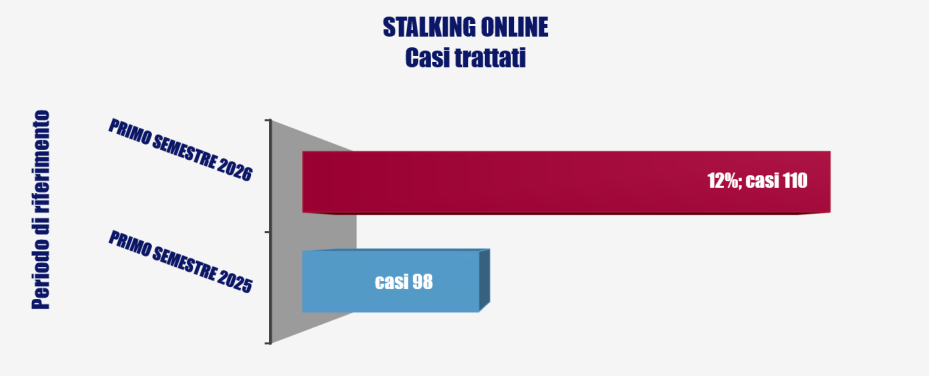
Il fenomeno dell'*hate speech*

Con 61 casi trattati e 9 persone indagate, dimostra come il linguaggio d'odio continui a rappresentare una minaccia per la convivenza civile online. L'intervento della Polizia Postale in questo ambito si è concentrato sull'identificazione dei responsabili e sulla rimozione dei contenuti offensivi. L'insieme di questi dati evidenzia il significativo impegno della Polizia Postale nel contrasto ai reati digitali, con particolare attenzione alla protezione delle persone dalle insidie del web, garantendo la sicurezza e il rispetto della legalità anche in rete.

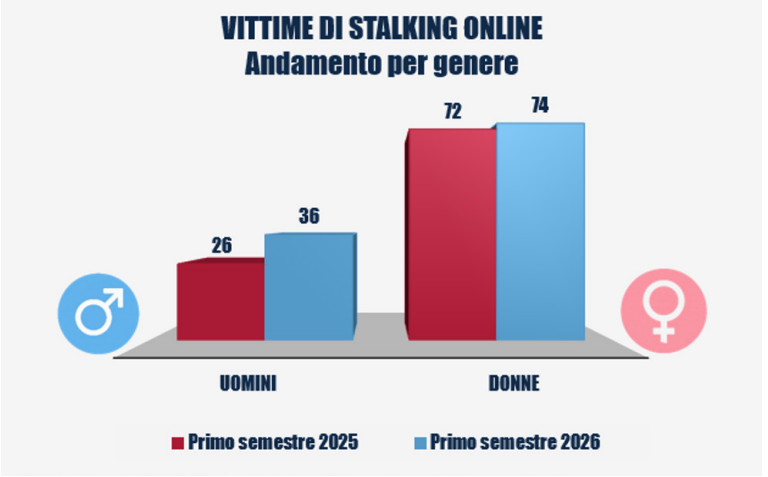
Il reato di stalking

La Polizia Postale è impegnata nel contrasto al *cyberstalking*, mediante l'acquisizione e la conservazione delle prove informatiche, l'analisi delle comunicazioni e la ricostruzione della sequenza degli episodi, per accertarne la continuità e identificarne gli autori, anche quando utilizzano profili anonimi o identità fittizie. A tali attività si affianca la tempestiva valutazione del rischio, essenziale per orientare gli interventi di protezione e prevenire l'aggravamento delle condotte.

Si evidenzia un incremento dei casi di *stalking online* nel primo semestre del 2026 rispetto al primo semestre 2025 del 12%. Emerge inoltre una tendenza significativa sul piano della dimensione di genere. Nei casi trattati, le donne costituiscono la maggioranza delle vittime in entrambi i periodi: 72 vittime su 98 casi (73%) nel primo semestre del 2024 e 74 vittime su 110 casi (67%) nello stesso periodo del 2026. Il numero delle persone indagate è in aumento, passando da 32 a 41 indagati nel primo semestre del 2026, con una crescita del 28%.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica



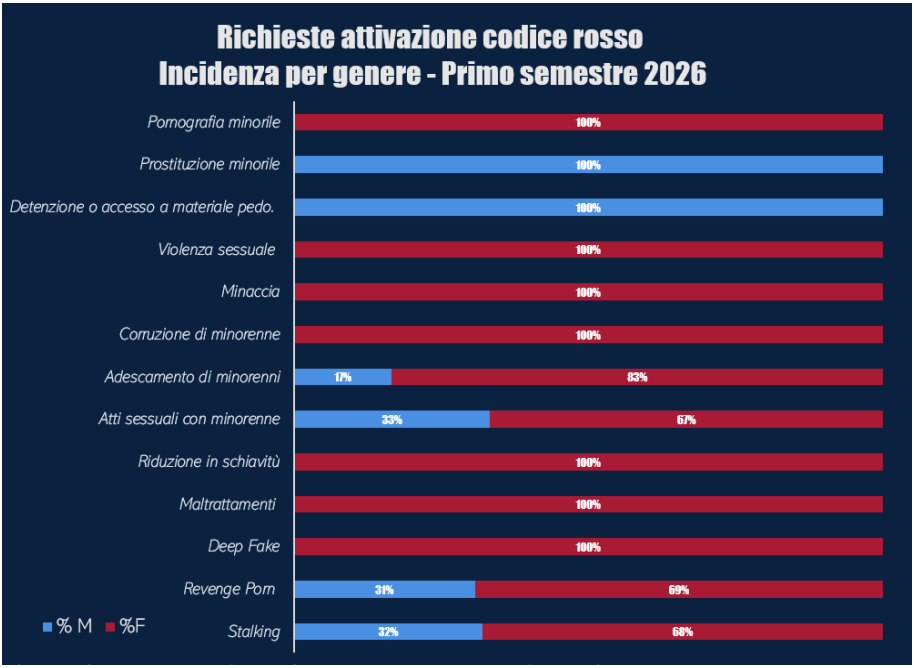
© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Romance Scam

L'attività investigativa della Polizia Postale nel contrasto alle truffe sentimentali online (*romance scam*) si concentra sull'analisi delle comunicazioni, sulla verifica delle identità digitali e sulla ricostruzione dei flussi di denaro, anche attraverso la cooperazione internazionale. Questi accertamenti consentono di ricostruire meccanismi fraudolenti fondati sulla creazione di legami affettivi fittizi, utilizzati per ottenere somme di denaro dalle vittime, con gravi ripercussioni economiche e personali. Gli autori stabiliscono il contatto sui social network e, attraverso un rapporto di fiducia costruito nel tempo, sfruttano il coinvolgimento emotivo e le fragilità legate alla solitudine o ai cambiamenti nella vita familiare per avanzare richieste economiche. Alle indagini si affiancano iniziative di sensibilizzazione volte a favorire il riconoscimento dell'inganno e la segnalazione degli episodi. Nel primo semestre del 2026, la Polizia Postale ha indagato su 162 casi di truffe romantiche (di cui 1 in danno di minori e 34 in danno a soggetti di età superiore ai 65 anni), deferendo all'Autorità giudiziaria 36 persone.

Codice Rosso

L'evoluzione tecnologica e la capillare diffusione degli spazi digitali hanno ridefinito i confini delle relazioni interpersonali, offrendo, al contempo, nuovi strumenti per l'attuazione di condotte vessatorie e violente. In questo scenario, il quadro normativo introdotto dalla Legge 19 luglio 2019, n. 69 (nota come "Codice Rosso") rappresenta il principale baluardo giuridico per il contrasto alla violenza domestica e di genere, garantendo una corsia preferenziale e accelerata per la tutela delle vittime.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

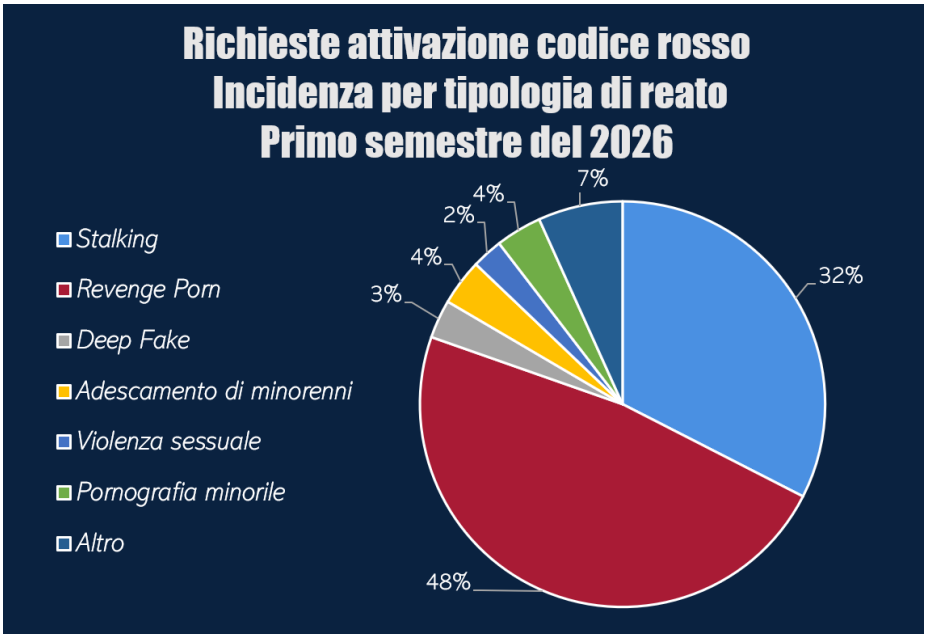
Sebbene la normativa nasca per rispondere a emergenze di natura fisica e domestica, l'attività della Polizia Postale e per la Sicurezza Cibernetica nel corso del primo semestre del 2026 evidenzia una pervasività sempre maggiore della violenza "tecnomediata".

Secondo i dati consolidati al primo semestre del 2026, la Polizia Postale ha proceduto all'attivazione di 162 richieste di Codice Rosso con una prevalenza netta di attivazioni per l'art 612 bis e 612 ter, che complessivamente rappresentano oltre i tre quarti del-

le segnalazioni. In particolare, la diffusione illecita di immagini o video a contenuto sessualmente esplicito (revenge porn) ha fatto registrare 78 richieste, di cui 54 riferite a donne e 24 a uomini, confermandosi come una delle forme di violenza più ricorrenti e trasversali, mentre lo stalking online ha determinato 53 attivazioni, con 36 vittime di sesso femminile e 17 di sesso maschile. In misura quantitativamente inferiore, ma non per questo meno rilevante sotto il profilo della sicurezza sociale, si collocano le attivazioni connesse a fattispecie quali i *deepfake*, adescamento di minorenni, pornografia minorile, maltrattamenti contro familiari o conviventi, la violenza sessuale, le minacce e i diversi reati a danno di minori.

Attivazione Codice Rosso	**PRIMO SEMESTRE 2026**	
	DONNE	**UOMINI**
Stalking (Art. 612 bis)	36	17
Revenge Porn (Art. 612 ter)	54	24
Deep Fake (Art 612 quater)	5	0
Maltrattamenti contro familiari o conviventi (Art. 572)	3	0
Riduzione o mantenimento in schivitù (Art. 600)	1	0
Atti sessuali con minorenne (Art. 609 quater)	2	1
Adescamento di minorenni (Art. 609 undecies)	5	1
Corruzione di minorenne (Art. 609 quinques)	1	0
Minaccia (Art. 612)	1	0
Violenza sessuale (Art. 609 bis)	4	0
Detenzione o accesso a materiale pedopornografico (Art 600 quater)	0	1
Prostituzione minorile (Art 600 bis)	0	1
Pornografia minorile (Art. 600 ter)	5	0
Totali per genere	**117**	**45**
TOTALI	**162**	

Nel loro complesso, tali evidenze restituiscono un panorama di complessità, confermando il ruolo cardine del Codice Rosso quale dispositivo di protezione tempestiva e risposta immediata a tutela dei soggetti in condizione di maggiore vulnerabilità.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

L'impegno della Seconda Divisione del Servizio Polizia Postale, nell'ambito dell'attività di contrasto dei siti contenenti immagini sessualmente esplicite con contenuti sessisti è stato significativo e ha portato risultati importanti grazie ad un monitoraggio costante delle piattaforme e nell'attività di contrasto grazie ad una sinergica cooperazione con Agenzie internazionali per la localizzazione dei domini e le procedure di sequestro mediante oscuramento.

Nel primo semestre del 2026, l'attività della Sezione Operativa della Seconda Divisione si è articolata in numerose indagini a tutela della persona negli ambienti digitali, condotte anche in raccordo con gli Uffici territoriali della Specialità e attraverso i canali di cooperazione internazionale; tra le operazioni di maggiore rilievo si segnalano le seguenti:

Sito di immagini sessualmente esplicite e contenuti sessisti – Sequestro di "phica.eu/phica.net"

L'indagine, coordinata dalla Procura di Roma, è stata avviata dal Servizio Polizia Postale e per la Sicurezza Cibernetica a seguito di segnalazione di diversi contenuti diffamatori e foto presenti sul suindicato sito, contenente diversi forum, nei quali

venivano pubblicate immagini pubbliche e private, di donne, tra le quali anche personaggi politici, del mondo dello spettacolo e influencer. La vicenda, attenzionata dalle maggiori testate giornalistiche nazionali per la complessità dei fenomeni, delle tematiche e delle vittime coinvolte, ha portato al sequestro del sito di proporzioni considerevoli contenenti, tra area pubblica e privata, 9.612.241 file, di cui 8.843.852 immagini e 768.389 video.

Sito Facebook Mia moglie (gennaio 2026)
L'indagine del Servizio Polizia Postale e per la Sicurezza Cibernetica, coordinata dalla Procura di Roma, è stata avviata a seguito delle segnalazioni sul gruppo Facebook denominato "*Mia moglie*" contenente immagini di donne in contesti sessualmente espliciti. Gli accertamenti hanno consentito di identificare soggetti ritenuti coinvolti nell'attivazione e nella gestione del gruppo e le perquisizioni effettuate nei loro confronti, con la collaborazione del C.O.S.C. di Bari e la S.O.S.C. di Lecce, hanno portato al sequestro di diversi dispositivi informatici.

Arresto atleta paralimpico (maggio 2026)
L'indagine, avviata a seguito di una segnalazione successiva alla sospensione sportiva di un atleta paralimpico e coordinata dalla Procura di Roma, ha ricostruito presunte condotte persecutorie, molestie e violenze sessuali ai danni di colleghe anche minorenni della Nazionale Paralimpica di Tiro con l'Arco. Gli accertamenti, supportati dalla perquisizione informatica del C.O.S.C. di Torino, hanno riguardato episodi protratti per anni negli impianti sportivi e sui social network. Nei confronti del quarantaduenne è stata disposta ed eseguita la misura cautelare degli arresti domiciliari.

Deepfake a sfondo sessuale – Oscuramento della piattaforma 'cFake.com' (giugno 2026)
L'indagine del Servizio Polizia Postale e per la Sicurezza Cibernetica, avviata nell'ottobre 2025 e coordinata dalla Procura di Roma, ha riguardato una piattaforma che diffondeva contenuti sessualmente espliciti, anche generati mediante intelligenza artificiale, raffiguranti donne della politica, dello spettacolo, dello sport e della cultura. Gli accertamenti hanno localizzato l'infrastruttura e portato, nel novembre 2025, al sequestro preventivo mediante oscuramento del sito in Italia. La successiva cooperazione con HSI e le autorità giudiziarie statunitensi ha consentito anche il sequestro dell'intero dominio localizzato negli Stati Uniti.

La Terza Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica

La Terza Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica costituisce un presidio specialistico dedicato alla protezione delle infrastrutture critiche nazionali e al contrasto delle minacce di matrice eversiva e terroristica veicolate attraverso il dominio digitale. In un contesto in cui la continuità dei servizi essenziali – energia, trasporti, comunicazioni, sanità e finanza – rappresenta un fattore determinante per la stabilità del Paese, la Divisione concorre al rafforzamento della sicurezza complessiva e alla prevenzione di attacchi suscettibili di produrre effetti sistemici.

L'azione operativa si fonda su un modello integrato che coniuga raccolta e analisi delle informazioni, competenze tecnico-forensi e attività investigative, con l'obiettivo di individuare tempestivamente indicatori di minaccia e contrastare le condotte ostili. Parallelamente, la Divisione promuove l'aggiornamento degli strumenti tecnologici e delle metodologie di analisi digitale, contribuendo al potenziamento delle capacità di risposta della Polizia di Stato e assicurando supporto specialistico all'Autorità giudiziaria e agli altri soggetti istituzionali competenti.

Un elemento qualificante della Terza Divisione è rappresentato dalle funzioni di indirizzo e coordinamento a livello nazionale nei confronti delle articolazioni territoriali, finalizzate ad assicurare uniformità di approccio, coerenza procedurale e tempestività degli interventi. La Divisione mantiene inoltre un raccordo costante con le altre componenti del sistema di sicurezza e con i partner internazionali, nell'ambito di una cooperazione essenziale per affrontare minacce transnazionali e fenomeni caratterizzati dall'interdipendenza tra dimensione fisica e digitale.

Attraverso indagini complesse, attività di prevenzione mirate e un'interlocuzione continuativa con istituzioni e operatori dei settori strategici, la Terza Divisione contribuisce alla sicurezza cibernetica del sistema Paese, valorizzando le competenze investigative e gli strumenti tecnologici di prevenzione e contrasto.

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – C.N.A.I.P.I.C.: ruolo e funzioni

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), istituito con decreto del Ministro dell'Interno del 9 gennaio 2008, costituisce uno dei centri di specialità del Servizio Polizia Postale e per la Sicurezza Cibernetica ed è dedicato alla prevenzione e al contrasto dei crimini informatici diretti contro le infrastrutture critiche e i servizi di rilevanza nazionale.

Mandato istituzionale

Quale struttura istituzionalmente denominata *"Organo del Ministero dell'Interno per la sicurezza e regolarità dei servizi di telecomunicazioni"*, il Centro svolge compiti di prevenzione e repressione dei crimini informatici di matrice comune, organizzata o terroristica che prendono di mira infrastrutture informatizzate di rilevanza strategica per il Paese.

Ambito operativo e modelli di intervento

Il C.N.A.I.P.I.C.:

- Opera in raccordo con i soggetti dell'architettura nazionale di cybersicurezza e con l'Autorità giudiziaria, anche attraverso protocolli d'intesa e procedure condivise per la segnalazione, la gestione e l'analisi degli incidenti.
- Contribuisce all'acquisizione e alla condivisione delle informazioni relative agli attacchi che interessano i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, favorendo la continuità dei flussi informativi anche nelle fasi successive alla prima segnalazione.
- Si avvale del raccordo con i Centri Operativi per la Sicurezza Cibernetica (COSC) e con i Nuclei Operativi per la Sicurezza Cibernetica (NOSC), che assicurano sul territorio capacità di intervento e prossimità operativa rispetto alle realtà da proteggere.
- Esercita funzioni di indirizzo e coordinamento nei confronti delle articolazioni territoriali, integrando attività strategiche e operative nel quadro delle strutture dipartimentali di pubblica sicurezza.
- Concorre alle attività di cooperazione internazionale in materia di criminalità informatica, anche nel quadro della Convenzione di Budapest, favorendo il tempestivo scambio di informazioni e la preservazione delle prove elettroniche, nel rispetto delle competenze delle autorità coinvolte e della normativa applicabile.

Partnership e scambio informativo

Il C.N.A.I.P.I.C. assolve i propri compiti istituzionali anche attraverso accordi e convenzioni con gestori di infrastrutture critiche, enti e operatori di settori sensibili. Tali forme di collaborazione favoriscono lo scambio di informazioni, anche di natura tecnica, utili alla comprensione delle minacce e all'adozione tempestiva di misure di mitigazione.

In tale ambito, il Centro diffonde segnalazioni e avvisi tecnici agli interlocutori interessati, contribuendo all'aggiornamento delle misure difensive e alla tempestiva attivazione degli interventi necessari sui sistemi esposti o colpiti da attacchi.

Monitoraggio e analisi delle minacce

Il personale specializzato del C.N.A.I.P.I.C. svolge attività continuative di monitoraggio e analisi delle tattiche, tecniche e procedure (TTP) impiegate dai gruppi criminali e dagli altri attori ostili, al fine di individuare l'evoluzione delle campagne di attacco e supportare le attività preventive e investigative.

Le metodologie investigative integrano accertamenti tecnico-forensi, elementi indiziari e analisi dei comportamenti osservati per ricostruire le modalità operative e le infrastrutture utilizzate, nonché valutare le eventuali attribuzioni sulla base delle evidenze disponibili.

L'attività anticrimine del C.N.A.I.P.I.C. e dei N.O.S.C. ha consentito, nel periodo di riferimento, di rilevare complessivamente **4.082** attacchi, nonché di diramare **23.940** *alert*. Le indagini avviate esclusivamente dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche hanno consentito di deferire all'Autorità Giudiziaria **84** persone e di dare seguito a **31** richieste di cooperazione internazionale pervenute in ambito Rete 24/7 High Tech Crime (Convenzione di Budapest).



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Scenario delle minacce e principali tendenze

L'analisi delle attività sopra illustrate si inserisce in uno scenario caratterizzato dalla persistente pressione della minaccia cibernetica, dalla diversificazione delle finalità degli attacchi e dal crescente sfruttamento delle interdipendenze digitali. Cittadini, pubbliche amministrazioni e imprese risultano esposti a condotte riconducibili tanto alla criminalità informatica di matrice economica quanto ad attività di spionaggio, hacktivismo e influenza informativa, fenomeni distinti e non necessariamente coordinati. Particolare rilievo assumono le vulnerabilità delle catene di fornitura tecnologiche e delle realtà produttive di minori dimensioni, il cui coinvolgimento può ripercuotersi sulla continuità di servizi e settori strategici.

Tra le principali modalità di attacco si confermano lo sfruttamento di vulnerabilità, anche di tipo zero-day, la compromissione di credenziali e identità digitali, il phishing mirato e l'impiego di malware e ransomware. Le attività più selettive, talora riconducibili ad attori sostenuti da Stati, possono essere orientate all'acquisizione di informazioni sensibili e al mantenimento di accessi riservati e persistenti, anche attraverso apparati di rete e rapporti con fornitori di servizi. Le campagne criminali a fini estorsivi, invece, continuano a sfruttare l'esfiltrazione dei dati e l'interruzione dell'operatività delle vittime; la riconducibilità dei singoli episodi deve in ogni caso essere valutata sulla base delle evidenze disponibili.

Permane il ricorso ad attacchi distribuiti di negazione del servizio (DDoS), anche mediante botnet e infrastrutture disponibili a noleggio, indirizzati verso portali istituzionali e servizi di interesse pubblico. In contesti di tensione internazionale, tali azioni possono assumere finalità dimostrative e propagandistiche, risultando talvolta accompagnate da rivendicazioni e campagne di amplificazione online. Nel quadro russo e filo-russo si osservano, accanto a iniziative di hacktivismo, attività di spionaggio e condotte di gruppi criminali russofoni, senza che la comune area linguistica o ideologica implichi di per sé un coordinamento o un collegamento con apparati statali.

Un ulteriore elemento di evoluzione è rappresentato dall'impiego dell'intelligenza artificiale generativa a supporto delle attività malevole. Tali strumenti possono agevolare la produzione di messaggi di phishing più credibili e personalizzati, la traduzione e diffusione su larga scala di contenuti ingannevoli e l'impersonificazione mediante voci, immagini o video sintetici (deepfake). Possono inoltre accelerare alcune fasi preparatorie delle campagne informatiche, senza che ciò comporti necessariamente una piena autonomia degli attacchi. Ne deriva un rafforzamento delle tecniche di ingegneria sociale e una maggiore difficoltà nel distinguere comunicazioni autentiche da contenuti fraudolenti.

© Clusit 2026

L'azione del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), nell'ambito delle competenze del Servizio Polizia Postale e per la Sicurezza Cibernetica, si colloca in un quadro normativo che ha progressivamente rafforzato gli strumenti investigativi anche nel dominio digitale, comprese, nei limiti e alle condizioni previsti dalla legge, le operazioni sotto copertura e le attività funzionali all'acquisizione della prova.

La natura transnazionale del cybercrime, la distribuzione geografica di infrastrutture e dati e la diversità delle discipline in materia di acquisizione della prova elettronica e conservazione dei dati continuano a incidere sull'efficacia del contrasto. Assumono pertanto rilievo l'individuazione precoce delle anomalie, il monitoraggio delle fonti aperte, la tempestiva acquisizione e conservazione delle evidenze informatiche e la correlazione di indicatori tecnici e risultanze investigative. La condivisione delle informazioni e la cooperazione con l'Autorità giudiziaria, gli organismi competenti e i partner internazionali consentono di ricostruire infrastrutture, modalità operative e possibili collegamenti tra episodi verificatisi in Paesi diversi.

Rapporto di Analisi sulle Minacce Informatiche – Primo semestre 2026

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) ha ricevuto e analizzato 1.669 segnalazioni di eventi e attacchi informatici nel periodo 1° gennaio – 30 giugno 2026. Tali dati, provenienti dall'Agenzia per la Cybersicurezza Nazionale (ACN) - CSIRT Italia e da altri enti pubblici e privati che collaborano con il Servizio, forniscono una visione chiara dei settori più esposti e delle metodologie di attacco prevalenti.
Dall'analisi emerge una netta prevalenza di incidenti a danno del settore delle **Imprese e Industrie**, che da solo rappresenta il **41%** del totale con **679 segnalazioni**. Tale concentrazione indica come il tessuto produttivo nazionale sia un bersaglio primario, probabilmente a causa del valore economico dei dati industriali, della proprietà intellettuale e delle informazioni commerciali detenute. Le conseguenze di tali attacchi possono spaziare dall'interruzione delle catene di produzione a significative perdite finanziarie.

Si osserva inoltre una forte pressione sui **fornitori di servizi di gestione delle tecnologie dell'informazione** (**246** casi) e sulla **Pubblica Amministrazione** (**229 casi**). I gestori di servizi TIC sono obiettivi strategici, poiché la loro compromissione può consentire attacchi a cascata verso i loro clienti, amplificando l'impatto. La Pubblica Amministrazione è invece bersagliata per la grande quantità di dati sensibili dei cittadini che gestisce e per il potenziale impatto sulla continuità dei servizi essenziali per la collettività.

Significative, sebbene numericamente inferiori, risultano le segnalazioni provenienti dal settore **dell'Energia (100)**. La criticità degli attacchi verso il comparto energetico, nonostante la minore frequenza, è dovuta alle ripercussioni dirette sulla sicurezza nazionale e sull'erogazione di servizi fondamentali per la popolazione. Seguono poi gli attacchi alle **società di servizi e commercio** (**76**), alla **sanità** (**76**), ai **trasporti** (**72**), ai **servizi bancari e finanziari** (**56**) e al **settore della ricerca e istruzione** (**50**).

Per quanto riguarda le **tecniche di attacco**, le segnalazioni indicano il **phishing** come il principale vettore, con **342 casi** registrati **(20%)**. Questa metodologia, basata sull'ingegneria sociale, si conferma un efficace strumento per ottenere un primo accesso ai sistemi aziendali, spesso fungendo da preludio ad attacchi più strutturati e dannosi.

Seguono per frequenza gli attacchi di tipo **ransomware** (**228 segnalazioni, 14%**), che mirano alla cifratura dei dati a scopo di estorsione, e gli episodi di **accesso abusivo** ai sistemi (**167 segnalazioni, 10%**). Il ransomware si caratterizza per l'impatto immediato e distruttivo, causando la paralisi operativa delle vittime. Gli accessi abusivi, invece, possono essere finalizzati a diverse attività illecite, tra cui lo spionaggio informatico e la preparazione di futuri attacchi.

Si registrano inoltre **140** episodi di **compromissione della casella mail** (Business Email Compromise - BEC). Questa tecnica, che mira a infiltrarsi nelle comunicazioni aziendali intercettando o sostituendosi ai canali ufficiali, rappresenta una minaccia insidiosa per le transazioni finanziarie e la riservatezza delle informazioni strategiche, facendo leva sulla vulnerabilità dei flussi di lavoro quotidiani.

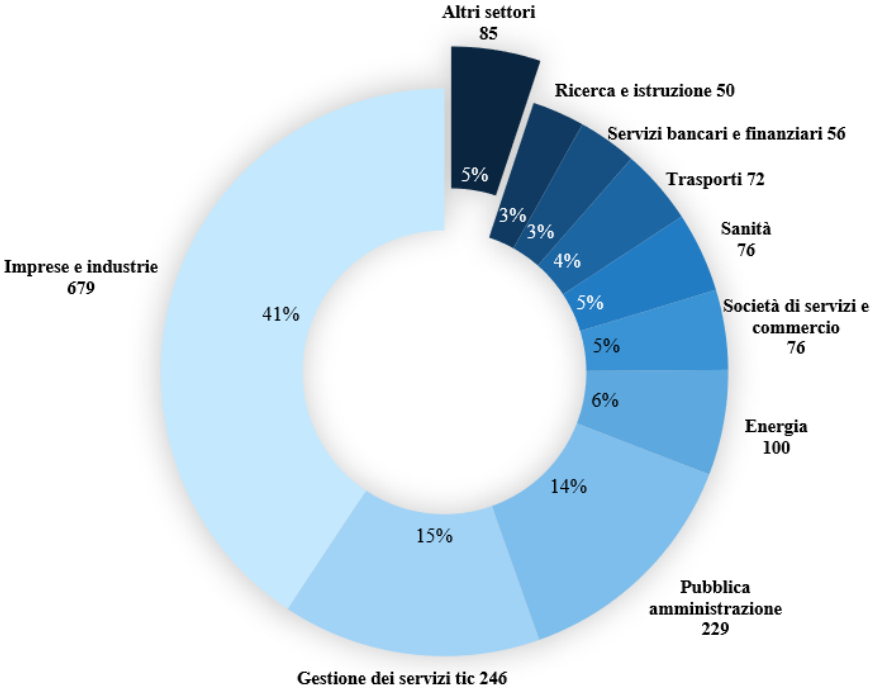
La stabilità delle infrastrutture di rete è stata messa a dura prova da **93** attacchi di tipo **DDoS** (Distributed Denial of Service). Tali offensive, finalizzate a saturare le risorse dei server bersaglio per renderli indisponibili agli utenti, non mirano direttamente al furto di dati, ma si configurano come uno strumento di forte pressione economica e di disturbo operativo, spesso utilizzato con finalità estorsive o dimostrative.

La diffusione e l'impiego di **malware** generico o specializzato – al di fuori delle già citate varianti ransomware – ha fatto registrare **92** casi. A questi si affiancano **87** eventi riconducibili allo sfruttamento di vulnerabilità, note o non note, presenti nei sistemi per aggirare le difese ed effettuare accessi non autorizzati.

Si evidenziano **81 casi** riconducibili a **databreach**, ovvero alla violazione e conseguente esfiltrazione di dati. Tali incidenti comportano non solo un grave danno d'immagine per le organizzazioni colpite, ma anche un rischio concreto per la privacy e la sicurezza degli individui cui le informazioni sottratte si riferiscono.

Infine, l'**esposizione dei dati** rappresenta il vettore d'attacco principale in **46 casi registrati**, configurandosi come il punto di vulnerabilità iniziale attraverso cui le informazioni riservate o non protette (es. database aperti) sono state direttamente intercettate e sfruttate per violare i sistemi.

Analisi Settoriale (Primo semestre del 2026)

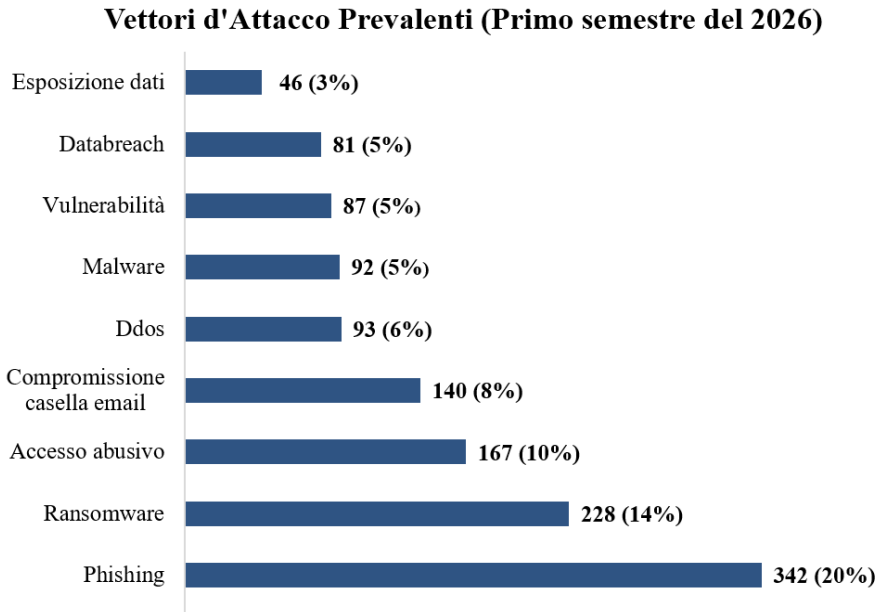


Nota: la categoria 'Altri settori' nel grafico include i seguenti settori (ciascuno con incidenza inferiore al 3%):

Privato: 29 eventi
Acqua potabile: 13 eventi
Fondazione: 11 eventi
Gestione dei rifiuti: 9 eventi
Acque reflue: 9 eventi
Spazio: 8 eventi
Media: 5 eventi
Difesa: 1 eventi

Settore	Totale – Primo semestre	Incidenza %
Imprese e industrie	679	40,68 %
Gestione dei servizi tic	246	14,74 %
Pubblica amministrazione	229	13,72 %
Energia	100	5,99 %
Società di servizi e commercio	76	4,55 %
Sanità	76	4,55 %
Trasporti	72	4,31 %
Servizi bancari e finanziari	56	3,36 %
Ricerca e istruzione	50	3,00 %
Privato	29	1,74 %
Acqua potabile	13	0,78 %
Fondazione	11	0,66 %
Gestione dei rifiuti	9	0,54 %
Acque reflue	9	0,54 %
Spazio	8	0,48 %
Media	5	0,30 %
Difesa	1	0,06 %

© Clusit 2026



Vettore d'Attacco	Valore Assoluto	Incidenza %
Phishing	342	20,49%
Ransomware	228	13,66%
Altro	182	10,90%
Accesso abusivo	167	10,01%
Compromissione casella email	140	8,39%
Ddos	93	5,57%
Malware	92	5,51%
Vulnerabilità	87	5,21%
Databreach	81	4,85%
Esposizione dati	46	2,76%
Attacchi web-based	38	2,28%
Esfiltrazione	32	1,92%
Defacement	29	1,74%

Vettore d'Attacco	Valore Assoluto	Incidenza %
Social engineering	18	1,08%
Guasto	16	0,96%
Supply chain	12	0,72%
Infostealer	11	0,66%
Data leak	10	0,60%
Compromissioni credenziali	10	0,60%
Compromissione di apparati scada	10	0,60%
Hacking	8	0,48%
Brand abuse	6	0,36%
Stuffing	4	0,24%
Tecniche apt	3	0,18%
Frode	2	0,12%
Possibile compromissione account microsoft office365	1	0,06%
Flusso crittografico	1	0,06%

Principali vettori per settore (top 6 – Primo semestre 2026)

La seguente tabella mostra, per ciascuno dei sei settori più colpiti, i primi tre vettori di attacco in termini di frequenza, con l'indicazione del numero di eventi e dell'incidenza percentuale sul totale del settore. Questa matrice consente di comprendere le minacce più rilevanti per ogni comparto e di orientare le misure di prevenzione in modo mirato.

Settore	Principali vettori d'attacco (top 3)
Imprese e industrie	Ransomware: 155 eventi (23%) Phishing: 125 eventi (18%) Accesso abusivo: 67 eventi (10%) Compromissione casella mail: 67 (10%)
Gestione dei servizi tic	Phishing: 52 eventi (21%) Malware: 33 eventi (13%) Accesso abusivo: 20 eventi (8%) Compromissione casella mail: 20 (8%) Vulnerabilità: 20 (8%)

© Clusit 2026

Settore	Principali vettori d'attacco (top 3)
Pubblica amministrazione	Phishing: 54 eventi (24%) Accesso abusivo: 31 eventi (14%) Ddos: 30 eventi (13%)
Energia	Altro: 19 eventi (19%) Esposizione dati: 18 eventi (18%) Phishing: 15 eventi (15%)
Società di servizi e commercio	Phishing: 22 eventi (29%) Ransomware: 16 eventi (21%) Accesso abusivo: 8 eventi (11%)
Sanità	Phishing: 17 eventi (22%) Compromissione casella mail: 11 eventi (14%) Ransomware: 7 eventi (9%)

Il Settore Cyberterrorismo

Nel corso del primo semestre del 2026, l'intensificarsi delle tensioni geopolitiche internazionali, con particolare riferimento agli scenari russo-ucraino e israelo-palestinese e all'emergere del confronto tra Iran e Stati Uniti, ha determinato un incremento dell'attenzione operativa nei confronti delle minacce ibride e delle relative manifestazioni nell'ecosistema digitale.

In tale contesto, sono state intensificate le attività di monitoraggio e raccolta informativa finalizzate all'individuazione di campagne di disinformazione, profili falsi e iniziative online riconducibili a strategie di manipolazione dell'opinione pubblica e di delegittimazione delle istituzioni. Particolare attenzione è stata riservata alla diffusione di *fake news*, alla creazione di account e pagine che riproducono impropriamente l'identità di enti e organismi istituzionali e all'utilizzo di profili fittizi per veicolare comunicazioni ingannevoli. Gli approfondimenti condotti hanno consentito di individuare numerosi account *fake*, impiegati per attività fraudolente o per condotte di impersonificazione, per i quali sono state attivate le procedure finalizzate alla rimozione, anche attraverso interlocuzioni con i gestori delle piattaforme digitali.

Un ulteriore ambito di intervento ha riguardato il contrasto alla diffusione di messaggi antisemiti e di espressioni d'odio rivolte alla comunità ebraica, fenomeni che hanno trovato nell'attualità geopolitica un ulteriore fattore di amplificazione. Sono state pertanto svolte specifiche attività di approfondimento investigativo su profili social utilizzati per la pubblicazione e la diffusione di contenuti antisemiti, finalizzate a ricostruire le modalità di propagazione dei messaggi, individuare gli account coinvolti e valutare eventuali profili di rilevanza penale.

A tali attività si è affiancata una mirata azione di raccolta informativa volta a intercettare possibili iniziative ostili in concomitanza con le principali festività e ricorrenze religiose ebraiche, così da consentire alle competenti articolazioni territoriali di disporre di elementi utili alla valutazione preventiva del rischio e all'eventuale adozione delle misure di competenza.

Parallelamente, il monitoraggio delle manifestazioni di dissenso sviluppatesi online in relazione ai principali scenari di crisi internazionale ha consentito di individuare espressioni di radicalizzazione, messaggi di incitamento alla violenza e possibili progettualità suscettibili di assumere rilievo sotto il profilo della sicurezza pubblica. Gli elementi informativi emersi sono stati condivisi con le competenti questure, al fine di supportare e integrare gli approfondimenti svolti dalle D.I.G.O.S. e favorire una tempestiva valutazione delle possibili ricadute sul territorio. L'attività ha riguardato, in particolare, l'analisi dei profili coinvolti, delle interazioni tra account, dei contenuti pubblicati e delle eventuali iniziative annunciate o promosse negli ambienti digitali, con l'obiettivo di individuare tempestivamente indicatori di rischio e possibili sviluppi operativi.

Preme rappresentare come tutto il semestre sia risultato fortemente condizionato da manifestazioni di dissenso connesso all'evoluzione degli scenari geopolitici internazionali, con iniziative di piazza prevalentemente incentrate sulla crisi mediorientale, sul sostegno alla causa palestinese, sulle tensioni connesse all'intervento statunitense in Venezuela e, nel mese di febbraio, sulla contestazione dei giochi olimpici e paralimpici invernali di Milano-Cortina 2026.

Le mobilitazioni hanno interessato le principali città, attraverso cortei e presìdi promossi da movimenti studenteschi, collettivi antagonisti e associazioni, con rivendicazioni di carattere politico, sociale e ambientale.

Particolare rilievo hanno assunto le iniziative di protesta connesse a Milano-Cortina 2026, in particolare il corteo del 7 febbraio a Milano, durante il quale alle contestazioni relative all'impatto ambientale delle opere, ai costi dell'evento e alle politiche di sicurezza si sono affiancate rivendicazioni legate alla situazione internazionale. La manifestazione, inizialmente pacifica, è stata interessata da successivi episodi di tensione e da condotte violente che hanno richiesto l'intervento delle forze dell'ordine.

In tale contesto, il monitoraggio dell'ecosistema digitale ha costituito uno strumento di supporto all'individuazione delle iniziative annunciate online, alla ricostruzione delle dinamiche di mobilitazione e alla rilevazione di eventuali indicatori di rischio, in raccordo con le competenti articolazioni territoriali, ai fini della prevenzione di possibili criticità per l'ordine e la sicurezza pubblica.

Non ultimo, la crisi internazionale ha imposto il mantenimento di un'allerta massima sul fronte del terrorismo di stampo jihadista.
La propaganda jihadista online ha assunto molteplici diramazioni, con canali, riviste periodiche, contenuti multimediali, gruppi che vengono puntualmente analizzati per ricostruire le possibili proiezioni sul territorio nazionale. Queste componenti sono state altresì affiancate dal contrasto alla c.d. "*cyber jihad*", ossia quell'espressione radicale dell'hacktivismo che vede *crew* di *hacker* attivi nell'attacco a infrastrutture sensibili per motivazioni di carattere religioso; in tal senso l'azione ha consentito di comprendere collegamenti tra *crew*, tecniche di attacco, nonché di apprendere in anticipo le possibili campagne ostili.

Non connesso al contesto geopolitico, ma connotato da portata internazionale, risulta essere l'estremismo minorile, che di recente sta assumendo una crescente rilevanza nelle agende di tutti gli organismi di *law enforcement* a livello europeo e mondiale.

Il primo semestre del 2026 restituisce in particolare un quadro in cui i ragazzi – con specifico riferimento ai minori – tendono ad affacciarsi alla dimensione criminale in quanto fortemente influenzati da una narrativa incentrata sulla esaltazione della violenza, non riconducibile tuttavia ad un unico filone ideologico definito.
Tale andamento, con riguardo al periodo in esame, trova riscontro nei nove casi di attivazione emergenziale registrati e monitorati dal servizio polizia postale, tutti riferibili a soggetti minorenni, alcuni dei quali infraquattordicenni.

I dati acquisiti nel periodo di riferimento, pur non esaurendo la complessità e l'ampiezza del fenomeno, consentono tuttavia di evidenziare alcuni elementi ricorrenti, considerabili come indicatori significativi di un processo di radicalizzazione violenta e di devianza maturato in contesti digitali.
Tra gli elementi più significativi emergono il richiamo e l'esaltazione di stragi compiute negli ultimi anni in contesti occidentali – ipotesi di *school shooting* e manifestazioni di intenti violenti spesso maturati in contesti di marginalizzazione sociale, episodi di bullismo e condizioni di isolamento protratto.

Si riportano, in sintesi, le principali attività condotte o coordinate dalla sezione Cyberterrorismo nel I Semestre 2026:

- nel mese di marzo 2026 il C.O.S.C. Emilia-Romagna e la D.I.G.O.S di Ferrara hanno condotto un'indagine nei confronti di un uomo accusato di condividere contenuti discriminatori sul *web*. L'attività investigativa è scaturita da una segnalazione pervenuta al sito del Commissariato di P.S. *online* e ha permesso di raccogliere numerosi elementi relativi alla pubblicazione, all'interno di un gruppo Facebook, di *post* a sfondo razzista e antisemita che incitavano alla violenza, oltre a materiale apologe-

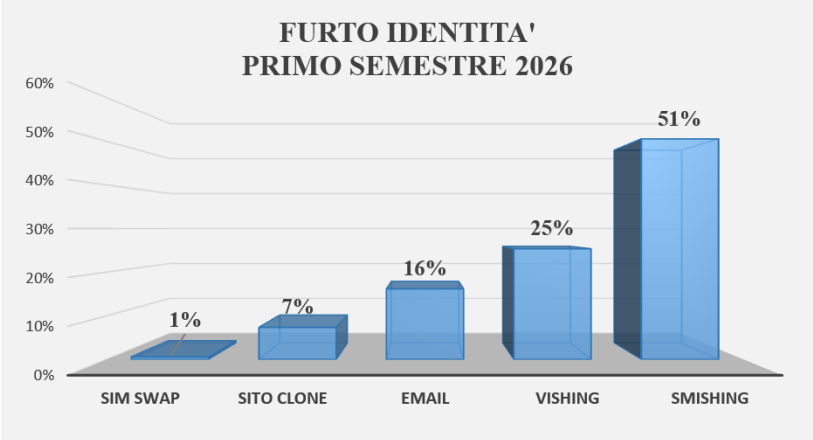
tico del nazismo e del fascismo, compresi ritratti di Hitler, Mussolini e immagini del campo di concentramento di Auschwitz.

- L'attività d'indagine si è conclusa con l'esecuzione di un decreto di perquisizione emesso dalla Procura di Ferrara che ha consentito di rinvenire e sequestrare, presso l'abitazione dell'uomo, armi, materiale propagandistico d'area e un chilogrammo di sostanze stupefacenti.
- L'uomo è stato arrestato e successivamente trasferimento presso la locale Casa circondariale;
- nel mese di marzo, personale del C.O.S.C e della D.I.G.O.S. di Perugia hanno dato esecuzione al decreto di perquisizione personale, locale e informatica emesso dalla Direzione Distrettuale Antimafia nei confronti di due cittadini marocchini e un tunisino residenti nel capoluogo umbro, indagati per i reati di cui agli artt. 270 bis c.p., 81 c.p.v. e 414 co. 2, 3 e 4 c.p., in quanto dediti al proselitismo e alla propaganda radicale jihadista e antioccidentale attraverso alcuni spazi social;
- operazione antiterrorismo "*Paint it Black*": nel mese di aprile il Servizio Polizia Postale e della Sicurezza Cibernetica, la D.C.P.P., il C.O.S.C. di Pescara e la D.I.G.O.S. della Questura di L'Aquila hanno eseguito un'ordinanza di custodia cautelare in carcere emessa dalla Procura Distrettuale Antimafia e Antiterrorismo di L'Aquila nei confronti di un venticinquenne cittadino italiano appartenente alla corrente anarchica di stampo primitivista e accelerazionista, per il delitto di addestramento con finalità di terrorismo, anche internazionale, e apologia di reato aggravata dalle finalità terroristiche. L'attività di indagine è scaturita da un meticoloso lavoro di monitoraggio del *web* che ha consentito di individuare il giovane, particolarmente attivo sia nella fruizione di contenuti propagandistici eversivi sui canali social, nonché nel reperire e archiviare, sui propri dispositivi, manuali tecnici dettagliati dedicati alla fabbricazione artigianale di ordigni esplosivi e istruzioni operative per la produzione di armi da fuoco mediante l'uso di stampanti 3D;
- nel mese di maggio il C.O.S.C. delle Marche, unitamente alla D.I.G.O.S. locale, hanno dato esecuzione a una perquisizione a carico di un minorenne indagato per i reati di cui agli artt. 342, 368, 414 e 612 bis c.p., nell'ambito di una più ampia indagine condotta unitamente a C.O.S.C. e D.I.G.O.S. di Torino su alcuni gruppi social di matrice neonazista, suprematista e antisemita, all'interno dei quali il giovane era particolarmente attivo nel pubblicare contenuti di esplicito incitamento all'odio e alla discriminazione razziale;
- nel mese di maggio il Servizio Polizia Postale, unitamente al C.O.S.C. di Genova e alla Direzione Centrale della Polizia di Prevenzione ha dato esecuzione ad un mandato di arresto europeo, emesso dal Giudice per le Indagini preliminari presso il Tribunale di Genova, nei confronti di un cittadino lettone. L'attività è scaturita

da una denuncia/querela presentata dal procuratore della società di navigazione "Grandi Navi Veloci" a seguito di un accesso abusivo a sistemi informatici rilevato a bordo di una motonave della flotta battente bandiera italiana. Gli accertamenti immediati hanno consentito di rilevare, a bordo della nave, la presenza di un dispositivo malevolo non autorizzato composto da un Raspberry e da un modem associato. Grazie ad un'attività di collaborazione internazionale, è stato possibile localizzare l'indagato in Spagna dove è stato tratto in arresto.

La Quarta Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica

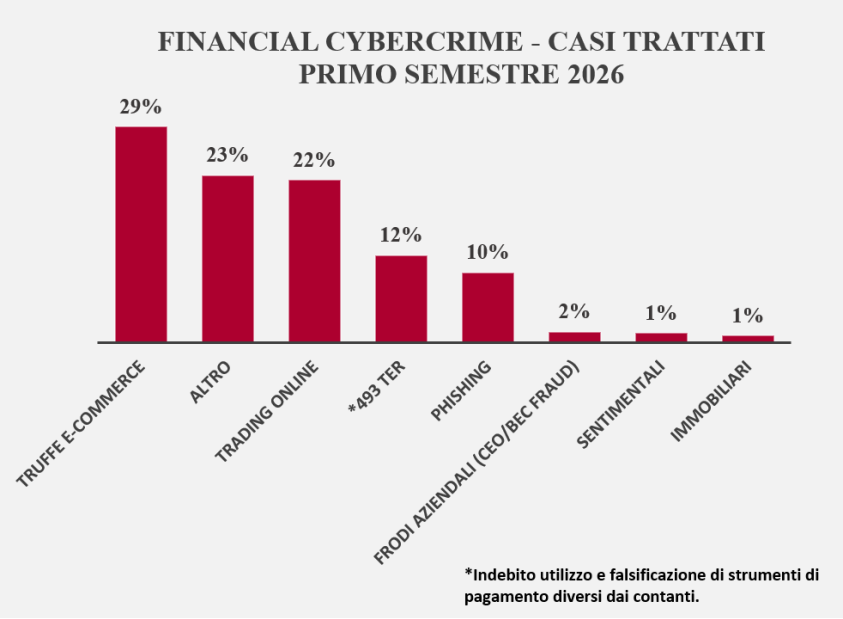
Nel primo semestre 2026, il *financial cybercrime* si conferma una delle principali forme di criminalità informatica, in crescita a livello globale. Le organizzazioni criminali utilizzano sempre più nuove tecnologie e intelligenza artificiale per rendere le frodi più sofisticate e credibili. Tra le tecniche più diffuse rimane il phishing, utilizzato per sottrarre credenziali bancarie e realizzare operazioni finanziarie illecite. Lo spoofing ha invece registrato un calo, anche grazie agli interventi dell'AGCOM, pur continuando a essere monitorato.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Ai danni delle imprese persistono soprattutto le frodi BEC e CEO Fraud, finalizzate a ottenere trasferimenti di denaro attraverso false comunicazioni aziendali. Un fenomeno in forte evoluzione è l'utilizzo dei deep fake, che permette di riprodurre immagini, video e voci di personaggi pubblici o dirigenti aziendali, rendendo più credibili le

truffe legate agli investimenti e ai trasferimenti di denaro. Particolare attenzione è rivolta anche alle criptovalute, il cui utilizzo e la cui complessità rendono più difficili le attività investigative, soprattutto nei casi di riciclaggio. La blockchain garantisce infatti trasparenza delle transazioni, ma anche un certo livello di pseudonimato. Infine, Internet continua a favorire contraffazione, pirateria e violazioni della proprietà intellettuale. Nel complesso, il documento evidenzia come il cybercrime sia sempre più organizzato, transnazionale e tecnologicamente avanzato, rendendo necessarie competenze specialistiche e una forte cooperazione internazionale.



© **2026** - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

L'analisi della distribuzione percentuale del *financial cybercrime* evidenzia una marcata eterogeneità nelle modalità operative adottate dai malintenzionati, con una netta prevalenza di illeciti legati al commercio elettronico e alle transazioni finanziarie online.

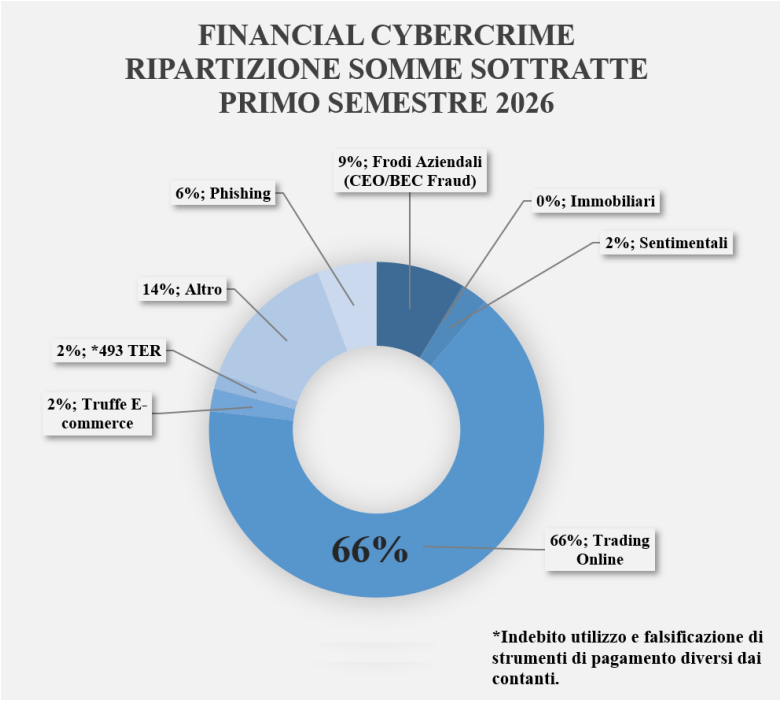
Truffa di natura commerciale e finanziaria: la categoria maggiormente rappresentata è costituita dalle truffe e-commerce, che da sole costituiscono il 29% del totale dei casi registrati colpendo una platea vastissima. A questa si affianca una quota rilevante legata al trading online (22%), a testimonianza di come i mercati finanziari digitali e

le piattaforme d'investimento rappresentino uno dei principali vettori di rischio per i risparmiatori. Nonostante questa truffa sia seconda come percentuale di casi trattati, rispetto all'e-commerce che è caratterizzata dalla sottrazione di cifre individuali relativamente basse in cui il danno per il singolo utente è circoscritto, nel falso trading online vengono presi di mira patrimoni accumulati negli anni, di conseguenza questa truffa assorbe i due terzi del danno finanziario complessivo.

Aggressioni ai sistemi di pagamento e phishing: le violazioni riconducibili all'indebito utilizzo e falsificazione di strumenti di pagamento (art. 493-ter c.p.) incidono per il 12%, mentre le attività di phishing rappresentano il 10% del totale. Tali evidenze confermano la persistenza e l'efficacia delle tecniche di ingegneria sociale mirate alla sottrazione di credenziali di accesso e dati sensibili.

Sebbene caratterizzate da frequenze percentuali inferiori, si rilevano fattispecie a elevata complessità o ad alto impatto socioeconomico, quali le frodi aziendali (CEO/BEC Fraud) (2%), le truffe di natura sentimentale (1%) e quelle in ambito immobiliare (1%). La ripartizione delle somme sottratte nel primo semestre 2026 evidenzia una forte concentrazione del danno economico nelle frodi connesse al trading online, responsabili del 66% degli importi complessivamente sottratti. Tale dato conferma la crescente capacità delle organizzazioni criminali di sfruttare falsi investimenti finanziari e piattaforme di trading fraudolente per indurre le vittime a effettuare versamenti di ingenti somme di denaro.

Seguono, con incidenze significativamente inferiori, le categorie residuali (14%), le frodi aziendali di tipo CEO/BEC Fraud (9%) e il phishing (6%), mentre truffe sentimentali, frodi e-commerce e altre fattispecie presentano percentuali più contenute. L'analisi mette in evidenza come, pur in presenza di una pluralità di schemi fraudolenti, il fenomeno del trading online continui a rappresentare la principale fonte di profitto per il cybercrime finanziario, assorbendo oltre due terzi delle risorse illecitamente sottratte nel periodo considerato.



© 2026 - Fonte Polizia Postale e per la sicurezza cibernetica – Settore Analisi e Pianificazione Strategica

Si riportano di seguito le attività più rilevanti realizzate nel corso del primo semestre 2026:

Truffa online nel settore autonoleggio

La Polizia Postale di Mantova ha denunciato due persone accusate di aver organizzato una truffa attraverso social network e piattaforme online. Una vittima aveva trovato su Facebook un'offerta di noleggio auto e aveva effettuato diversi bonifici, per un totale di oltre 4.000 euro, senza ricevere il veicolo. Gli indagati avrebbero creato una falsa attività di autonoleggio utilizzando siti web, profili social, numeri telefonici ed e-mail apparentemente riconducibili a società reali. Le indagini hanno inoltre collegato agli stessi soggetti altri episodi simili verificatisi in diverse province italiane.

Frode alle colonnine di ricarica elettrica

La Polizia Postale di Perugia ha denunciato tre persone accusate di aver utilizzato dispositivi elettronici per clonare i codici identificativi delle tessere RFID e ottenere

ricariche gratuite delle proprie auto elettriche. Le indagini, avviate dopo numerose segnalazioni di addebiti non riconosciuti, hanno portato a perquisizioni durante le quali sono stati trovati i dispositivi di clonazione e i relativi software. La frode avrebbe provocato un danno superiore a 10.000 euro.

Operazione "FAKE CHECK" a Foggia

La Polizia Postale di Foggia ha eseguito misure cautelari nei confronti di 20 persone, accusate di far parte di un'associazione dedita a truffe, riciclaggio e falsificazione di documenti e assegni. I criminali si presentavano come operatori bancari e convincevano le vittime a emettere assegni con il pretesto di proteggere i propri risparmi. Gli assegni venivano poi incassati attraverso conti fraudolenti. Le indagini hanno individuato truffe pianificate per oltre 750.000 euro e permesso di evitare la perdita di oltre 400.000 euro, successivamente restituiti alle vittime.

Truffa telefonica con falso SMS bancario

Un settantasettenne è stato vittima di una truffa basata su un falso SMS bancario. Contattando il numero indicato nel messaggio, è stato convinto da un falso operatore a effettuare un bonifico di 14.800 euro, necessario, secondo il truffatore, per bloccare una presunta frode. La S.O.S.C. di Crotone ha ricostruito i movimenti del denaro, individuato il conto destinatario e recuperato integralmente la somma, identificando il titolare del conto.

Ricettazione di materiale informatico a Foggia

La Polizia Postale di Foggia ha denunciato un uomo per la presunta ricettazione di un iPad e altri beni rubati a una donna. Grazie all'applicazione "Dov'è", la vittima ha potuto localizzare il dispositivo, consentendo agli agenti di recuperarlo insieme agli altri oggetti sottratti.

Frode informatica "Account Takeover"

La Polizia Postale del Lazio ha recuperato oltre 400.000 euro sottratti da conti correnti aziendali attraverso una frode di tipo Account Takeover (ATO). I criminali avevano ottenuto illegalmente le credenziali di home banking delle vittime e utilizzato i conti per effettuare numerosi bonifici. Il tempestivo intervento della Polizia ha permesso di bloccare e recuperare le somme, mentre proseguono le indagini per individuare tutti i responsabili.

La Quinta Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica

La Quinta Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica assicura il supporto tecnico e operativo alle attività istituzionali della Specialità, contribuendo al rafforzamento delle capacità investigative ed alla protezione delle infrastrutture It in uso. La sua azione integra ricerca, innovazione, programmazione delle risorse e sviluppo delle competenze, con l'obiettivo di tradurre l'evoluzione tecnologica in strumenti e metodologie concretamente utilizzabili dagli uffici centrali e territoriali nelle attività di contrasto al crimine informatico.

In tale ambito, la Divisione cura l'individuazione, la valutazione e l'acquisizione di tecnologie a supporto delle indagini nel settore del crimine informatico, dell'analisi delle evidenze digitali per il contrasto allo sfruttamento sessuale dei minori online etc. L'attività comprende, tra l'altro, l'analisi dei fabbisogni operativi, la pianificazione degli investimenti, la predisposizione delle procedure di acquisizione e la gestione dei rapporti contrattuali, assicurando coerenza tra esigenze investigative, sostenibilità delle scelte e requisiti di sicurezza. L'attività di coordinamento delle esigenze delle articolazioni territoriali costituisce una componente essenziale di questo impegno. In particolare, attraverso il confronto con gli uffici territoriali della Specialità, la Divisione raccoglie le necessità emergenti, favorisce la diffusione di metodologie condivise e sostiene il potenziamento delle capacità tecniche – investigative sull'intero territorio nazionale. Parallelamente, assicura la gestione e l'evoluzione delle infrastrutture informatiche del Servizio, la continuità dei servizi e il raccordo per l'accesso alle banche dati istituzionali e investigative, nel rispetto degli indirizzi formulati dall'Amministrazione e della normativa applicabile.

Nello specifico, tra i compiti principali della predetta divisione rientrano:

- fornire assistenza tecnica e operativa per l'attuazione delle attività d'Istituto in materia di sicurezza digitale, assicurando il necessario supporto alle strutture interessate;
- mantenere i rapporti con enti e istituzioni pubbliche e private, coinvolte nella ricerca e nell'innovazione scientifica, al fine di raccogliere informazioni aggiornate sulle nuove metodologie e sulle soluzioni tecnologiche più avanzate; inoltre partecipa alla definizione dei piani formativi specialistici;
- elaborare una pianificazione per l'acquisizione di sistemi IT, nonché predisporre la programmazione triennale dei fabbisogni con la conseguente gestione dei contratti di fornitura e delle procedure di acquisto;
- coordinare le articolazioni territoriali della Specialità nei settori tecnici di rispettiva

competenza, prendendo in considerazione l'analisi delle esigenze ed il supporto per la realizzazione di nuovi sistemi IT a sostegno delle attività investigative;
- gestire e implementare l'infrastruttura tecnologica del Servizio, attingendo agli indirizzi e alle politiche di sicurezza IT delineate dai competenti uffici della Polizia di Stato, in linea con gli standard e le normative di settore;
- svolgere la gestione completa degli asset tecnologici della Specialità a livello nazionale, assicurando il ruolo di focal-point per l'accesso alle banche dati istituzionali ed investigative in uso al Servizio.



In tema di Innovazione e Ricerca Tecnologica, presso la predetta divisione, è stato istituito **l'AILab@Cyber**, ovvero un laboratorio di ricerca nel settore dell'intelligenza artificiale per la cybersecurity. In particolare, il laboratorio provvede ad analizzare gli impatti del Regolamento Europeo sull'Intelligenza Artificiale (EU Reg.2024/1689) e della legge nazionale sull'IA (d. lgs.vo nr.132/2025 e nr.160/2026) in relazione allo sviluppo ed impiego di modelli e sistemi di IA idonei a supportare le attività investigative nel settore del contrasto al crimine informatico.

L'approccio adottato nella sperimentazione di tali tecnologie ha posto al centro l'affidabilità dei risultati, la tutela delle informazioni investigative, la supervisione umana e la possibilità di ricostruire le attività svolte dai sistemi. Al riguardo, la sperimentazione in ambienti controllati di tecnologie di IA rappresenta, in questa prospettiva, un passaggio fondamentale per accompagnare l'introduzione di nuove capacità operative. Tale approccio, infatti, consente di verificare preventivamente la sicurezza e l'adeguatezza delle soluzioni, definire procedure di utilizzo e individuare le misure necessarie prima della loro adozione nelle attività d'istituto. L'obiettivo è consolidare un percorso nel quale innovazione, verifica tecnica e conformità normativa procedano congiuntamente.

Nello specifico, nell'anno in esame, è stata avviata una specifica progettualità volta alla realizzazione di una infrastruttura It dedicata alla sperimentazione ed impiego di sistemi e modelli di intelligenza artificiale (c.d. Sandbox AI). Al completamento di detta infrastruttura, sarà possibile avviare, in un ambiente sicuro ed isolato dalla rete internet, alcune progettualità volte alla sperimentazione di modelli e sistemi di IA di frontiera a supporto delle investigazioni volte al contrasto del crimine informatico.

Al riguardo, sono state incentivate le collaborazioni con Università, Enti di ricerca, Aziende e altri interlocutori istituzionali con l'obiettivo di favorire il trasferimento delle conoscenze dal contesto della ricerca a quello operativo. A tali attività, è stata affiancata, altresì, una progettualità volta all'analisi delle nuove modalità di impiego criminale dell'IA, al fine di individuare tempestivamente le priorità di intervento, investimento e formazione.

Il ruolo della V Divisione è stato rafforzato anche in ambito internazionale attraverso il rilevante contributo tecnico-specialistico fornito nei consessi europei e multilaterali, che ha consentito di condividere esperienze operative nonché partecipare alla definizione di indirizzi comuni per l'innovazione tecnologica nelle attività di polizia. In tale quadro si colloca la partecipazione al gruppo G7 Roma-Lione, sottogruppo High Tech Crime, nell'ambito dei cui lavori sono stati approfonditi i temi concernenti l'accesso legittimo alle evidenze digitali e l'impiego criminale delle tecnologie di intelligenza artificiale.

Gli ulteriori incarichi svolti dalla Divisione nell'ambito dell'European Clearing Board e del relativo Governing Board nonché il ruolo di Presidenza ricoperto nel gruppo di lavoro sui sistemi di identificazione biometrica, hanno contribuito a qualificare la presenza italiana della Polizia di Stato e del Dipartimento della P.S. nei processi europei di sviluppo delle capacità investigative. Inoltre, la partecipazione ai gruppi dedicati alla strategia sull'IA, alla spiegabilità dell'IA, alle applicazioni avanzate dell'intelligenza artificiale, nonché al gruppo di esperti della Commissione europea per il settore degli affari interni, ha offerto ulteriori occasioni per raccordare esigenze operative, ricerca e garanzie giuridiche

Per quanto riguarda le dotazioni tecnologiche a supporto delle investigazioni, si è provveduto a dare particolare impulso all'avvio di un rilevante programma di potenziamento sia hardware che software, anche in ragione del rilevante incremento di organico avuto dalla Specialità nell'anno in esame. Tale rilevante programma di potenziamento ha consentito, altresì, di acquisire soluzioni di digital forensics di ultima generazione. In particolare, sono state acquisite/rinnovate:

- tecnologie avanzate per supportare le attività di digital forensics mediante la fornitura di nuove apparecchiature hardware ad elevate prestazioni nonché tecnologie software per l'acquisizione e l'analisi forense di dispositivi digitali;
- strumentazioni di ultima generazione volte all'analisi degli incidenti informatici;
- piattaforme di servizi info-investigativi atte a supportare le attività d'indagine;
- postazioni di lavoro fisse e mobili per soddisfare le esigenze degli uffici territoriali e centrali;
- sistemi ed infrastrutture per erogare e servire sistemi di intelligenza artificiale.

Significativi gli sforzi della Divisione in ambito formativo. In particolare, sono stati realizzati nuovi moduli formativi in tema di digital forensics ed intelligenza artificiale per la cyber security e le investigazioni cyber.

Ulteriori aspetti trattati hanno riguardato le tematiche di awareness concernenti l'uso corretto e responsabile delle tecnologie di IA, affrontando anche la tematica concernente benefici e possibili rischi associati all'uso non corretto di dette tecnologie. Tali moduli formativi sono stati resi disponibili al personale della Polizia di Stato in vari ruoli direttivi e non direttivi.

I percorsi formativi sviluppati nel settore dell'impiego dell'IA sono stati affiancati dall'approfondimento tecnico su tali tecnologie nonché sulla consapevolezza dei rischi, delle responsabilità e delle condizioni di impiego di tali innovative tecnologie. Particolare attenzione è stata dedicata all'uso corretto dell'IA, alla valutazione critica dei risultati prodotti da tali sistemi e alla tutela delle informazioni trattate, con iniziative rivolte sia al personale specialistico sia ai ruoli direttivi chiamati a orientarne l'introduzione e l'utilizzo. Per il nuovo anno, è previsto un impegno ancora più rilevante volto al consolidamento delle conoscenze nonché allo sviluppo di progettualità che prevedono l'impiego dell'intelligenza artificiale a supporto delle investigazioni. Il programma comprenderà lo sviluppo di tool destinati agli uffici centrali e territoriali e la definizione delle procedure necessarie per un impiego sicuro, controllato e coerente con le finalità istituzionali.

In ultimo, va ricordato che la progressiva applicazione degli obblighi previsti dal Regolamento europeo sull'intelligenza artificiale e dalla disciplina nazionale renderà centrale il lavoro di adeguamento dei processi di acquisizione, sperimentazione e utilizzo dei sistemi di IA, in particolare di quelli ad alto rischio. Al riguardo, la Divisione dedicherà specifica attenzione alla valutazione dei rischi, alla definizione delle responsabilità, alla documentazione delle attività svolte e alle misure di supervisione, secondo gli obblighi e le scadenze previste dalla normativa di settore. La sicurezza informatica e delle informazioni costituirà una parte integrante di questo percorso, con particolare riguardo alla protezione dei dati investigativi, al controllo degli accessi, alla tracciabilità delle operazioni e alla gestione delle vulnerabilità e degli incidenti.

Sicurezza e frodi informatiche in Banca

[A cura di Maria Ferrucci, CERTFin]

Il Report "Sicurezza e Frodi Informatiche in Banca" viene realizzato annualmente dal CERTFin - CERT (Computer Emergecy Response Team) Finanziario Italiano - e fornisce una fotografia aggiornata del livello di rischio cyber e delle frodi e truffe informatiche nel settore finanziario italiano allo scopo di aiutare banche e operatori finanziari a comprendere l'evoluzione delle minacce e dove rafforzare prevenzione, controlli e investimenti.

A seguire si riportano i principali contenuti del Rapporto 2026, che raccoglie i dati segnalati da 35 organizzazioni rappresentative di oltre il 90% del settore.

Iniziative di awareness, formazione e investimenti

Dalla rilevazione emerge una progressiva diffusione della cultura della sicurezza all'interno dell'intera organizzazione. La formazione "interna" su frodi e attacchi informatici coinvolge ormai in modo sistematico il personale di filiale (100% dei rispondenti) e, con livelli molto elevati, anche i team specialistici di sicurezza, il Top Management, l'Help Desk, il Back Office e il Contact Center, consolidando l'attenzione verso le strutture maggiormente esposte al rapporto con la clientela e alla gestione degli eventi operativi più sensibili.

Oltre alla formazione "interna", gli istituti rivolgono particolare attenzione alle iniziative di sensibilizzazione verso la clientela. L'analisi delle tematiche affrontate mostra una forte concentrazione sui contenuti più direttamente collegati ai meccanismi di frode oggi prevalenti, tra cui social engineering, uso sicuro degli strumenti di pagamento e rischi legati agli investimenti online. Anche la frequenza delle iniziative è significativa: il 78% delle organizzazioni sul segmento delle persone fisiche (c.d. "Retail") e il 69% sul segmento delle imprese (c.d. "Corporate") realizzano attività con frequenza inferiore ai sei mesi.

Il 77% degli istituti ha attivato, inoltre, formazione o sensibilizzazione verso i fornitori ICT, con temi più legati alla relazione tra terza parte e istituto: dall'identificazione e segnalazione degli incidenti, alla protezione dei dati e ai requisiti di sicurezza, fino a normativa di settore, continuità operativa e disaster recovery.

Il peso strategico che il tema della sicurezza riveste per il settore finanziario è confermato anche dal livello degli investimenti, con una quota media di spesa IT dedicata alla sicurezza pari al 6,45% nel 2025 e una stima dell'8% per il 2026. Aumenta, inol-

tre, il budget di sicurezza destinato alla prevenzione e al contrasto delle frodi, con il 13,5% del totale della spesa IT.

Il report 2026 ha per la prima volta approfondito i principali ambiti tecnologici sui quali si concentreranno prevalentemente le iniziative di investimento in materia di cybersicurezza e resilienza operativa nel prossimo biennio (**Figura 1**): emerge che gli investimenti in cybersicurezza si concentreranno soprattutto su resilienza operativa digitale, soluzioni antifrode e gestione delle identità.

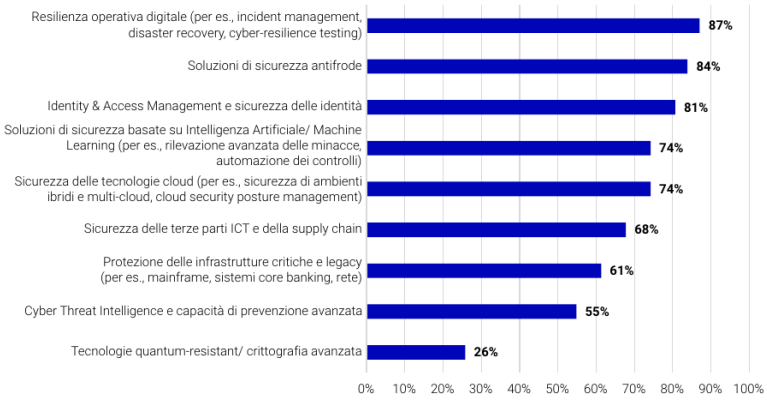


Figura 1 - Principali ambiti tecnologici di investimento nel prossimo biennio *(Fonte: CERTFin, Report Sicurezza e frodi informatiche in banca, maggio 2026)*

Dimensionamento delle frodi e strumenti di pagamento

Tra gli strumenti di pagamento preferiti dai frodatori per la realizzazione dell'attacco, nel segmento Retail il bonifico istantaneo nazionale è il principale (40% dei tentativi di frode in termini di numerosità), seguito dal bonifico ordinario nazionale (30%). Nel segmento delle imprese, invece, il bonifico ordinario nazionale prevale con il 53% degli eventi anomali registrati dal campione. Con riferimento all'efficacia dell'attacco (rapporto tra operazioni effettive e totale transazioni anomale), il bonifico istantaneo nazionale presenta una quota di operazioni effettive più alta rispetto all'ordinario, sia nel segmento Retail che nel Corporate.

Le vittime "più mature" (oltre i 45 anni) rappresentano oltre il 70% del totale, con gli over 60 al 43%, mentre le microimprese vengono colpite in oltre la metà degli attacchi.

Guardando all'efficacia dei presidi di prevenzione e contrasto, emerge che la quota prevalente delle transazioni anomale viene intercettata prima che possa produrre effetti economici, sia con riferimento alla numerosità che agli importi economici associati agli eventi, come si evince dalla **Figura 2**. Si registra, inoltre, un forte aumento degli importi recuperati, che crescono di oltre il 50% passando da 23 a 35 milioni di euro, anche grazie al Protocollo di collaborazione antifrode tra PSP italiani attivato dal CERTFin nel 2020.

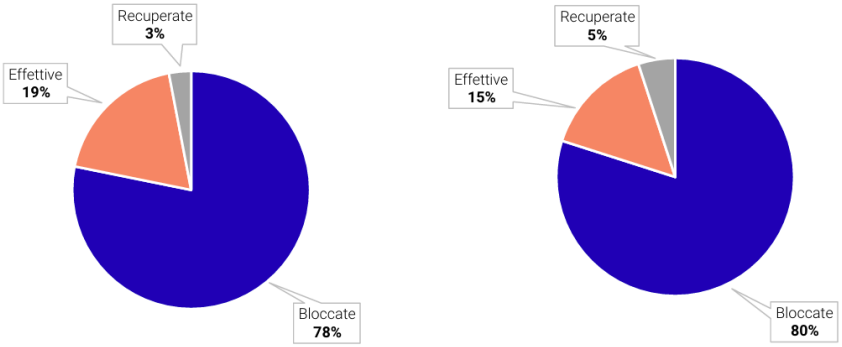


Figura 2 - Ripartizione percentuale delle tipologie di transazioni anomale (bloccate, recuperate ed effettive) – analisi sul numero di accadimenti (complessivo Retail e Corporate) (*Fonte: CERTFin, Report Sicurezza e frodi informatiche in banca, maggio 2026)*

Inoltre, le transazioni anomale si concentrano nettamente sul segmento Retail, che rappresenta la quasi totalità degli eventi (95%) e la maggior parte degli importi (84%). Il Corporate, pur incidendo molto meno in termini di numerosità, presenta tuttavia transazioni mediamente di valore più elevato.

Le transazioni fraudolente mostrano, infine, una crescente dimensione internazionale. All'interno dello Spazio Economico Europeo (SEE), Malta emerge come principale destinazione, seguita da Lituania e Germania, mentre fuori dallo SEE prevale il Regno Unito, seguito da Svizzera e Stati Uniti. Particolarmente significativo è l'aumento degli importi diretti all'estero, più che raddoppiati rispetto all'anno precedente (113 milioni di euro). Si segnala la necessità, pertanto, di una maggiore collaborazione transfrontaliera.

© Clusit 2026

Dinamiche e modalità operative delle frodi informatiche

Con un trend in aumento rispetto all'anno precedente, anche nel 2025 si conferma la prevalenza della manipolazione del pagatore tra le modalità operative di realizzazione della frode (81% nel Retal e 70% nel Corporate). Tale tecnica prevede un'attività manipolatoria posta in essere dal frodatore ai danni del pagatore, finalizzata a indurlo a emettere in buona fede un ordine di pagamento o a impartire un'istruzione di pagamento verso un conto che egli ritiene appartenere a un beneficiario legittimo. Emissione di un ordine di pagamento da parte del frodatore e modifica di un ordine legittimo (entrambe "operazioni non autorizzate" compiute direttamente dal frodatore) occupano rispettivamente il 18% e l'1% nel Retail e il 24% e il 6% nel segmento delle imprese.

Per quanto riguarda i canali o vettori di primo contatto, nel Retail il 46% delle frodi effettive origina ancora da telefonate e SMS, ma il dato è in calo rispetto a circa il 60% della rilevazione precedente e all'87,5% di due anni prima. Le chiamate telefoniche, invece, pesano per il 36% del totale: 24% riconducibile a spoofing del numero chiamante, 9% a spoofing di numeri verdi e 3% a chiamate senza alterazione. Gli SMS incidono per il 10%, metà dei quali con alias falsificato. Al di fuori del canale telco, i social media raggiungono il 22% e le instant messaging app il 10%, confermando uno spostamento verso ambienti meno "controllabili" dal prestatore di servizi di pagamento (psp). Sempre più si manifesta, quindi, l'esigenza di rafforzare la collaborazione tra più settori nel contrasto alle frodi e truffe digitali.

La finalizzazione delle frodi Retail è dominata dal social engineering (ingegneria sociale o impersonificazione), schema che prevede lo sfruttamento di leve emotive, urgenza, pressione psicologica e fiducia artificiale per manipolare le vittime e realizzare la frode, con il 77% dei casi. Di questi i falsi investimenti costituiscono la tipologia più ricorrente (36%), seguiti dai task scam (25%), come rappresentato in **Figura 3**.

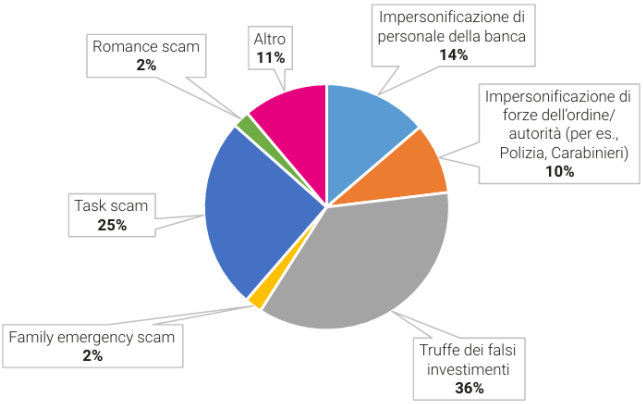


Figura 3 - Distribuzione degli eventi fraudolenti di social engineering nel segmento Retail *(Fonte: CERTFin, Report Sicurezza e frodi informatiche in banca, maggio 2026)*

Nel segmento Corporate il social engineering rappresenta il 37%, mentre la BEC (Business E-mail Compromise), occupa il 23% delle tecniche. Quest'ultima fattispecie è tipica degli attacchi perpetrati verso le imprese, in quanto la finalizzazione della frode si realizza generalmente attraverso l'alterazione o l'intercettazione delle comunicazioni aziendali, allo scopo di indurre l'impresa a eseguire pagamenti verso coordinate fraudolente, sovente nell'ambito di rapporti commerciali apparentemente legittimi. La differenza tra i segmenti suggerisce due diverse superfici di rischio tra i due comparti di clientela: persuasione diretta della persona nel Retail e compromissione dei processi comunicativi e autorizzativi nel Corporate.

Infine, dalla rilevazione del CERTFin emerge che il 96% delle frodi effettive risulta eseguito con Strong Customer Authentication (SCA) correttamente completata, mettendo in evidenza che i presidi di autenticazione forte non vengono elusi in senso tecnico, bensì risultino inefficaci in presenza di un cliente già manipolato e indotto ad autorizzare l'operazione.

Meccanismi di rilevazione e contrasto alle frodi

Tra i metodi adottati per l'individuazione e la segnalazione delle frodi, il controllo delle transazioni effettuato direttamente dalla banca (transaction monitoring interno) continua a rappresentare il principale strumento attraverso il quale vengono inter-

cettate disposizioni di pagamento anomale o fraudolente (57% nel Retail e 58% nel Corporate). Il disconoscimento delle operazioni da parte dei clienti rimane il secondo canale più utilizzato per l'individuazione delle frodi, mentre filiali, canali di infosharing settoriale e servizi di segnalazione specifici acquistati da soggetti terzi rappresentano ulteriori fonti di segnalazione sono rappresentate.

Per quanto riguarda gli strumenti utilizzati per valutare la legittimità delle operazioni all'interno dell'organizzazione, dalla rilevazione emerge che la maggior parte degli istituti tende a utilizzare almeno dieci indicatori differenti nella valutazione delle operazioni, tra cui indirizzi IP, browser e identificativi dei device (93% dei rispondenti), seguiti dalla tipologia di dispositivo, dal Paese destinatario della transazione e dalla presenza di un nuovo beneficiario (87% dei rispondenti).

Con riferimento agli strumenti tecnologici adottati dalle organizzazioni per monitorare e individuare potenziali attacchi informatici diretti verso la propria clientela, ai primi due posti figurano monitoraggio delle transazioni anomale effettuate tramite Internet banking e tramite mobile app. Interessante, inoltre, menzionare l'utilizzo di tecnologie di Artificial Intelligence, alla base – in media – del 25% di tali strumenti.

Infine, rispetto alle contromisure utilizzate per limitare le frodi sui bonifici ordinari e istantanei, emerge un quadro caratterizzato da un ampio ricorso a presidi di prevenzione e intercettazione con un livello di adozione sostanzialmente elevato, che vede al primo posto il blocco delle operazioni verso IBAN segnalati come sospetti, indicato dalla quasi totalità dei rispondenti, seguito dagli alert verso il cliente e dall'applicazione di limiti operativi (**Figura 4**).

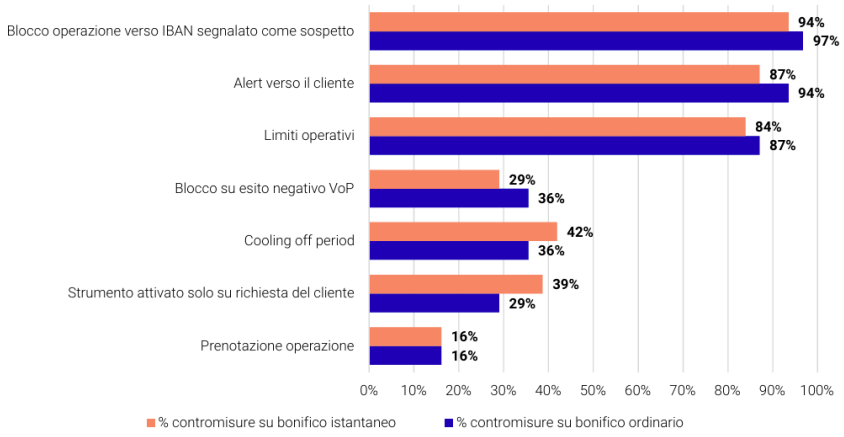


Figura 4 - Distribuzione contromisure bonifici ordinari e istantanei *(Fonte: CERTFin, Report Sicurezza e frodi informatiche in banca, maggio 2026)*

Cybersecurity

La sezione cybersecurity evidenzia una riduzione di alcune minacce "classiche" e, parallelamente, un aumento del rischio "indiretto". Nel 2025 sono stati rilevati infatti 76 data breach, con una crescita del 27% rispetto all'anno precedente. In particolare, il 31% delle organizzazioni dichiara di avere subito un breach diretto, contro il 23% della precedente rilevazione, mentre il 35% segnala almeno un breach indiretto riconducibile a fornitori o supply chain. Tale dato sottolinea la necessità di estendere i controlli sull'intera catena di fornitura.

Per quanto riguarda la distribuzione degli incidenti (**Figura 5**), il social engineering, incluso il phishing, è al primo posto con quasi la metà degli accadimenti, seguito dagli attacchi DDoS. La prevalenza della dinamica dell'ingegneria sociale anche tra gli incidenti cyber conferma che il fattore umano attraversa sia la dimensione delle frodi sia quella della sicurezza informatica tradizionale.

© Clusit 2026

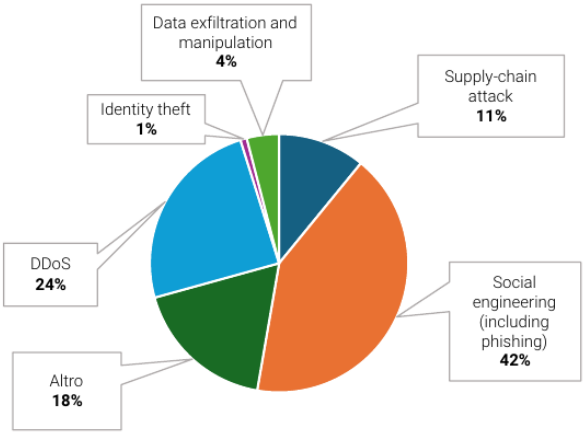


Figura 5 -Distribuzione degli incidenti di sicurezza rilevati nel campione *(Fonte: CERTFin, Report Sicurezza e frodi informatiche in banca, maggio 2026)*

Sul fronte dei DDoS, il 70% degli istituti dichiara di avere rilevato almeno un attacco. Tuttavia, gli attacchi classificati come "gravi" scendono però a due casi, anche grazie al fatto che il 97% disponeva già nel 2025 di contromisure tecnologiche volte a mitigare tali attacchi e che il 70% le ha rafforzate nel corso del 2025.

Nel campione non risultano infezioni ransomware, a fronte del 7% della rilevazione precedente, e non vengono registrati terminali o server danneggiati da ransomware. Il report invita comunque a leggere il dato con cautela, in quanto l'assenza di eventi nel campione non implica la scomparsa della minaccia e può convivere con una riallocazione dell'azione criminale verso fornitori e soggetti della supply chain.

Infine, per la prima volta all'interno del Report viene approfondita anche la dimensione geopolitica del rischio cyber, in considerazione della crescente instabilità dello scenario internazionale. Tra i dati più significativi, emerge che il 56% degli istituti ha integrato il rischio cyber geopolitico nei propri processi di risk assessment e che il 90% delle organizzazioni dispone di un processo strutturato di threat intelligence volto a presidiare le minacce di natura geopolitica.

Conclusioni

Nel complesso, la rilevazione CERTFin 2026 evidenzia un settore bancario che intercetta una quota elevata delle transazioni anomale e investe in modo crescente nel rafforzamento della sicurezza digitale. Il principale cambio di paradigma riguarda però la natura dell'attacco: la tecnologia continua a essere essenziale, ma una parte sempre più rilevante delle perdite nasce da operazioni correttamente autenticate e volontariamente autorizzate da clienti manipolati. È sempre più necessaria, quindi, una risposta coordinata che coinvolga non solo le organizzazioni del settore ma anche clienti, fornitori e altri settori.

© Clusit 2026

Analisi dei principali incidenti cyber noti del primo semestre 2026 verso il settore Manufacturing a livello globale e in Italia

Il settore Manufacturing continua a rappresentare uno degli ambiti maggiormente esposti alla crescente pressione delle minacce cyber e, vista la sua criticità, è sempre oggetto di una valutazione dedicata sul nostro aggiornamento annuale.

In questa analisi, presentiamo alcuni dati a complemento del Rapporto Clusit 2026 considerando gli incidenti cyber noti, divenuti di pubblico dominio nel primo semestre dell'anno e li confrontiamo con l'andamento osservato nel periodo 2018-2025. L'analisi distingue, come sempre, lo scenario globale da quello italiano e prende in considerazione non soltanto il numero degli incidenti, ma anche la tipologia di attaccante, le tecniche utilizzate, la distribuzione geografica delle vittime e la severity degli eventi in modo da ricomporre un quadro completo a disposizione di tutti gli esperti di settore.

Le due tabelle permettono innanzitutto di cogliere la progressiva crescita del fenomeno. A livello globale, gli incidenti di sicurezza noti verso il settore Manufacturing sono passati dai 34 casi del 2018 ai 400 del 2025; val la pena notare che, nel solo primo semestre 2026, ne sono già stati registrati 267.

A livello Global, la situazione è la seguente:

ATTACCANTI	2018	2019	2020	2021	2022	2023	2024	2025	H1 2026	TOTALE
Cybercrime	21	24	58	68	116	149	212	376	260	1284
Hacktivism	0	0	0	0	4	7	20	11	1	43
Information Warfare	3	0	1	0	0	0	0	9	6	19
Espionage / Sabotage	10	12	6	4	9	6	4	4	0	55
Totale per anno	34	36	65	72	129	162	236	400	267	1401
Totale attacchi per anno	1554	1667	1874	2049	2489	2779	3771	5275	4911	26369

ATTACCANTI	2018	2019	2020	2021	2022	2023	2024	2025	H1 2026	TOTALE
% attacchi su Totale dell'anno	2.2%	2.2%	3.5%	3.5%	5.2%	5.8%	6.3%	7.6%	5.4%	5.3%
% Crescita anno su anno	0.0%	0.0%	0.0%	0.0%	79.2%	25.6%	45.7%	69.5%		

A livello Italia, la stessa tabella, presenta una situazione differente:

ATTACCANTI	2018	2019	2020	2021	2022	2023	2024	2025	H1 2026	TOTALE
Cybercrime	0	0	8	12	35	41	54	62	44	256
Hacktivism	0	0	0	0	0	0	4	1	1	6
Espionage / Sabotage	2	2	1	0	0	0	0	0	0	5
Information Warfare	0	0	0	0	0	0	0	0	0	0
Totale per anno	2	2	9	12	35	41	58	63	45	267
Totale attacchi per anno ITA	30	37	48	70	188	310	373	507	245	1808
% attacchi su Totale dell'anno	6.7%	5.4%	18.8%	17.1%	18.6%	13.2%	15.5%	12.4%	18.4%	2.5%
% Crescita anno su anno	0.0%	0.0%	0.0%	0.0%	191.7%	17.1%	41.5%	8.6%		

Nelle tabelle è stata calcolata la percentuale di crescita anno su anno, portando a 0% il 2018.

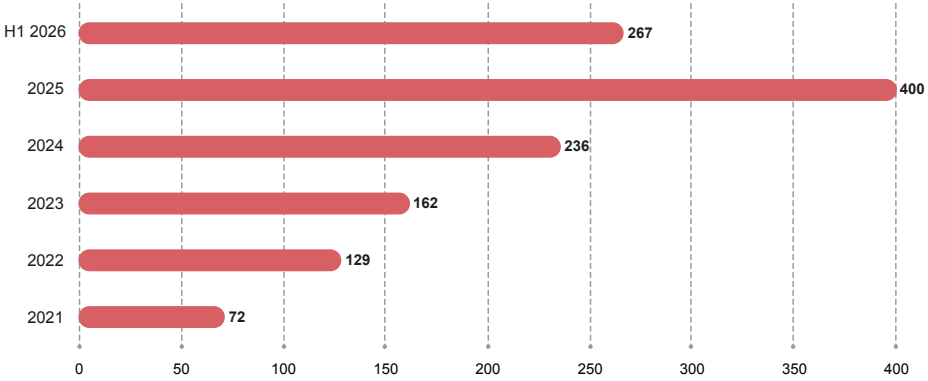
Pur con tutte le cautele necessarie quando si proietta su base annua un dato semestrale, mantenendo lo stesso ritmo, il 2026 potrebbe quindi superare i 530 incidenti nel settore con un incremento di oltre il 30% rispetto al 2025.

È interessante, tuttavia, osservare contemporaneamente anche il peso relativo al settore del Manufacturing sul totale pari al 7,6% degli incidenti globali occorsi nel 2025

mentre rappresenta il 5,4% nel primo semestre 2026. Attenzione perché questo non indica necessariamente una diminuzione dell'esposizione del comparto! Infatti, gli incidenti Manufacturing stanno aumentando in valore assoluto, mentre l'intero fenomeno cyber cresce ad un ritmo ancora più elevato.

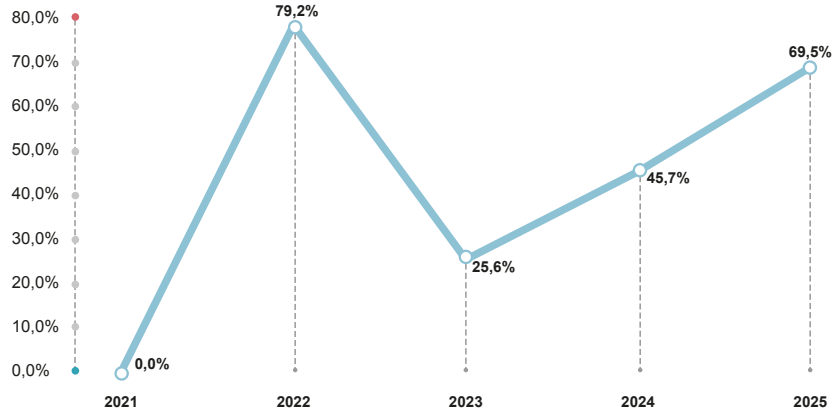
In altre parole, il rischio industriale cresce all'interno di un ecosistema di minacce che sta crescendo ancora più velocemente.

Incidenti Cyber Manufacturing 2021 - H1 2026



© Clusit - Rapporto 2026 sulla Cybersecurity

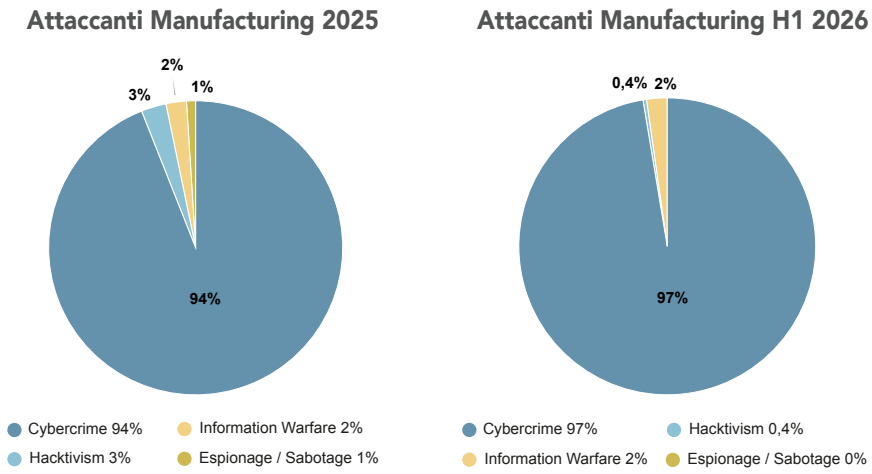
Manufacturing crescita % anno su anno



© Clusit - Rapporto 2026 sulla Cybersecurity

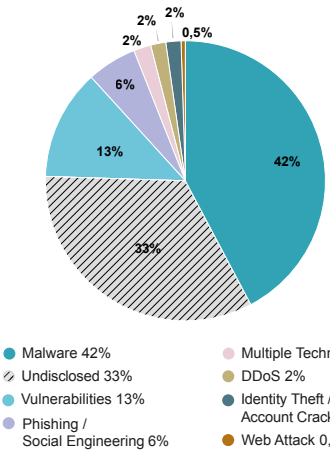
Il Cybercrime si conferma con chiarezza la motivazione principale degli incidenti inerenti al settore Manufacturing. Nel primo semestre 2026, sono riconducibili a questa categoria 260 dei 267 episodi osservati a livello globale, mentre Hacktivism, Information Warfare ed Espionage/Sabotage rimangono complessivamente residuali con la categoria di Hacktivism in sensibile discesa.

Il dato potrebbe suggerire una considerazione importante legata al fatto che il settore industriale non venga colpito soltanto per il proprio valore strategico, tecnologico o geopolitico, ma soprattutto perché economicamente monetizzabile. Per un'impresa manifatturiera, infatti, l'indisponibilità dei sistemi di produzione potrebbe tradursi rapidamente nel fermo delle linee produttive, in ritardi nelle consegne o perdita di capacità operativa con pesanti conseguenze e ripercussioni lungo la supply chain. È proprio questa forte dipendenza dalla continuità operativa dei processi industriali a rendere il Manufacturing particolarmente appetibile per un cybercrime sempre più organizzato ed orientato al ritorno economico.

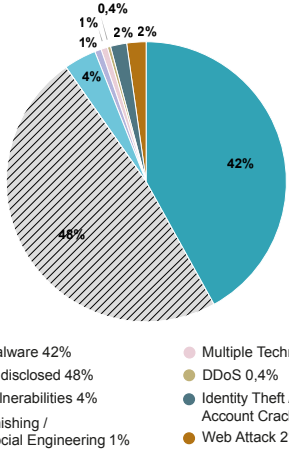


© Clusit - Rapporto 2026 sulla Cybersecurity

Tecniche attacco Manufacturing 2025



Tecniche attacco Manufacturing H1 2026



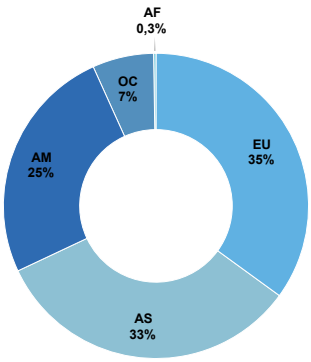
© Clusit - Rapporto 2026 sulla Cybersecurity

Il malware continua a rappresentare una componente centrale nel settore: nel 2025 pesava per il 42% e mantiene la stessa quota nel primo semestre 2026 con una stabilità che mostra come la "pesca" del malware sia meno onerosa ma renda sempre. Parallelamente diminuiscono gli episodi attribuiti direttamente allo sfruttamento di vulnerabilità, dal 13% al 4%, mentre cresce sensibilmente la categoria Undisclosed, che raggiunge il 48%.

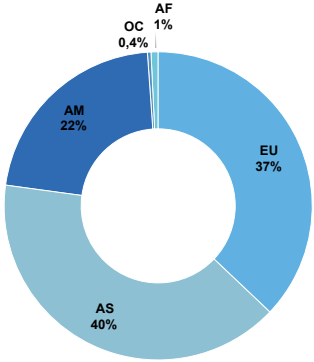
Quest'ultimo dato richiede, ancora una volta, particolare cautela nell'interpretazione, poiché una quota così elevata di incidenti per i quali la tecnica di attacco non sia pubblicamente disponibile limita la possibilità di ricostruire con precisione la catena di compromissione. Inoltre, come ben sappiamo, la tecnica rilevata o resa pubblica non coincide necessariamente con il vettore iniziale dell'attacco: il malware o il ransomware possono costituire soltanto la fase maggiormente visibile di una compromissione iniziata attraverso credenziali sottratte, social engineering, servizi esposti o sfruttamento di vulnerabilità.

La fotografia delle tecniche deve quindi essere letta come rappresentazione di ciò che è stato possibile osservare e classificare, non necessariamente dell'intera superficie di attacco.

Geografia vittime Manufacturing 2025



Geografia vittime Manufacturing H1 2026

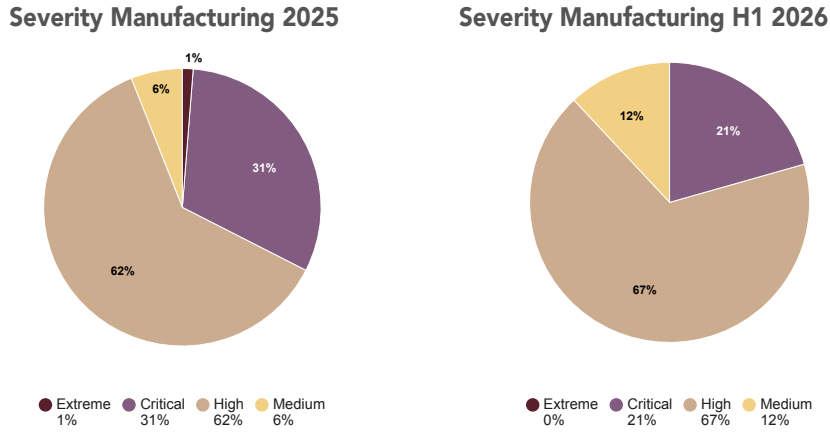


© Clusit - Rapporto 2026 sulla Cybersecurity

Dal punto di vista geografico, la distribuzione degli incidenti mostra nel primo semestre 2026 uno spostamento del baricentro verso l'Asia che passa dal 33% del 2025 al 40% e diventa l'area maggiormente rappresentata. L'Europa cresce leggermente dal 35% al 37%, mentre le Americhe scendono dal 25% al 22%. La distribuzione appare quindi meno equilibrata rispetto al 2025 con Asia ed Europa che insieme concentrano oltre tre quarti degli eventi osservati.

Anche questi valori devono essere interpretati considerando la differente disponibilità di informazioni pubbliche nelle diverse aree geografiche. Il dato conferma tuttavia un elemento strutturale: il rischio cyber industriale è ormai pienamente globale e, per il Manufacturing, questo assume particolare rilevanza perché le catene di approvvigionamento sono sempre più interconnesse e la superficie di rischio di un'impresa non coincide più soltanto con il suo perimetro tecnologico diretto, ma tende ad estendersi all'intera catena del valore.

Sul fronte degli impatti emerge un segnale apparentemente positivo con la contrazione degli incidenti classificati come Critical scesi dal 31% del 2025 al 21% del primo semestre 2026. Va notato tuttavia che gli eventi classificati come High salgono dal 62% al 67% e quindi la diminuzione degli eventi più estremi non può essere interpretata automaticamente come una riduzione del rischio visto che la maggioranza degli attacchi continua a produrre conseguenze elevate.

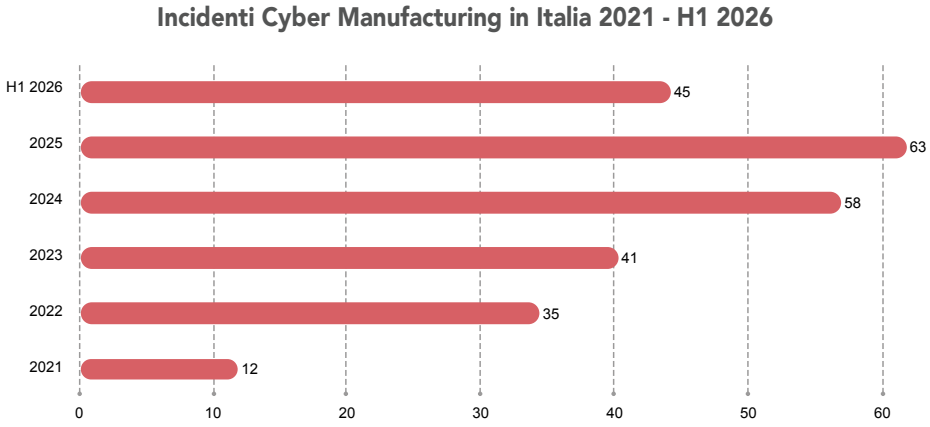


© Clusit - Rapporto 2026 sulla Cybersecurity

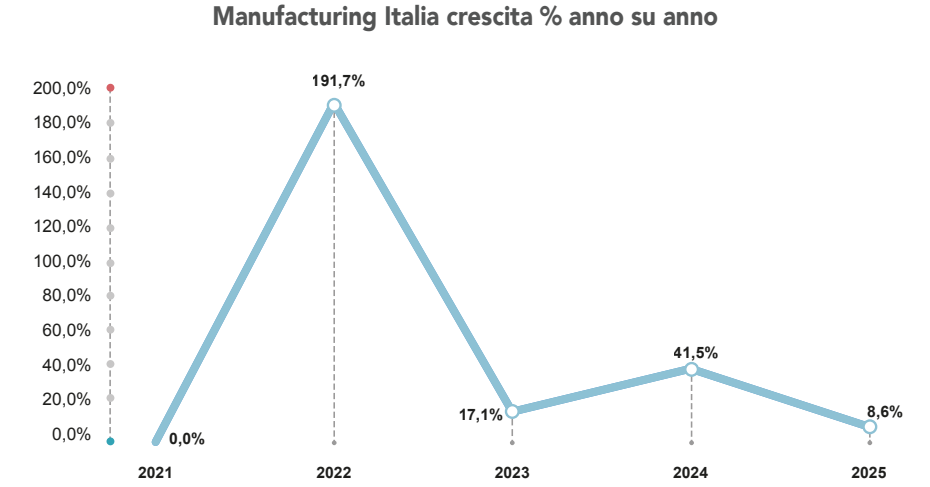
Come già sottolineato più volte dal CLUSIT, il dato sottolinea ancora una volta come sia fondamentale non solo la capacità di prevenire gli incidenti, ma anche la capacità di contenerne gli impatti. E, per il settore del Manufacturing, siano quindi centrali non soltanto protezione e detection, ma anche governance, segmentazione degli ambienti, business continuity, disaster recovery e gestione coordinata della crisi.

Il quadro italiano presenta alcune caratteristiche peculiari.

Nel primo semestre 2026 sono stati registrati 45 incidenti nel settore Manufacturing su 245 complessivi, pari al 18,4% del campione osservato nel Paese. Nel 2025 erano stati 63 su 507 con un'incidenza del 12,4%.



© Clusit - Rapporto 2026 sulla Cybersecurity

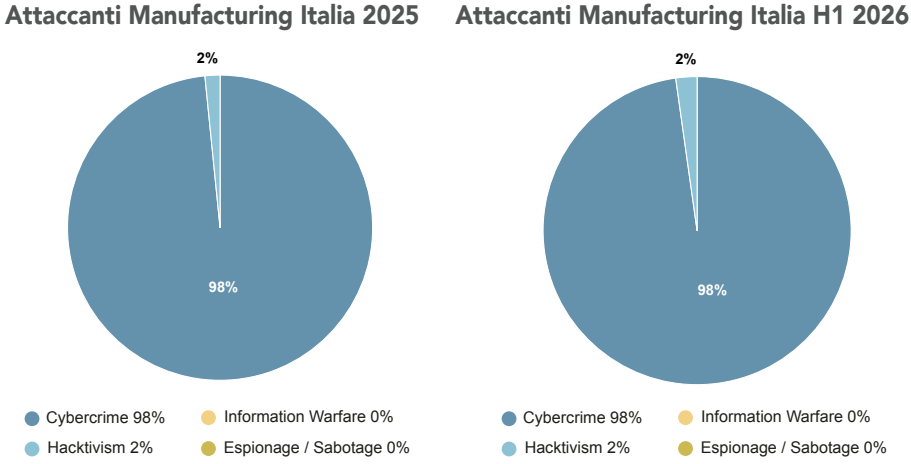


© Clusit - Rapporto 2026 sulla Cybersecurity

Il confronto internazionale rende questo dato ancora più significativo perché, nello stesso periodo, il Manufacturing rappresenta il 5,4% degli incidenti globali contro il 18,4% di quelli italiani. Il peso relativo del settore nel nostro Paese risulta quindi oltre tre volte superiore a quello osservato globalmente.

Sappiamo che questo dato da solo non consente di concludere che il Manufacturing italiano sia proporzionalmente più vulnerabile poiché incidono su questa valutazione anche la struttura produttiva del Paese, la composizione del campione e il livello di visibilità degli incidenti; esso mostra però con chiarezza quanto il comparto industriale assuma un peso particolare nel panorama Cyber nazionale.

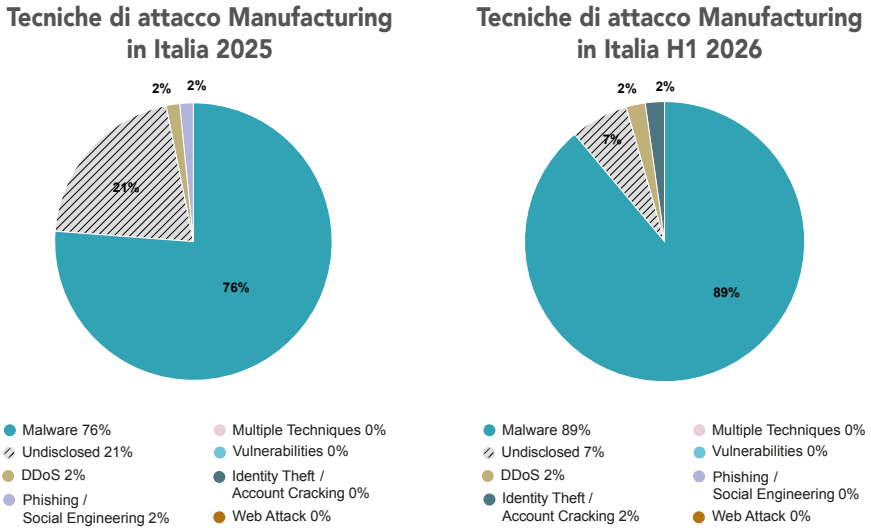
Inoltre, se il ritmo dei primi sei mesi si mantenesse costante, si arriverebbe a circa 90 episodi nell'intero 2026 contro i 63 del 2025. Anche in questo caso si tratterebbe esclusivamente di una proiezione lineare, ma il dato indica che il rallentamento osservato nel 2025 potrebbe non rappresentare un'inversione strutturale della tendenza.



© Clusit - Rapporto 2026 sulla Cybersecurity

Anche in Italia il Cybercrime domina in maniera pressoché assoluta nel Manufacturing. Il fenomeno appare quindi sempre meno episodico e sempre più riconducibile a un modello criminale organizzato nel quale l'impresa industriale costituisce un obiettivo particolarmente interessante proprio per l'elevato costo associato all'interruzione delle attività.

La possibilità di bloccare produzione e servizi essenziali aumenta infatti la pressione sulla vittima e, di conseguenza, il potenziale ritorno economico dell'attacco.



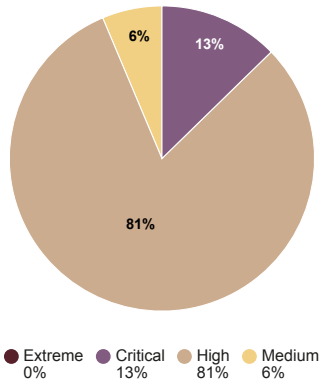
© Clusit - Rapporto 2026 sulla Cybersecurity

Il dato italiano relativo alle tecniche è ancora più netto. Nel primo semestre 2026 il malware rappresenta circa l'89% degli incidenti, rispetto al 76% del 2025, mentre i casi classificati come Undisclosed si sono ridotti dal 21% al 7%.

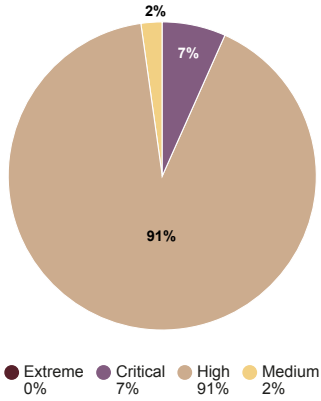
La variazione potrebbe essere interpretata in due modi differenti e non necessariamente alternativi. Da un lato potrebbe riflettere un'effettiva maggiore incidenza delle campagne malware e ransomware. Dall'altro, la riduzione dei casi non classificati potrebbe essere legata anche ad una maggiore disponibilità di informazioni sugli incidenti e ad una progressiva maturazione dei meccanismi di rilevazione, classificazione e reporting, come si evince altresì dal report sulla Cyber OT della survey svolta da Women For Security.

Questo è un aspetto particolarmente importante perché quando aumenta la capacità di comprensione e consapevolezza del fenomeno, si verifica anche una maggior capacità di individuarlo e descriverlo.

Severity Manufacturing in Italia 2025



Severity Manufacturing in Italia H1 2026



© Clusit - Rapporto 2026 sulla Cybersecurity

Anche sul fronte della severity il dato italiano si inserisce nella dinamica già analizzata a livello globale: diminuisce la quota degli eventi classificati come Critical, ma aumenta quella degli incidenti High. In Italia il fenomeno è particolarmente accentuato, con i casi classificati come Critical che scendono dal 13% del 2025 al 7% nel primo semestre 2026, mentre i casi classificati come High salgono dall'81% al 91%. In ogni caso questo significa che il 98% degli incidenti cyber di settore osservati in Italia ricadono in una delle due classi di maggiore severità.

Vero è che la diminuzione degli episodi Critical costituisce certamente un elemento da valutare positivamente, ma questo sostanzialmente non modifica un quadro nel quale quasi tutti gli incidenti andati a buon fine continuano ad avere conseguenze significative.

Per concludere: i dati del primo semestre 2026 mostrano un settore Manufacturing sottoposto ad una pressione Cyber sempre crescente e legata prevalentemente alla cybercriminalità. Inoltre mostrano come la questione stia progressivamente cambiando natura passando dalla protezione dei sistemi informativi alla protezione della capacità produttiva. La cybersecurity si conferma pertanto una componente centrale della continuità operativa e, in ultima analisi, della competitività e della resilienza stessa delle imprese manifatturiere.

Una fotografia sulla cybersecurity degli ambienti OT nelle imprese italiane

[A cura di Georgia Cesarone, Women for Security]

Come abbiamo sottolineato spesso all'interno del Rapporto CLUSIT, la crescente interconnessione tra Information Technology e Operational Technology sta modificando profondamente il profilo di rischio delle organizzazioni industriali, determinando un unico ecosistema cyber-fisico nel quale un incidente informatico produce conseguenze che vanno ben oltre la compromissione del dato.

È in questo scenario che si colloca l'importante iniziativa promossa dalle Women for Security con l'Assessment Cybersecurity OT che ha raccolto le risposte di 75 organizzazioni attraverso 60 domande articolate in 17 aree tematiche. L'indagine attraversa sostanzialmente l'intero ciclo della sicurezza industriale dalla conoscenza degli asset alla protezione dei dati, dalla configurazione sicura dei sistemi alla gestione degli accessi, dalla segmentazione delle reti al monitoraggio fino alla gestione degli incidenti, alla continuità operativa, alla supply chain, alla formazione e alla governance. Un'analisi completa della postura delle aziende intervistate nell'ambito OT e della relativa convergenza con gli ambienti IT.

Più che una misura assoluta della maturità del sistema industriale, i risultati restituiscono una fotografia interessante delle sue disomogeneità. Il dato forse più significativo non è infatti la semplice presenza o assenza di singole misure di sicurezza, ma la quantità di risposte "parzialmente/in corso" rilevate dal questionario. Molte organizzazioni sembrano avere già intrapreso un percorso di rafforzamento della sicurezza OT, pur senza averlo ancora trasformato in un sistema pienamente strutturato e integrato.

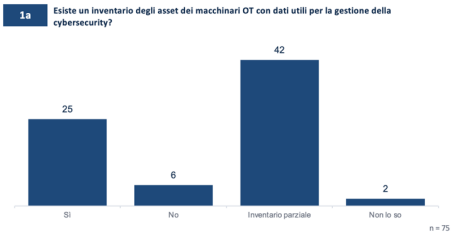
È una situazione che emerge chiaramente anche nella sintesi complessiva dell'assessment.

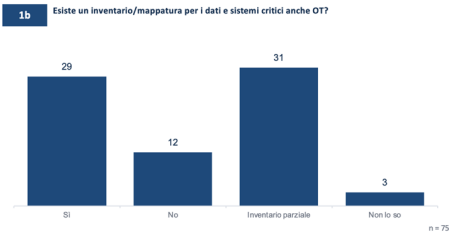


Il confronto tra le aree più mature e quelle più deboli rende ancora più evidente questa dinamica. L'80% delle organizzazioni utilizza VPN per gli accessi remoti OT, il 78% dispone di alimentazioni ridondate, UPS o gruppi di continuità, il 76% ha implementato misure minime per il controllo degli accessi fisici, il 75% dispone di misure di sicurezza ambientale e il 73% segmenta gli asset collegati a cloud o web. Quando però ci si sposta verso processi che richiedono continuità nel tempo, competenze specialistiche ed una maggiore integrazione organizzativa, le percentuali scendono sensibilmente e vediamo che soltanto il 21% estende gli aggiornamenti software e di sistema operativo validati ai dispositivi OT/SCADA, il 25% dispone di una policy per il ciclo di vita degli asset OT, il 25% testa nuovi macchinari o modifiche in un ambiente separato, il 27% effettua periodicamente Vulnerability Assessment sugli asset OT critici e circa un terzo dispone di un SOC con competenze specificamente OT.

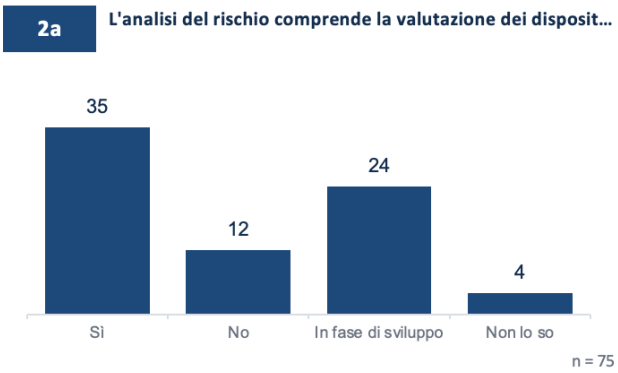
Si delinea così la prima chiave di lettura dell'intera indagine che ci permette di riflettere sul fatto che le organizzazioni sembrino mediamente più mature nel proteggere il perimetro e nel mettere in campo misure preventive anziché nel governare in maniera continuativa il rischio OT. Non emerge quindi tanto l'assenza di misure in ambito cybersecurity, quanto una cybersecurity ancora frequentemente costruita per singoli controlli verticali.

© Clusit 2026

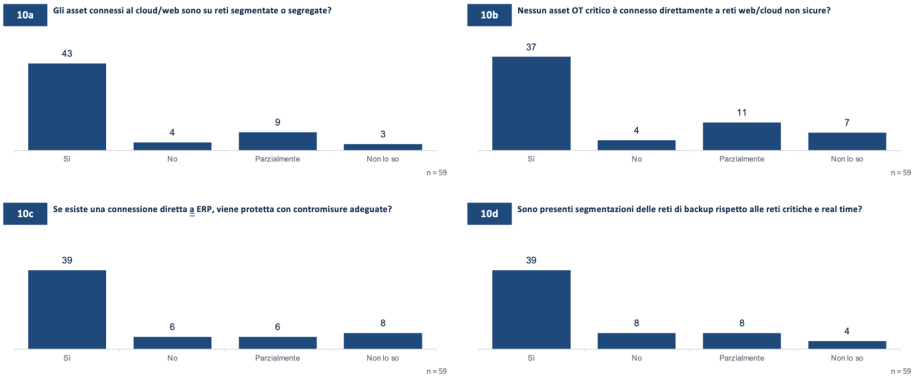




La stessa dinamica appare evidente nel campo della gestione degli asset. Solo 25 organizzazioni su 75 dichiarano di disporre di un inventario completo degli asset OT, mentre 42 ne possiedono uno parziale. La mappatura dei sistemi critici presenta una situazione molto simile: 29 organizzazioni la considerano completa e 31 parziale. È un dato particolarmente importante perché tutto ciò che viene dopo dipende inevitabilmente dalla conoscenza di ciò che deve essere protetto. L'inventario, inoltre, non può e non deve limitarsi all'elenco dei dispositivi presenti. L'assessment evidenzia invece come spesso manchino proprio le informazioni rilevanti ai fini della cybersecurity quali owner, criticità, dipendenze e modalità di accesso remoto. In un ambiente industriale, la criticità di un asset non dipende necessariamente dal suo valore economico o dalla sua complessità tecnologica, ma dal suo essere essenziale se la sua indisponibilità determina l'interruzione di un processo, produce conseguenze sulla safety o impedisce il funzionamento di altri sistemi. La conoscenza dell'asset dovrebbe quindi evolvere progressivamente dalla semplice inventariazione alla comprensione delle dipendenze e dell'impatto sul processo e sul rischio ad esso collegato.



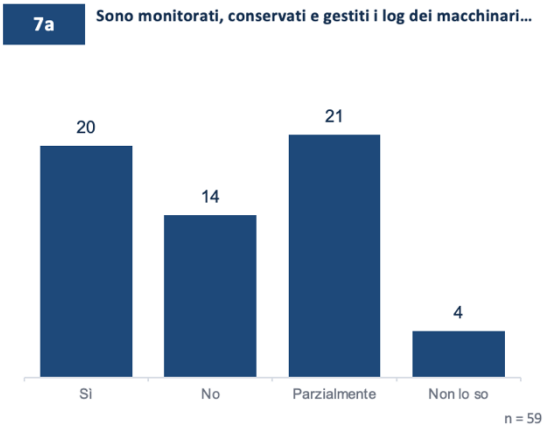
E infatti, da questo punto di vista, è il dato relativo al risk assessment a mostrarci un quadro più avanzato con 35 organizzazioni su 75 dichiarano che l'analisi del rischio comprende già l'ambiente OT e altre 24 stanno lavorando in questa direzione. È forse uno dei segnali più interessanti dell'indagine, perché indica che la specificità del rischio industriale comincia ad essere riconosciuta. Come ben sappiamo, nel mondo OT le conseguenze di un incidente non rimangono confinate alla dimensione digitale, ma possono propagarsi alla produzione, alla disponibilità dell'impianto, alla sicurezza delle persone e dell'ambiente ed è quindi proprio la relazione tra asset, processo e conseguenza a diventare centrale.



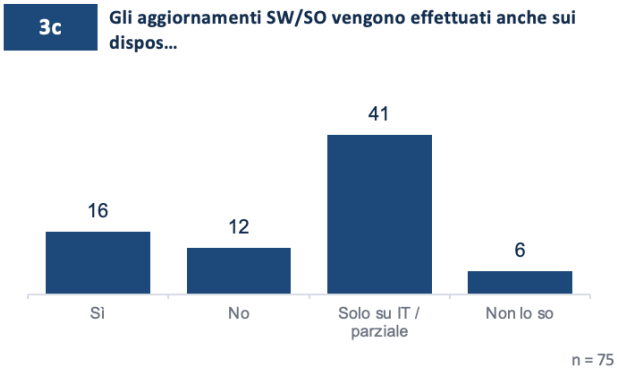
Anche sul fronte della segmentazione emergono segnali positivi. Il 73% delle organizzazioni segmenta gli asset collegati a cloud o web, il 63% evita collegamenti diretti degli asset OT critici verso reti non sicure e il 66% protegge le connessioni dirette verso sistemi ERP. Sono percentuali che mostrano come la separazione e il controllo delle comunicazioni tra ambienti siano ormai concetti abbastanza consolidati, ma il dato diventa però più interessante se confrontato con quello relativo al monitoraggio: soltanto 28 organizzazioni su 59 utilizzano strumenti quali SIEM, NIDS, EDR o XDR in grado di segnalare eventi cyber nell'ambiente OT e 34 dichiarano di non disporre di un SOC con competenze OT.

Si crea così una sorta di asimmetria nella quale la capacità di impedire o limitare l'accesso appare più sviluppata della capacità di osservare ciò che accade una volta all'interno dell'ambiente industriale. I dati relativi al Log Management rafforzano questa interpretazione con solo 20 organizzazioni su 59 che dichiarano un monitoraggio ed una conservazione strutturata dei log dei macchinari OT, mentre 21 lo

fanno parzialmente. Inoltre, un quarto dei rispondenti non sa se gli asset utilizzino una sorgente temporale comune. Quest'ultimo elemento può apparire secondario, ma assume grande importanza quando occorre ricostruire la sequenza degli eventi durante un incidente!

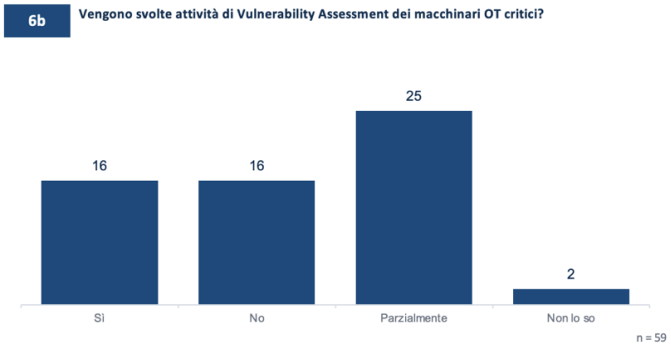


È probabilmente questo il passaggio che consente di leggere in modo unitario i risultati dell'assessment. Il tema non sembra essere più soltanto la capacità di proteggere un asset, ma la capacità dell'organizzazione di governarlo durante tutto il suo ciclo di vita dal rilevare un'anomalia a reagire ad un incidente per riportare il processo in condizioni operative.



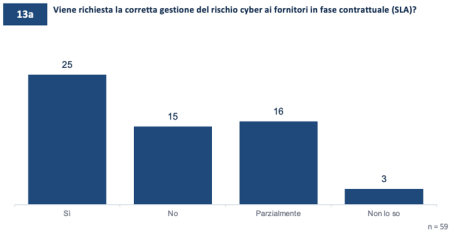
Nell'ambito del patch management vediamo che solo il 21% delle organizzazioni dichiara di effettuare aggiornamenti software o di sistema operativo anche sui dispo-

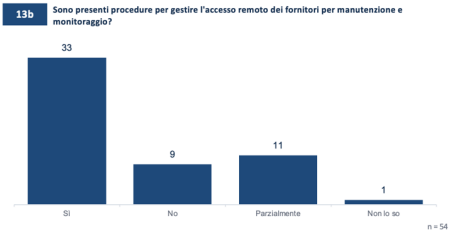
sitivi OT/SCADA, mentre nel 55% dei casi questa pratica rimane confinata prevalentemente o esclusivamente al mondo IT. È un dato che va letto tenendo conto della complessità specifica degli ambienti industriali nei quali aggiornare un sistema OT può incidere sulla disponibilità del processo, sulla compatibilità con altri componenti e sulla continuità operativa. Il problema non è quindi semplicemente "applicare più patch", ma costruire un processo che consenta di valutare, validare, testare e distribuire gli aggiornamenti in maniera controllata e periodica.



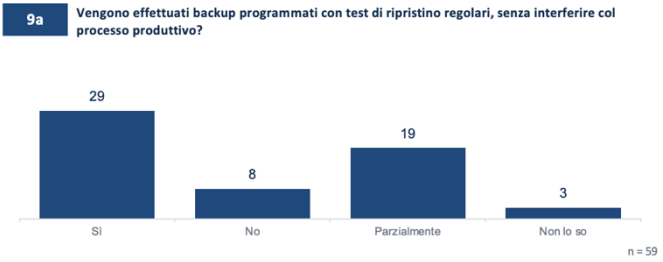
La stessa complessità emerge nel valutare le attività di vulnerability management. Soltanto 16 organizzazioni su 59 effettuano in maniera continuativa Vulnerability Assessment sui macchinari OT critici, 25 lo fanno parzialmente e 16 non lo fanno. Anche in questo caso il dato racconta probabilmente qualcosa di più di una semplice carenza tecnologica. Negli ambienti industriali una scansione attiva può interferire con sistemi legacy o dispositivi particolarmente sensibili, rendendo necessario un approccio progressivo basato sulla conoscenza degli asset, sulla criticità e sulla possibilità di effettuare test in condizioni controllate. Proprio quest'ultimo aspetto rappresenta uno dei risultati più importanti dell'assessment: soltanto il 25% delle organizzazioni testa nuovi macchinari OT o modifiche ai sistemi in un ambiente separato dalla produzione, mentre il 49% non lo fa. È un gap particolarmente significativo perché collega molti degli aspetti che abbiamo visto emergere nelle altre aree. Infatti, la possibilità di disporre di ambienti separati permette di verificare aggiornamenti, configurazioni, vulnerabilità e comportamenti inattesi senza trasferire direttamente il rischio sul processo produttivo ed è pertanto particolarmente rilevante.

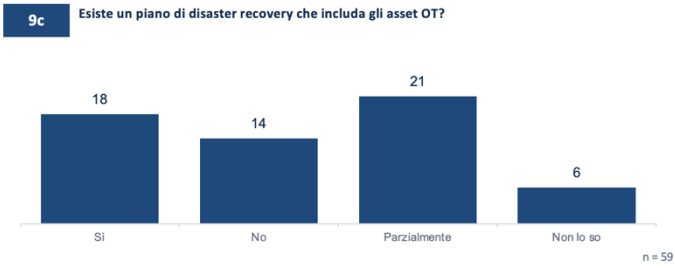
© Clusit 2026





Un altro elemento che attraversa trasversalmente i risultati è il rapporto con i fornitori perché solo 25 organizzazioni su 59 dichiarano di richiedere contrattualmente ai propri fornitori una corretta gestione del rischio cyber, ma allo stesso tempo 33 organizzazioni su 54 hanno definito procedure per il loro accesso remoto. È un dato particolarmente rilevante negli ambienti OT, dove manutentori e fornitori possono accedere direttamente ai sistemi che governano il processo industriale. Il perimetro della sicurezza non coincide quindi più necessariamente con quello dell'organizzazione perché una parte del rischio viene condivisa con soggetti esterni e deve essere governata prima, durante e dopo il loro accesso ai sistemi.





Anche i risultati relativi alla continuità operativa mostrano la distanza tra disponibilità di singole misure e costruzione di una capacità complessiva di governance. 29 organizzazioni su 59 effettuano backup programmati accompagnati da test di ripristino e 31 dispongono di copie offline, ma soltanto 18 hanno un Disaster Recovery Plan che comprenda esplicitamente gli asset OT. Il backup, quindi, appare più maturo della capacità di recovery. Ed è proprio questa differenza a diventare cruciale in ambiente industriale, perché ripristinare dati non equivale necessariamente a ripristinare un processo, perché per farlo occorre conoscere le dipendenze tra sistemi, recuperare configurazioni, definire sequenze di riavvio e riportare l'impianto in condizioni operative e sicure.

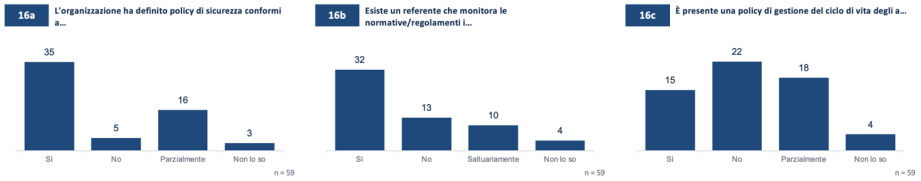
Sul fronte dell'Incident Management il quadro appare relativamente più maturo. 32 organizzazioni su 59 dispongono di piani o prassi consolidate per la gestione degli incidenti, 37 hanno definito flussi informativi verso le autorità competenti e 29 hanno formalizzato ruoli e responsabilità. Anche in questo caso, tuttavia, la sfida consiste nel trasformare il piano in capacità operativa, soprattutto quando l'incidente coinvolge contemporaneamente cybersecurity, produzione, manutenzione, safety, management e fornitori. Riteniamo che le normative entrate in vigore possano aver giocato un ruolo significativo da questo punto di vista.

61%

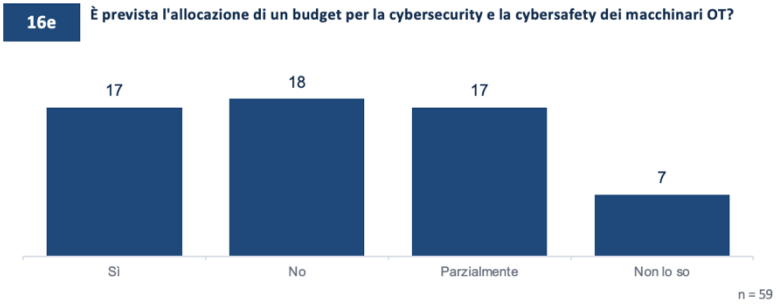
risponde "Sì" a questa domanda

Sono previste attività di formazione in merito alle politiche cybersecurity industriale e sulla cyber safety?

Tra gli elementi più positivi della rilevazione emerge sicuramente la formazione: il 61% delle organizzazioni dichiara di svolgere attività dedicate alla cybersecurity industriale e alla cyber safety, mentre soltanto il 15% dichiara di non farlo. È un risultato importante, ma anche in questo caso può rappresentare un punto di partenza più che di arrivo dettato dalle normative vigenti. Ora occorre un passaggio evolutivo necessario nel quale la specificità degli ambienti OT porti l'azienda a differenziare progressivamente la formazione in funzione dei ruoli. La maturità non consiste soltanto nel conoscere il rischio cyber, ma nel sapere come comportarsi quando quel rischio entra nel processo industriale.



Alla fine del percorso, come spesso ripetiamo, è la governance ad offrire probabilmente la chiave di lettura più interessante dell'intera indagine. Il 59% delle organizzazioni dichiara di disporre di policy di sicurezza conformi alle normative e il 54% dispone di un referente che monitora l'evoluzione normativa, ma soltanto il 25% ha una policy per la gestione del ciclo di vita degli asset OT e solo il 41% assegna ruoli e responsabilità di cybersecurity che comprendano esplicitamente anche l'OT. Ancora più significativo è il dato economico con solo 17 organizzazioni su 59 che dichiarano di allocare un budget strutturato per cybersecurity e cybersafety OT. Dà da pensare che 18 aziende non ne dispongano e 17 lo prevedano soltanto parzialmente e saltuariamente.



Questi numeri consentono forse di rileggere tutti gli altri con una nuova consapevolezza. Se inventario, vulnerability management, patching, monitoring, incident response, disaster recovery e supply chain presentano livelli di maturità differenti, una parte della spiegazione potrebbe risiedere proprio nella difficoltà di trasformare la cybersecurity OT da insieme di iniziative tecniche verticali in capo ai relativi responsabili a processo di governance industriale strutturato dotato di responsabilità, risorse e continuità nel tempo.

La fotografia restituita dall'assessment non è quindi quella di organizzazioni prive di difese. Al contrario, mostra che numerose misure sono già presenti e che in molti casi sono stati avviati grandi percorsi di miglioramento.

La frequenza delle risposte parziali suggerisce però che una parte significativa di questi percorsi sia ancora in evoluzione. Non dobbiamo quindi ragionare tanto su una contrapposizione tra organizzazioni "sicure" e "non sicure", quanto comprendere che esista un passaggio ancora incompleto da una cybersecurity OT costruita per singoli controlli ad una capacità di resilienza industriale costruita per processi.

La maturità successiva sembra quindi giocarsi soprattutto sulle connessioni tra questi verticali grazie ad una maggiore capacità di governance in grado di integrare i controlli esistenti all'interno di un modello aziendale coerente.

In questa prospettiva, il passaggio dalla protezione alla resilienza rappresenta forse la sintesi più efficace della fotografia emersa. Proteggere rimane indispensabile, ma come sempre non è sufficiente. Un ambiente industriale maturo deve essere in grado di comprendere cosa stia accadendo, reagire quando un controllo venga superato rimettendo il processo in condizioni di sicurezza. Ed è proprio nella trasformazione dei controlli ancora in parte isolati in una capacità strutturata e permanente di gestione del rischio cyber-fisico che sembra collocarsi la principale sfida evidenziata dai risultati dell'assessment aperta a tutti i professionisti del settore e alle aziende.

© Clusit 2026

AI Act, una normativa particolare

[A cura di Giancarlo Butti]

L'AI ACT è una normativa molto particolare. La sua applicazione interessa milioni di organizzazioni, in quanto chiunque utilizzi un sistema (o un modello) di AI è soggetto a tale normativa. Tuttavia la quasi totalità di queste organizzazioni non deve mettere in atto alcun adempimento.

Giancarlo Butti

L'entrata in vigore del Regolamento (UE) 2024/1689 (noto come **AI Act**) segna una svolta storica nella regolamentazione europea sulle tecnologie emergenti. Tuttavia, l'approccio di molte aziende a questa normativa risulta spesso condizionato da messaggi allarmistici (in particolare a causa di articoli, corsi, presentazioni sul tema) e da proposte consulenziali poco focalizzate sul contenuto reale della legge.

Un esame attento del testo normativo rivela una realtà ben diversa: sebbene il Regolamento si rivolga potenzialmente a qualsiasi organizzazione, le prescrizioni più complesse e onerose si applicano soltanto a una quota molto ridotta di scenari e di operatori (termini con cui la normativa identifica i vari soggetti coinvolti).

Questo articolo vuole fare luce sulla reale portata del Regolamento e permettere alle organizzazioni di comprendere meglio quello che è un corretto percorso per essere conformi alla normativa e, soprattutto, per evitare di cadere vittime di speculazioni attivando inutili e costosi progetti di adeguamento.

1. La reale portata dell'AI ACT

L'abitudine di affidarsi a sintesi e a materiale divulgativo, espone le organizzazioni al rischio di interpretazioni distorte di una normativa. Persino i documenti informativi pubblicati sui portali dell'Unione Europea hanno uno scopo puramente orientativo, rendendo indispensabile il riscontro diretto sul testo legislativo.

Infatti, solo la lettura diretta dell'intero testo di una normativa costituisce lo strumento che garantisce una piena comprensione della stessa. Qualunque altro tipo di approcciò deve considerarsi come una interpretazione, con tutti i limiti del caso.

Per quanto attiene all'AI ACT, sebbene la normativa si presenti con un'estensione imponente (**144 pagine, 180 considerando, 113 articoli e 13 allegati** integrati da altri

pochi articoli e da un nuovo allegato dopo le modifiche apportate dal Regolamento 2026/1744), l'impianto prescrittivo è altamente selettivo.

Gli articoli a carattere prescrittivo sono circa 40 e stabiliscono obblighi a carico degli operatori (fornitori, deployer, fabbricanti, rappresentanti autorizzati, importatori e distributori).

Di questi, circa 30 regolano in modo esclusivo i sistemi ad alto rischio, 5 sono dedicati alla disciplina dei modelli di AI per finalità generali mentre il solo articolo 50 definisce le misure di trasparenza che si applicano a 5 casistiche ben definite.

Quindi, se non si hanno sistemi ad alto rischio o sistemi che ricadono nelle casistiche previste dall'articolo 50 gli adempimenti richiesti si limitano ad un censimento e classificazione dei sistemi/modelli in uso presso l'organizzazione. Nessun altro adempimento è richiesto.

In presenza di modelli per finalità generale gli adempimenti sono in carico al solo fornitore, termine che nel gergo dall'AI ACT identifica il soggetto che sviluppa il sistema o modello[1] e quindi difficilmente coinvolgono una normale organizzazione.

Anche l'articolo 4 dedicato alla alfabetizzazione sull'intelligenza artificiale, unico articolo di portata generale, è stato semplificato dal Regolamento 2026/1744. In effetti gli articoli aggiuntivi all'AI ACT, introdotti da questo regolamento, introducono semplificazioni, in particolare per alcuni adempimenti che riguardano principalmente i sistemi ad alto rischio.

A conferma del limitato impatto che l'AI ACT ha sulla maggior parte delle organizzazioni si riporta quanto affermano le linee guida ufficiali dell'Unione Europea (Commission Guidelines on the definition of an artificial intelligence system) che stabiliscono al considerando (63):

Only certain AI systems are subject to regulatory obligations and oversight under the AI Act. The AI Act's risk-based approach means that only those systems giving rise to the most significant risks to fundamental rights and freedoms will be subject to its prohibitions laid down in Article 5 AI Act, its regulatory regime for high-risk AI systems covered by Article 6 AI Act and its transparency requirements for a limited number of pre-defined AI systems laid down in Article 50 AI Act. **THE VAST MAJORITY OF SYSTEMS, EVEN IF THEY QUALIFY AS AI SYSTEMS WITHIN THE**

[1] Più precisamente: «fornitore»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito;

MEANING OF ARTICLE 3(1) AI ACT, WILL NOT BE SUBJECT TO ANY REGULATORY REQUIREMENTS UNDER THE AI ACT.

Entrando maggiormente nel dettaglio, per quanto riguarda i **sistemi ad alto rischio**, il quadro prescrittivo include, fra gli altri, presidi per la gestione dei rischi, requisiti di robustezza e resilienza informatica, governance dei dati, documentazione tecnica dettagliata, istruzioni d'uso per gli utilizzatori...

La maggior parte di tali adempimenti fa capo al **fornitore**. Al contrario, le figure che si limitano a utilizzare tali sistemi (**deployer**) hanno una serie di adempimenti molto più limitati.

Per quanto attiene i sistemi per i quali sono richieste regole di trasparenza, le obbligazioni sono in parte per i fornitori (2) e in parte per i deployer (3). Per questi ultimi gli adempimenti sono molto semplici da implementare, limitandosi all'obbligo di dare evidenza dell'uso di un sistema di AI.

In sintesi quindi vi è una sproporzione notevole fra gli articoli che impegnano i fornitori rispetto a quelli che richiedono qualche attività ad un deployer.

2. Identificazione, mappatura e classificazione

Poiché gli obblighi più stringenti riguardano solo un numero molto limitato di sistemi di AI, l'attività preliminare ed essenziale per ogni organizzazione consiste nel censire il proprio parco software e determinare la categoria di appartenenza degli eventuali sistemi e modelli AI presenti.

Questa azione è imprescindibile, in quanto solo dopo lo svolgimento di tale attività una organizzazione sarà in grado di valutare se dovrà mettere in atto qualche adempimento ai sensi dell'AI ACT o se ha già esaurito i propri adempimenti.

2.1 Censire i sistemi e i modelli di AI

Il censimento iniziale non è un'attività semplice, in quanto l'inventario delle tecnologie non deve limitarsi agli applicativi esplicitamente dichiarati come AI, ma deve analizzare, fra gli altri:

- integrazioni invisibili (embedded): funzionalità di intelligenza artificiale inserite all'interno di software gestionali, piattaforme SAAS o apparati hardware di fornitori terzi;
- agenti AI: flussi operativi che eseguono decisioni o compiti senza supervisione umana diretta;

- utilizzi non tracciati (shadow AI): strumenti o servizi online utilizzati in autonomia dal personale al di fuori delle direttive ICT aziendali;
- casi d'uso specifici di AI generativa: uso di AI generativa per funzionalità che in alcuni casi possono essere simili a quelle dei sistemi che l'AI ACT classifica come ad alto rischio o vietati;
- …

Al censimento dei potenziali sistemi/modelli di AI deve far seguito l'analisi del singolo caso, al fine di verificare che lo stesso sia effettivamente un sistema o un modello ai sensi dell'AI ACT.

Quest'ultimo infatti prevede dei casi di esclusione ed il documento **Orientamenti della Commissione sulla definizione di sistema di intelligenza artificiale stabilita dal regolamento (UE) 2024/1689 (regolamento sull'IA)** aiuta nella attività di corretta identificazione della singola applicazione.

2.2 Una classificazione basata sul rischio

La consueta schematizzazione dell'AI ACT in quattro distinti livelli di rischio (sistemi vietati, ad alto rischio, a rischio minimo e con obblighi di trasparenza) è concettualmente scorretta, in quanto il Regolamento vieta specifiche pratiche (**Capo II, Art. 5**), disciplina i sistemi ad alto rischio (**Capo III, Art. 6**), ma l'**Articolo 50** non individua una classe di rischio a sé stante, ma prescrive obblighi informativi e di trasparenza per sistemi caratterizzati da particolari casi d'uso (ad esempio, sistemi che interagiscono con persone fisiche, strumenti di riconoscimento delle emozioni o di categorizzazione biometrica, e generatori di contenuti sintetici o deepfake).

Di conseguenza, una soluzione ad alto rischio può essere contestualmente soggetta agli obblighi dell'Articolo 50, il cui paragrafo 6 di fatto recita:

> *I paragrafi da 1 a 4 lasciano impregiudicati i requisiti e gli obblighi di cui al capo III, così come gli altri obblighi di trasparenza stabiliti dal diritto dell'Unione o nazionale per i deployer dei sistemi di IA.*

Trattare quindi i sistemi che ricadono nell'articolo 50 come alternativi all'alto rischio costituisce un errore di impostazione che espone a non-conformità.

Per quanto attiene infine ai sistemi vietati ai sensi dell'articolo 5, questi devono essere semplicemente dismessi e quindi per loro l'AI ACT non prevede alcun ulteriore adempimento.

È importante comprendere che la classificazione dei sistemi non avviene tramite un'analisi del rischio, ma tramite un riscontro del singolo caso d'uso con i casi previsti dagli articoli 5, 6 e 50.

Si tratta di una semplice comparazione, anche se non mancano i casi che possono presentare qualche ambiguità interpretativa e che devono essere analizzati molto dettagliatamente.

Deve essere inoltre chiaro che sia il censimento, sia la classificazione, devono prendere in considerazione i singoli casi d'uso di un sistema e, per quanto attiene i sistemi di AI generativa, i singoli prompt sottomessi agli strumenti.

Una mancata presa d'atto di questa eventualità o una sua liberalizzazione potrebbe costituire un tentativo di eludere i requisiti normativi: se il monitoraggio dei lavoratori tramite un sistema di AI ne determina una sua classificazione come sistema ad alto rischio, se ottengo lo stesso risultato con un sistema di AI generativa perché il legislatore dovrebbe considerare questo caso d'uso in modo diverso?

È su quest'ultimo punto che le organizzazioni stanno correndo i rischi maggiori, in quanto non è ancora chiaro che l'AI ACT regolamenta l'uso che si fa dei sistemi AI, non i sistemi AI in quanto tali.

Da qui la necessità di una policy molto restrittiva sull'uso dell'IA generativa, che regolamenti non solo i prodotti utilizzabili, ma soprattutto i singoli casi d'uso.

La policy dovrebbe essere necessariamente accompagnata da robusti presidi tecnici che permettano di intercettare i singoli prompt per un'analisi a posteriore del rispetto delle regole aziendali (ovviamente dopo aver attivato tutti i presidi di legge previsti in questi casi).

Un aspetto particolarmente importante è che l'attività di censimento, identificazione e classificazione non può e non deve essere svolta una tantum.

È pertanto necessario implementare una procedura che consenta di intercettare ogni nuovo sistema o modifica di sistema esistente, al fine di consentirne una corretta classificazione[2].

2.3 La classificazione ex post

La classificazione condotta da una organizzazione ha natura *ex ante*. Le autorità di controllo conservano poteri di riclassificazione *ex post* in virtù dei seguenti articoli:

[2] Per maggiori dettagli si rimanda al testo: AI ACT, G.Butti, ITER 2026, https://iterdigital.it/it_it/ai-act-in-pratica/

Articolo 79 - Procedura a livello nazionale per i sistemi di IA che presentano un rischio

1.Un sistema di IA che presenta un rischio è inteso come un «prodotto che presenta un rischio» quale definito all'articolo 3, punto 19, del regolamento (UE) 2019/1020 nella misura in cui presenta rischi per la salute o la sicurezza o per i diritti fondamentali delle persone.

2.Qualora l'autorità di vigilanza del mercato di uno Stato membro abbia un motivo sufficiente per ritenere che un sistema di IA presenti un rischio di cui al paragrafo 1 del presente articolo, essa effettua una valutazione del sistema di IA interessato per quanto riguarda la sua conformità a tutti i requisiti e gli obblighi di cui al presente regolamento. Particolare attenzione è prestata ai sistemi di IA che presentano un rischio per i gruppi vulnerabili. Qualora siano individuati rischi per i diritti fondamentali, l'autorità di vigilanza del mercato informa anche le autorità o gli organismi pubblici nazionali competenti di cui all'articolo 77, paragrafo 1, e coopera pienamente con essi. I pertinenti operatori cooperano, per quanto necessario, con l'autorità di vigilanza del mercato e con le altre autorità o gli altri organismi pubblici nazionali di cui all'articolo 77, paragrafo 1.

…

Articolo 82 - Sistemi di IA conformi che presentano un rischio

1.Se, dopo aver effettuato una valutazione a norma dell'articolo 79 e aver consultato la pertinente autorità pubblica nazionale di cui all'articolo 77, paragrafo 1, l'autorità di vigilanza del mercato di uno Stato membro ritiene che un sistema di IA ad alto rischio, pur conforme al presente regolamento, rappresenti comunque un rischio per la salute o la sicurezza delle persone, per i diritti fondamentali o per altri aspetti della tutela dell'interesse pubblico, essa chiede all'operatore pertinente di adottare tutte le misure adeguate a far sì che il sistema di IA in questione, all'atto della sua immissione sul mercato o messa in servizio, non presenti più tale rischio senza indebito ritardo entro un termine che essa può prescrivere.

…

A questi presidi si affianca l'**Articolo 80 - Procedura per i sistemi di IA classificati dal fornitore come non ad alto rischio in applicazione dell'allegato III**, che attribuisce ulteriori facoltà di intervento, ed in particolare la possibilità di revocare l'esclusione dagli adempimenti richiesti per un sistema di AI, che non era stato classificato come ad alto rischio pur in presenza dei requisiti per esserlo, in virtù di quanto previsto dall'articolo 6.3.

Quindi la classificazione effettuata da una organizzazione, può essere soggetta a revisione da parte delle autorità.

2.4 Classificazione dei modelli di AI

L'AI ACT articola una disciplina specifica per i modelli:

- **modelli di IA generici,** la cui definizione non è presente nell'AI ACT;
- **modelli di IA per finalità generali (GPAI):** definiti dall'**Articolo 3, punto 63**: *«modello di IA per finalità generali»: un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l›autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato;*
- **modelli GPAI con rischio sistemico:** definiti dall'**Articolo 51**:
  1. Un modello di IA per finalità generali è classificato come modello di IA per finalità generali con rischio sistemico se soddisfa una delle condizioni seguenti:
  a) presenta capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento;
  b) sulla base di una decisione della Commissione, ex officio o a seguito di una segnalazione qualificata del gruppo di esperti scientifici, presenta capacità o un impatto equivalenti a quelli di cui alla lettera a), tenendo conto dei criteri di cui all'allegato XIII.

3. Gli errori più comuni nella implementazione

Nelle strategie di adeguamento all'AI ACT occorre evitare alcune impostazioni errate molto diffuse:

Iniziare il percorso di adeguamento con una gap analysis generalizzata rappresenta un errore. Se dal censimento iniziale emerge che l'organizzazione non impiega sistemi ad alto rischio né soluzioni soggette all'Articolo 50, gran parte della normativa non trova applicazione, rendendo l'analisi della situazione as is, un mero costo privo di utilità. Inoltre, non essendoci precedenti normative che regolavano questo ambito, non rileva una gap analysis con altre normative.

Purtroppo molte organizzazioni si affidano a consulenti che propongono un dispendioso ed inutile approccio tradizionale, mentre l'unica cosa giusta da fare è procedere

secondo i passi descritti in precedenza e, solo in presenza di sistemi rientranti negli ambiti previsti dagli articoli 6 e 50 procedere ad una gap analysis.
Un approccio tradizionale all'AI ACT comporta solo una perdita di tempo e un onere finanziario che può anche essere rilevante.

4. Utilizzo di strumenti ufficiali gratuiti

Per facilitare sia l'identificazione che la classificazione di un sistema/modello ai sensi dell'AI ACT, senza la necessità di ricorrere a servizi esterni onerosi, l'Unione Europea ha reso disponibile l'**EU AI Act Compliance Checker**[3]. Questo applicativo interattivo permette di verificare se un software rientri nell'ambito della norma e di individuarne la fascia di rischio, costituendo un punto di partenza tecnico autorevole. Nonostante un disclaimer suggerisca di non basare le proprie valutazioni solo su questo strumento, sicuramente lo stesso può essere un valido aiuto per un inquadramento iniziale.

Se il sistema in valutazione non presenta aspetti che richiedano una analisi più approfondita, è possibile compiere una valutazione definitiva utilizzando solo questo strumento.

Questo evidenzia come nella realtà dei fatti, non sia necessario ricorrere a costosi interventi esterni per condurre le fasi iniziali di adeguamento all'AI ACT che, per la quasi totalità delle organizzazioni, esauriscono gli adempimenti richiesti dalla normativa.

5. Make or buy

Come evidenziato nei paragrafi precedenti, l'uso di sistemi ad alto rischio comporta l'implementazione di numerose misure tecniche ed organizzative, nonché l'espletamento di diversi altri adempimenti.

Il rischio di non conformità, anche in presenza di tali adempimenti rimane alto e quindi sarebbe ragionevole chiedersi se il rapporto costo benefici dell'uso di un sistema di AI in uno dei casi che ne determinano una classificazione come ad alto rischio, sia giustificabile.

Ad esempio perché un'azienda dovrebbe implementare un'applicazione di AI per una analisi preliminare dei CV ricevuti?
Tale scelta potrebbe avere un senso per un'azienda di selezione del personale, ma la ricezione di quanti CV giornalieri potrebbe giustificare in un'azienda normale una soluzione di questo tipo?

---

[3] https://ai-act-service-desk.ec.europa.eu/en/eu-ai-act-compliance-checker

Ai costi dell'applicazione (costo iniziale e costi ricorrenti) va infatti sommato un costo non indifferente legato alla implementazione della conformità all'AI ACT a cui va sommato anche il costo del rischio di non conformità e, in molti casi, il potenziale rischio risarcitorio se qualcuno dovesse subire un danno in conseguenza di una decisione legata all'uso di un sistema di AI.

Solo prendendo in considerazione tutti questi elementi si potrà fare una corretta valutazione del rapporto costi/benefici.

Un altro fattore assolutamente determinante è il ruolo assunto dalla organizzazione. Come si è visto, la quasi totalità degli adempimenti previsti per un sistema ad alto rischio (e relativi rischi sanzionatori) sono in carico al fornitore.

Perché quindi una organizzazione dovrebbe decidere di sviluppare un sistema di AI se lo può acquisire sul mercato?

Nel primo caso, opzione MAKE, l'organizzazione assume contestualmente la qualifica di *fornitore* e d*eployer*, facendosi carico di tutti gli adempimenti ex-ante e delle attività di controllo post-commercializzazione.

Nel caso di opzione BUY l'organizzazione opera come semplice *deployer*, limitando i propri compiti ad esempio alla verifica delle istruzioni d'uso, alla supervisione umana e alla conservazione dei file di registro (log)...

Per verificare quanto si discostino i costi di queste 2 diverse opzioni ho chiesto a CLAUDE di sviluppare un modello e di applicarlo ad un relativo esempio concreto.

Nei paragrafi che seguono riporto una sintesi dei risultati.

© Clusit 2026

6. Il modello di confronto MAKE e BUY

Ho chiesto a CLAUDE di sviluppare un modello che tenesse conto dei costi dell'applicazione, di quelli di conformità, del rischio sanzionatorio e del rischio risarcitorio. Per quanto attiene i costi operativi sono stati presi in considerazione i seguenti parametri:

Opzione MAKE (Fornitore + Deployer): componenti di costo

Voce di costo	Descrizione	Natura
R&D (ricerca e sviluppo)	Progettazione dell'architettura, ricerca applicata, prototipazione	Una tantum
Data ingestion e labeling	Raccolta, pulizia ed etichettatura dei dataset di training	Una tantum / ricorrente
Compute / GPU	Capacità di calcolo per training e re-training periodico del modello	Ricorrente
Stipendi Data Scientist / ML Engineer	Team interno dedicato allo sviluppo e al mantenimento del modello	Ricorrente
Manutenzione ed evoluzione architetturale	Aggiornamento del modello, gestione del model drift, refactoring	Ricorrente

Opzione BUY (solo Deployer): componenti di costo

Voce di costo	Descrizione	Natura
Licenze software / SaaS	Canone di licenza o abbonamento alla piattaforma del fornitore	Ricorrente
Integrazione API / sistemi legacy	Sviluppo delle interfacce verso i sistemi aziendali esistenti	Una tantum
Customizzazione	Adattamento della soluzione standard alle esigenze specifiche	Una tantum
Canoni di supporto e manutenzione	Contratti di assistenza tecnica con il fornitore	Ricorrente
Costo di lock-in contrattuale	Onere stimato di uscita/migrazione in caso di cambio fornitore	Contingente

Il costo di sistema di ciascuna opzione è allocato sull'orizzonte di valutazione di *n* anni secondo un criterio di ammortamento lineare per i costi una tantum, sommato ai costi ricorrenti di ciascun anno dell'orizzonte secondo le seguenti formule:

C_sistema_MAKE = Σ Costi una tantum MAKE + Σ (t=1 → n) Costi ricorrenti MAKE(t)
C_sistema_BUY = Σ Costi una tantum BUY + Σ (t=1 → n) Costi ricorrenti BUY(t)

I costi di conformità sono determinati secondo la seguente formula, dove la voce **C_trasversali** indica il costo di conformità ad altre normative, quali il GDPR:

C_compliance_MAKE = C_ex-ante + C_post-market + C_trasversali
C_compliance_BUY = C_obblighi deployer + C_trasversali

Il rischio sanzionatorio viene calcolato con un'unica formula, ma nell'opzione BUY viene introdotto un fattore di mitigazione derivante dalla eventuale possibile rivalsa sul fornitore.

E[C_sanzioni] = P(Ispezione) × P(Non-Conformità) × Sanzione Stimata + Spese Legali
E[C_sanzioni_BUY_netto] = E[C_sanzioni_BUY] − Recupero da Manleva Contrattuale

Il rischio sanzionatorio viene calcolato con un'unica formula e anche in questo caso, viene introdotto un fattore di mitigazione derivante dalla eventuale possibile rivalsa sul fornitore.

E[C_danni] = (Frequenza Incidenti × Danno Medio) − Copertura Assicurativa (al netto di franchigie)
E[C_danni_BUY_netto] = E[C_danni_BUY] − Recupero da Manleva Fornitore

Quindi la formula finale è la seguente:

TCO_MAKE = C_sistema_MAKE + C_compliance_Fornitore+Deployer + E[C_sanzioni_MAKE] + E[C_danni_MAKE]
TCO_BUY = C_sistema_BUY + C_compliance_Deployer + E[C_sanzioni_BUY_netto] + E[C_danni_BUY_netto]

7. Il caso proposto da CLAUDE

Nelle tabelle seguenti si riportano i valori del caso sviluppato da CLAUDE.

Confronto del costo del sistema

Voce	MAKE (€, 3 anni)	BUY (€, 3 anni)
R&D / Licenze SaaS	250.000	180.000
Data ingestion/labeling / Integrazione API	90.000	45.000
Compute-GPU / Customizzazione	90.000	30.000
Stipendi Data Scientist / Canoni di supporto	540.000	45.000
Manutenzione ed evoluzione architetturale	120.000	-
TOTALE C_sistema	1.090.000	300.000

Confronto costi di compliance

Voce	MAKE (€, 3 anni)	BUY (€, 3 anni)
Obblighi ex-ante/post-market (MAKE) o da Deployer (BUY)	320.000	92.000
Normative trasversali (GDPR, NIS2/DORA, sicurezza sul lavoro)	70.000	70.000
TOTALE C_compliance	390.000	162.000

Confronto costo di sanzioni

Voce	MAKE (€, 3 anni)	BUY (€, 3 anni)
Probabilità ispezione	18%	12%
Probabilità di non-conformità	25%	15%
Sanzione stimata	€ 1.000.000	€ 400.000
Spese legali	€ 80.000	€ 30.000

Per il caso BUY manleva contrattuale recuperabile = 40% della quota di sanzione attribuibile al fornitore.

La valutazione di CLAUDE qui riportata è molto ottimistica per quanto attiene la probabilità di non conformità.

E[C_sanzioni_MAKE] = (0,18 × 0,25 × 1.000.000) + 80.000 = 45.000 + 80.000 = 125.000 €
E[C_sanzioni_BUY] = (0,12 × 0,15 × 400.000) + 30.000 = 7.200 + 30.000 = 37.200 €
E[C_sanzioni_BUY_netto] = 37.200 − (40% × 7.200) = 37.200 − 2.880 = 34.320 €

Confronto danni

Voce	MAKE (€, 3 anni)	BUY (€, 3 anni)
Frequenza incidenti	6%	5%
Danno medio	€ 350.000	€ 350.000
Copertura assicurativa netta attesa	6% × (300.000 − 60.000) = € 14.400.	5% × (200.000 − 40.000) = € 8.000

Manleva fornitore aggiuntiva = 50% della quota residua.

E[C_danni_MAKE] = (0,06 × 350.000) − 14.400 = 21.000 − 14.400 = 6.600 €
E[C_danni_BUY] = (0,05 × 350.000) − 8.000 = 17.500 − 8.000 = 9.500 €
E[C_danni_BUY_netto] = 9.500 − (50% × 9.500) = 9.500 − 4.750 = 4.750 €

Calcolo del TCO comparativo

Componente	MAKE (€)	BUY (€)
C_sistema	1.090.000	300.000
C_compliance	390.000	162.000
E[C_sanzioni]	125.000	34.320
E[C_danni]	6.600	4.750
TCO (totale, 3 anni)	1.611.600	501.070

© Clusit 2026

8. Conclusioni Operative

L'adeguamento all'AI Act richiede un approccio metodologico rigoroso basato sulle seguenti linee d'azione:

- evitare sovrastrutture burocratiche inadeguate: la maggior parte delle aziende utilizza strumenti a rischio minimo e non deve affrontare percorsi di conformità gravosi;
- prioritizzare censimento e classificazione: l'impiego di strumenti istituzionali come l'*EU AI ACT compliance checker* consente di definire il perimetro prescrittivo reale evitando inutili gap analysis;
- governare l'IA generativa: l'adozione di regole d'uso interne e il monitoraggio dei prompt costituiscono la misura principale per prevenire casi d'uso classificabili come ad alto rischio o pratiche vietate;
- validare le scelte make-or-buy con modelli quantitativi che prendano in considerazione l'impatto economico complessivo, le responsabilità legali e la quota di rischio trasferibile a terzi, in particolare per i sistemi ad alto rischio.

Shadow AI: il rischio invisibile nell'era dell'AI

Trend, sfide e strategie di governance per le organizzazioni

Dalla proliferazione silenziosa degli strumenti di AI non autorizzati, alle best practice per una governance sicura, responsabile e conforme al quadro normativo europeo.

[A cura di Federica Maria Rita Livelli]



Immagine illustrativa generata con Gemini

Introduzione

La Shadow AI si è affermata come una delle minacce più insidiose e a più rapida crescita nel panorama della cybersecurity aziendale. Non si tratta più di un fenomeno marginale legato a pochi utenti evoluti, ma di una pratica diffusa che può interessare ogni funzione aziendale, ogni settore e ogni livello organizzativo, con impatti diretti su: sicurezza dei dati, privacy, compliance e continuità operativa.

È inoltre fondamentale comprenderne le cause, riconoscerne le manifestazioni e misurarne i rischi, così da costruire strategie di risposta coerenti con il quadro normativo

© Clusit 2026

europeo in materia di sicurezza dei dati, protezione della privacy e cybersecurity, senza rinunciare ai benefici di produttività offerti dall'AI.

Che cos'è la Shadow AI?

Il termine Shadow AI indica l'uso non autorizzato o non governato di strumenti di AI che i dipendenti adottano in autonomia per aumentare la propria produttività, spesso aggirando i processi di governance ufficiali dell'organizzazione.

Secondo il rapporto Deloitte *"2026 State of AI in the Enterprise"*, l'accesso dei lavoratori a strumenti di AI è cresciuto del 50% nel solo 2025. Inoltre, solo un'azienda su cinque dispone, oggi, di un modello di governance sufficientemente maturo per supervisionarne l'uso effettivo.

Shadow AI vs. Shadow IT: differenze e sfide

È doveroso evidenziare che la Shadow AI rappresenta un'evoluzione del più noto fenomeno dello Shadow IT, ma presenta caratteristiche proprie che la rendono più pervasiva e più difficile da controllare: non riguarda soltanto l'adozione di software non approvato, ma anche l'elaborazione di dati, la generazione di contenuti e l'automazione di decisioni o di attività operative.

Inoltre, lo Shadow IT è tradizionalmente adottato da utenti tecnicamente preparati, al contrario, la Shadow AI può coinvolgere qualsiasi dipendente: man mano che gli strumenti di AI diventano più accessibili e *user-friendly*, vengono adottati senza l'approvazione formale dei team IT e di sicurezza.

Ancora, se da un lato questi strumenti di Shadow AI possono aumentare la produttività, automatizzare compiti e colmare lacune nei flussi di lavoro, dall'altro operano spesso al di fuori della visibilità dei team di sicurezza, bypassando i controlli e creando nuovi punti ciechi.
Infine, la Shadow AI coinvolge sistemi che elaborano, generano e, spesso, conservano dati sensibili, con un potenziale di esposizione strutturalmente più elevato dei dati, di superfici d'attacco ampliate e di sicurezza delle identità indebolita.

La Shadow AI: un fenomeno in rapida espansione

I dati si seguito riportati sono tratti principalmente dal report *"The State of Shadow AI 2026"* di Unseen Security, che raccoglie e sintetizza statistiche provenienti da ricerche di IBM, Microsoft, Gartner, Forrester, Salesforce, Netskope, Awareways, Software AG, CybSafe e National Cybersecurity Alliance, oltre a ulteriori report di Verizon, Reco, Proofpoint, World Economic Forum (WEF) e Cloud Security Alliance (CSA).

I report citati confermano un'adozione sempre più massiva dell'AI generativa nelle organizzazioni, a una velocità superiore alla capacità di molte aziende di governarla. In questo scenario, la Shadow AI rappresenta una delle principali aree di rischio emergente per la cybersecurity, la protezione dei dati e la compliance normativa.

In particolare, secondo il *"Shadow AI Trend Report 2025"* di Awareways, il 59% dei dipendenti utilizza abitualmente strumenti di Shadow AI e soltanto il 16% ricorre esclusivamente a strumenti autorizzati dall'organizzazione. Il report "AI *Oversight Gap*" di Optro rileva, inoltre, che l'80% delle organizzazioni segnala un utilizzo da moderato a diffuso della Shadow AI.

Il *"Work Trend Index 2024"* di Microsoft, realizzato in collaborazione con LinkedIn, evidenziava già che il 78% dei lavoratori utilizzava strumenti AI personali sul lavoro, fenomeno noto come *BYOAI (Bring Your Own AI)*.

Ancora, il *"Cloud & Threat Report 2026"* di Netskope rileva che il 47% degli utenti di AI generativa accede alle piattaforme tramite account personali, bypassando i controlli aziendali; mentre secondo il già citato report di Awareways il 54% dei dipendenti installa strumenti di AI senza coinvolgere il proprio reparto IT.

Il quadro trova conferma anche nel *"2026 Data Breach Investigations Report"* di Verizon, che segnala un utilizzo regolare dell'AI nel lavoro da parte di una quota significativa di professionisti e un ricorso frequente ad account personali non autorizzati, ampliando i punti ciechi per i team IT, oltre che aumentare la probabilità di esposizione dei dati aziendali.

Inoltre, lo *"2025 State of Shadow AI Report"* di Reco conferma la natura sistemica del fenomeno, stimando che il 91% degli strumenti di AI presenti negli ambienti aziendali operi al di fuori del controllo dell'IT, con una media di 269 applicazioni Shadow AI ogni 1.000 dipendenti.

L'aspetto preoccupante di questo scenario è che si sta assistendo a una progressiva perdita di controllo da parte dei dipartimenti IT. Inoltre, il problema non riguarda soltanto ChatGPT o Copilot, dato che la Shadow AI comprende oggi centinaia di servizi SaaS, estensioni browser, plug-in per ambienti di sviluppo, strumenti di traduzione, generatori di immagini, agenti autonomi e funzionalità integrate nei software aziendali, spesso attivate automaticamente, senza una preventiva valutazione del rischio.

© Clusit 2026



Immagine illustrativa generata con Gemini

Il governance gap: la nuova frontiera del rischio aziendale

Come già evidenziato, la criticità principale nell'era dell'AI non risiede nella sua adozione, ma nel crescente divario tra la velocità dell'innovazione tecnologica e la capacità delle organizzazioni di governarne il rischio. Una carenza definita come *governance gap* e che rappresenta una vulnerabilità strutturale che espone le aziende a rischi crescenti.

Il divario parte dal vertice: mancanza di competenze e di maturità - Le difficoltà di governance spesso si originano ai massimi livelli decisionali. Secondo la ricerca *"2026 State of AI in the Enterprise"* di Deloitte risulta che:

- Il 66% dei board dichiara di avere poca o nessuna esperienza in materia di AI.
- Solo una azienda su cinque possiede un modello di governance maturo per supervisionare l'uso reale dell'AI.

L'assenza di policy e il problema della "Shadow AI" - La mancanza di leadership si traduce in un vuoto operativo e regolamentare e, precisamente:

- **Visibilità IT minima -** Meno dell'11% delle applicazioni AI realmente in uso nei luoghi di lavoro è visibile ai team IT.
- **Controlli inefficaci -** Solo il 12% delle aziende è in grado di rilevare la totalità dello Shadow AI presente nel proprio perimetro. Il 43% non possiede alcuna policy specifica.

- **Cultura aziendale contraddittoria -** L'89% dei dipendenti dichiara di conoscere le regole sull'uso dell'AI, ma ammette di aggirarle nella maggioranza dei casi.

Le previsioni di Gartner e la necessità di accelerazione - Nonostante l'inerzia attuale, Gartner prevede una necessaria accelerazione: l'80% delle organizzazioni formalizzerà una policy AI entro il 2026 (rispetto al 37% di oggi). Un dato che segna una crescente consapevolezza da parte di board e C-level, ora costretti a dare priorità al tema della Shadow AI.

Il quadro globale: un rischio cyber in crescita - Il problema non è solo operativo, ma rappresenta un grave rischio di sicurezza su scala globale. Il *"Global Cybersecurity Outlook 2026"* del World Economic Forum (WEF) segnala che l'87% delle organizzazioni considera le vulnerabilità derivate dall'AI il rischio cyber in più rapida crescita.

Inoltre, tale vulnerabilità è amplificata dalla diffusione di agenti AI autonomi che si connettono a sistemi esterni (come i server MCP - *Model Context Protocol*) senza alcuna valutazione di sicurezza, convogliando "silenziosamente" dati aziendali sensibili verso destinazioni non verificate.

Le ricerche di Microsoft e Cloud Security Alliance (CSA) confermano la gravità della situazione:

- **Microsoft -** Il 75% dei CISO ha già scoperto strumenti GenAI non autorizzati nei propri ambienti.
- **Cloud Security Alliance -** L'86% delle organizzazioni non ha una visibilità completa sui flussi di dati diretti verso strumenti di AI, e solo il 37% possiede una policy strutturata.

© Clusit 2026



Immagine illustrativa generata con Gemini

L'urgenza dell'incident response e il ruolo del quadro normativo

La carenza di governance e di visibilità espone a rischi inevitabili. Lo *"State of AI Security Report 2025"* di Proofpoint evidenzia che il 49% delle organizzazioni prevede incidenti legati alla Shadow AI nei prossimi dodici mesi, mentre il 23% ammette di non essere adeguatamente preparato ad affrontarli.

Inoltre, il panorama normativo europeo rende la governance dell'AI un requisito sempre più rilevante: con l'introduzione dell'AI Act - insieme agli obblighi previsti da NIS2, DORA e GDPR - le organizzazioni dovranno dimostrare non solo di utilizzare sistemi conformi, ma anche di disporre di visibilità adeguata su chi utilizza quali strumenti, con quali dati, per quali finalità e con quali controlli.

Di fatto, senza adeguata visibilità sugli strumenti, sui dati e sulle modalità di utilizzo dell'AI, non può esistere una governance realmente efficace.

I costi della Shadow AI

La Shadow AI non è solamente un problema tecnologico o di compliance: produce un impatto economico diretto e misurabile sulle organizzazioni.

Secondo il "*Cost of a Data Breach Report 2026*" di IBM, la diffusione incontrollata della Shadow AI sta superando le capacità di difesa di molte aziende. Il report evidenzia, inoltre, che gli incidenti di sicurezza che coinvolgono la Shadow AI sono più

che raddoppiati nel 2026, passando dal 20% al 43% delle organizzazioni violate.

Ancora, gli incidenti legati all'Shadow AI stanno generando sanzioni in circa un caso su cinque. Si tratta di un dato significativo perché mostra come la Shadow AI sia passata da problema di controllo interno a rischio normativo.

Di fatto, quando un dipendente inserisce dati di un cliente in un chatbot non autorizzato per redigere una risposta più rapida, non viola soltanto una policy aziendale: può determinare una potenziale violazione del GDPR, soprattutto se i dati includono informazioni personali identificabili (PII – *Personal Identifiable Information*) o informazioni sanitarie protette (PHI – *Protected Health Information*), con possibili obblighi di notifica e rischio di sanzioni.



Shadow AI: Dati, Costi e Impatti - Immagine illustrativa generata con Gemini sulla base dei dati IBM, "*Cost of a Data Breach Report 2026*".

A questi costi diretti si aggiungono impatti indiretti spesso sottovalutati, tra cui:

- Perdita di fiducia da parte di clienti e partner
- Rallentamento dei processi decisionali
- Incremento delle attività di audit
- Revisione delle policy aziendali
- Maggiore esposizione al rischio reputazionale.

L'impatto cresce ulteriormente quando l'uso non autorizzato dell'AI coinvolge informazioni strategiche, codice sorgente, dati personali o documentazione riservata: in questi casi la Shadow AI diventa un vero moltiplicatore del rischio aziendale, capace

di compromettere contemporaneamente sicurezza informatica, continuità operativa e conformità normativa.

Le cause strutturali del fenomeno della Shadow AI

Quattro fattori organizzativi principali alimentano la diffusione della Shadow AI:

- **Accessibilità universale degli strumenti AI -** I moderni strumenti di AI non richiedono competenze tecniche né processi di approvazione: i dipendenti possono accedere immediatamente a potenti modelli linguistici e strumenti di automazione.
- **Carenza di governance e policy -** In assenza di politiche chiare sull'uso dell'AI, i dipendenti decidono autonomamente quali strumenti usare e come, spesso senza comprenderne le implicazioni di sicurezza.
- **Bisogni aziendali insoddisfatti -** Quando le soluzioni approvate non rispondono ai requisiti operativi, i dipendenti adottano strumenti AI per colmare lacune di produttività o velocizzare il lavoro.
- **Il fenomeno del "vibe coding" -** Costruire applicazioni rapidamente tramite prompt in linguaggio naturale, senza adeguati accordi di gestione dei dati, può far trapelare codice proprietario, dati dei clienti e segreti aziendali nei dataset pubblici di addestramento.

La tassonomia dei rischi

La Shadow AI genera rischi interconnessi che possono essere ricondotti alle macro-aree, di seguito riportate, che consentono di leggere il fenomeno non come una serie di minacce isolate, ma come un insieme di vulnerabilità tecniche, organizzative e regolatorie che si rafforzano reciprocamente.

Esposizione e fuga di dati - Dipendenti e sviluppatori, per velocizzare le attività quotidiane, possono inserire nelle piattaforme di AI generativa informazioni riservate, come dati dei clienti, informazioni finanziarie, documenti aziendali, proprietà intellettuale o frammenti di codice contenenti chiavi API, credenziali e token di accesso. Una volta inseriti, questi dati escono dal perimetro aziendale e l'organizzazione perde visibilità su come vengano conservati, elaborati o riutilizzati. Ai sensi del GDPR, un trasferimento incontrollato di questo tipo può costituire una violazione soggetta a notifica obbligatoria.

Espansione della superficie d'attacco - Ogni strumento non approvato può includere API o plugin non verificati, e l'accesso tramite account o dispositivi personali colloca l'attività al di fuori dei controlli di sicurezza aziendali, rendendola invisibile al monitoraggio di rete tradizionale.

Manipolazione degli agenti AI e disinformazione - Gli agenti AI progettati per agire autonomamente, ad esempio prenotando viaggi, accedendo a database o interagendo con sistemi esterni, possono eseguire azioni indesiderate se manipolati tramite prompt injection, data poisoning o istruzioni malevole. Il rischio non riguarda solo l'accuratezza delle risposte, ma anche la possibilità che l'agente compia operazioni non autorizzate con impatti su processi aziendali, integrità delle informazioni e continuità operativa.

Malware potenziato dall'AI e rischi di supply chain - Le minacce più recenti sfruttano gli stessi strumenti AI degli sviluppatori per automatizzare il furto di credenziali e propagarsi lungo l'intera catena software dell'organizzazione, estendendo l'impatto a partner e clienti.

Impatto sulla gestione delle identità (IAM - Identity and Access Management) - La proliferazione di account personali su piattaforme AI e di account di servizio non supervisionati genera nuove identità, sia umane sia non umane (NHI, *Non-Human Identity*), aumentando il rischio di escalation di privilegi e accessi non autorizzati difficili da governare.

Elusione dei controlli di sicurezza tradizionali - La maggior parte delle piattaforme AI comunica tramite connessioni HTTPS cifrate, rendendo difficile per i controlli tradizionali analizzare i contenuti senza funzionalità di ispezione SSL/TLS. Inoltre, i modelli di comunicazione delle applicazioni conversazionali differiscono da quelli aziendali, complicando il monitoraggio e aumentando il rischio di esfiltrazione dei dati.

Rischi di compliance - In materia di compliance, la Shadow AI può rendere più difficile dimostrare il rispetto degli obblighi previsti da AI Act, NIS2, DORA e GDPR, soprattutto quando l'organizzazione non dispone di visibilità sugli strumenti utilizzati, sui dati trattati e sulle finalità d'uso.

È doveroso ricordare che l'AI Act europeo prevede un sistema sanzionatorio significativo, con importi che possono arrivare fino al 7% del fatturato annuo globale per le violazioni più gravi; in questo contesto, Gartner prevede che oltre il 40% delle organizzazioni sperimenterà incidenti di conformità e sicurezza legati alla Shadow AI entro il 2030.

Gestione e mitigazione della Shadow AI: strategie di compliance e best practice aziendali

Le organizzazioni, per arginare i rischi legati all'utilizzo incontrollato della Shadow AI, dovrebbero adottare un modello integrato articolato nelle seguenti quattro aree

che costituiscono componenti complementari di un unico sistema di compliance e di gestione del rischio.

1. Visibilità e controllo tecnico

Inventario delle applicazioni AI - Non è possibile proteggere ciò che non si conosce: è necessario implementare meccanismi di rilevamento tramite log di rete e proxy, piattaforme di gestione SaaS (*Software-as-a-Service*) e monitoraggio delle chiamate API non approvate, delle estensioni browser e delle integrazioni non autorizzate.

Limiti tecnici - Prevenzione della perdita di dati (*Data Loss Prevention* - DLP) sugli endpoint, per impedire l'inserimento di dati sensibili -PII (*Personally Identifiable Information)* o codice proprietario - in strumenti AI non autorizzati; alternative di livello enterprise conformi, ospitate nell'UE o contrattualizzate (ad esempio istanze Azure OpenAI Service o modelli on-premise).

Valutazioni del rischio unificate - Far confluire tutti gli strumenti AI approvati in un inventario centralizzato dei trattamenti dei dati ai fini GDPR; monitorare i termini di servizio dei fornitori per dimostrare la resilienza della catena di approvvigionamento ai sensi di NIS2 e DORA; effettuare una FRIA per i sistemi AI utilizzati in contesti ad alto rischio.

2. Governance, responsabilità e compliance

Governance continua e alfabetizzazione in materia di AI - Adottare lo standard ISO/IEC 42001 per formalizzare un sistema di gestione dell'AI e garantire a dirigenza e dipendenti un livello adeguato di alfabetizzazione sull'AI, come richiesto dall'AI Act.

Stabilire una politica di AI responsabile - Definire i tipi di dati che i dipendenti possono elaborare, le attività vietate e i protocolli di sicurezza da seguire, richiedendo che ogni nuovo progetto AI sia sottoposto a revisione e approvazione IT prima dell'implementazione; aggiornare la policy con la stessa velocità con cui evolve la tecnologia.

Assegnare accountability chiara - Designare un team o un responsabile che supervisioni l'uso dell'AI, mantenga la conformità e gestisca i rischi, con ruolo e autorità ben definiti.

Favorire la collaborazione interdisciplinare – Le funzioni di IT, sicurezza, conformità e business devono collaborare per definire standard coerenti di selezione, integrazio-

ne e monitoraggio degli strumenti AI, considerando che regole condivise rendono le lacune di sicurezza più facili da individuare.

Procedere per gradi (governance incrementale) - Avviare programmi pilota in ambienti controllati per poi estendere progressivamente l'adozione, riducendo il sovraccarico di governance e la resistenza al cambiamento.

Offrire alternative sicure e approvate - Mettere a disposizione strumenti di AI aziendali che rispondano realmente alle esigenze operative dei dipendenti, così da ridurre l'incentivo all'uso di soluzioni consumer non autorizzate. Le licenze enterprise, se correttamente configurate e contrattualizzate, consentono standard superiori di sicurezza, privacy, controllo sui dati e auditabilità.

Definire un framework di governance strutturato - Stabilire policy chiare per l'utilizzo dell'AI nell'organizzazione, definendo ruoli, responsabilità, processi di approvazione, criteri di classificazione dei dati e controlli minimi di sicurezza. Il framework dovrebbe includere anche procedure per la valutazione dei bias, la documentazione delle decisioni e il riesame periodico degli strumenti approvati.

3. Adozione sicura e supporto agli utenti

Istituire strutture organizzative dedicate - Creare una funzione – i.e. centro di eccellenza - per centralizzare la gestione delle iniziative di AI, coordinando in modo coerente la strategia, l'adozione e la supervisione dei sistemi.

Investire in formazione e cultura della sicurezza - Promuovere programmi formativi continui, calibrati sul ruolo degli utenti, per spiegare non solo i benefici dell'AI, ma anche i rischi legati a dati personali, informazioni riservate, proprietà intellettuale, codice sorgente e credenziali. Una formazione pratica, basata su casi d'uso realistici, aiuta i dipendenti a riconoscere quando uno strumento non è conforme e a scegliere alternative approvate.

Garantire supporto continuo - Affiancare alla formazione help desk, guide operative e strumenti di adozione digitale, così da rendere semplice per i dipendenti segnalare nuovi strumenti e porre domande.

Aggiornare i processi con continuità - Programmare revisioni periodiche delle policy per incorporare nuove best practice, affrontare i rischi emergenti e allinearsi agli obiettivi aziendali in evoluzione, coinvolgendo team interdisciplinari e raccogliendo il feedback dei dipendenti.

Implementare politiche e controlli operativi - Adottare policy specifiche per regola-

mentare la condivisione dei dati con gli strumenti di AI; garantire una stretta sinergia tra business e IT per assicurare la conformità agli standard di sicurezza e performance.

Consentire la sperimentazione controllata - Predisporre "sandbox" o ambienti protetti e monitorati in cui i team possano testare nuove applicazioni di AI in totale sicurezza, ricorrendo esclusivamente a versioni enterprise che impediscano l'uso di dati sensibili per il training dei modelli.

4. Monitoraggio continuo e miglioramento

Garantire trasparenza e monitoraggio continuo - Comunicare apertamente i vantaggi dell'uso responsabile dell'AI, spiegando come vengono trattati i dati dagli strumenti approvati; utilizzare strumenti di quality assurance per verificare regolarmente i risultati e individuare utilizzi non autorizzati.

Strumenti e tecnologie a supporto della gestione della Shadow AI

Gli strumenti tecnologici a supporto della gestione della Shadow AI dovrebbero aiutare le organizzazioni a rilevare utilizzi non autorizzati e monitorare flussi di dati anomali. In particolare, risultano rilevante:

Integrare i controlli con IAM e DLP - Estendere le policy di prevenzione della perdita di dati e la gestione delle identità, umane e non umane, a tutti gli strumenti AI, applicando il principio del privilegio minimo e l'autenticazione a più fattori.

Adottare una soluzione di AI-BOM (AI Bill of Materials) - Offre una fotografia delle configurazioni di un sistema AI in un dato momento, facilitando l'identificazione di modifiche, compromissioni o deviazioni rispetto allo stato atteso.

Implementare piattaforme AI Control Plane - Piattaforme indipendenti che identificano e valutano in modo continuo l'attività AI, offrendo ai team di sicurezza la visibilità necessaria a gestire i rischi emergenti senza affidarsi alla registrazione manuale.

Adottare soluzioni CASB e SSPM - I *Cloud Access Security Broker* (CASB) e le soluzioni di *SaaS Security Posture Management* (SSPM) possono essere configurati per rilevare il traffico verso endpoint AI noti e applicare controlli coerenti con le policy aziendali.

I vantaggi di una governance efficace della Shadow AI

La gestione efficace della Shadow AI implica costruire una cultura di uso responsabile e sicuro dell'AI, ovvero: rendere semplice per i dipendenti segnalare nuovi strumenti, aggiornare le policy con continuità e far collaborare IT, sicurezza e business su linee

guida condivise. Ciò si traduce in benefici concreti, quali:

- Piena visibilità su quali strumenti AI sono in uso e a quali dati accedono.
- Riduzione dell'esposizione regolatoria rispetto a framework come GDPR, HIPAA (Health Insurance Portability and Accountability Act, normativa statunitense su privacy e sicurezza dei dati sanitari, spesso rilevante per i gruppi multinazionali) ed EU AI Act.
- Adozione dell'AI più rapida e sicura, grazie a strumenti verificati e linee guida complete.
- Maggiore adozione di strumenti AI approvati, con conseguente riduzione della dipendenza da alternative non sicure.
- Auditabilità e documentazione solide, a beneficio di revisori e autorità di controllo.

Conclusione

La Shadow AI non è più soltanto una deviazione dai processi IT o una violazione delle policy aziendali: è diventata una questione strutturale di governance, cybersecurity, protezione dei dati e compliance normativa.

Ogni utilizzo non autorizzato di strumenti AI può esporre l'organizzazione a perdita di controllo sui dati, violazioni del GDPR, inefficienze operative, responsabilità legali e rischi reputazionali. Per questo motivo, le organizzazioni non possono limitarsi a vietare l'uso dell'AI o a inseguire singoli comportamenti non conformi.

Pertanto, si consiglia di costruire un modello di governance fondato su visibilità continua, inventario degli strumenti, controllo degli accessi, classificazione dei dati, formazione degli utenti e disponibilità di alternative enterprise sicure.

Strumenti come l'AI-BOM e standard come ISO/IEC 42001 indicano una direzione ormai chiara: la governance dell'AI è destinata a diventare una componente stabile dei sistemi di gestione aziendali, al pari della sicurezza delle informazioni e della gestione del rischio operativo.

La vera sfida, quindi, non è impedire ai dipendenti di utilizzare l'AI, ma permettere loro di farlo in modo sicuro, tracciabile e conforme. Inoltre, le imprese capaci di colmare il divario tra innovazione e controllo potranno trasformare la Shadow AI da rischio invisibile a leva di competitività, di fiducia e di resilienza digitale.

Fonti

- Cloud Security Alliance (CSA) – "The Invisible Enterprise: Shadow AI and the Ungoverned Frontier" - https://labs.cloudsecurityalliance.org/research/csa-whitepaper-shadow-ai-asset-blindness-systemic-risk-20260/
- Deloitte — "The State of AI in the Enterprise: 2026 AI Report" — https://www.deloitte.com/us/en/what-we-do/capabilities/applied-artificial-intelligence/content/state-of-ai-in-the-enterprise.html
- Gartner — "Gartner Identifies Critical GenAI Blind Spots That CIOs Must Urgently Address" — https://www.gartner.com/en/newsroom/press-releases/2025-11-19-gartner-identifies-critical-genai-blind-spots-that-cios-must-urgently-address0
- IBM — "Cost of a Data Breach Report 2026" — https://www.ibm.com/reports/data-breach
- Microsoft — "2024 Annual Work Trend Index from Microsoft and LinkedIn" — https://news.microsoft.com/annual-wti-2024/
- Netskope — "Cloud and Threat Report: 2026" — https://www.netskope.com/resources/cloud-and-threat-reports/cloud-and-threat-report-2026
- Optro — "The AI Oversight Gap: Adoption is Scaling. Governance Controls Aren't" — https://optro.ai/resources/ebook/the-ai-oversight-gap-adoption-is-scaling-governance-controls-arent
- Proofpoint – "State of AI Security Report 2025" - https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-the-state-of-ai-security-2025.pdf
- Reco — "2025 State of Shadow AI Report" — https://www.reco.ai/state-of-shadow-ai-report
- Salesforce — "New Slack Research: Daily AI Usage Among Workers Surges 233%" — https://www.salesforce.com/news/stories/daily-ai-workforce-use-growth/
- Verizon — "2026 Data Breach Investigations Report" — https://www.verizon.com/business/en-en/resources/reports/dbir/
- Unseen Security — "The State of Shadow AI 2026" — https://www.unseensecurity.ai/shadow-ai-report
- World Economic Forum (WEF) — "Global Cybersecurity Outlook 2026" — https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

NOTA – AI Disclosure (AI Act 2025 – Legge italiana 132/2025) – Il presente contenuto testuale è stato realizzato da *Federica Maria Rita Livelli* con il supporto di strumenti di intelligenza artificiale, tra cui Gemini, ChatGPT e Copilot, per attività di revisione editoriale e ottimizzazione SEO, sotto la supervisione e responsabilità editoriale dell'autrice, nel rispetto dei principi di trasparenza, accuratezza e responsabilità.

La maturità cyber delle mPMI italiane dalle evidenze del PID Cyber Check 2025

[A cura di Georgia Cesarone, Paola Girdinio, Giovanni Manigrasso, Fabio Martinelli, Alessio Misuri, Antonio Romeo, Paolo Spagnoletti, Giorgia Tombesi, Artsiom Yautsiukhin]

Quasi tremila imprese, un'unica metrica di rischio ed una fotografia di un anno e mezzo che mette in discussione due luoghi comuni ancora molto diffusi:

1) che la piccola impresa sia troppo piccola per interessare agli attaccanti, convinzione smentita ormai troppo spesso dall'esperienza diretta delle imprese;
2) che il divario digitale tra Nord e Sud si traduca automaticamente in un analogo divario nell'esposizione alle minacce cyber.

L'edizione 2025 del PID Cyber Check, lo strumento di autovalutazione, promosso da Unioncamere e dal sistema delle Camere di Commercio attraverso la rete dei Punti Impresa Digitale, offre uno dei pochi osservatori su scala nazionale costruiti a partire direttamente dalle imprese, comprese quelle realtà di minori dimensioni che affrontano il rischio cyber disponendo spesso di risorse limitate, sia in termini di budget che in termini di competenze.

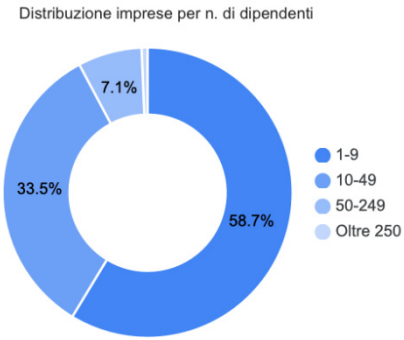
Lo strumento è il risultato di un percorso di collaborazione tra il sistema camerale, il mondo della ricerca e i Competence Center nazionali. Il modello originario è stato predisposto dall'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche (IIT-CNR) e successivamente sviluppato nell'ambito del sistema dei PID con il contributo degli esperti di DINTEC e dei Competence Center CYBER 4.0 e START 4.0. La sua evoluzione ha progressivamente consolidato un modello di self-assessment pensato specificamente per le mPMI con l'obiettivo di offrire uno strumento semplice ed accessibile per una prima valutazione della propria esposizione al rischio cyber.

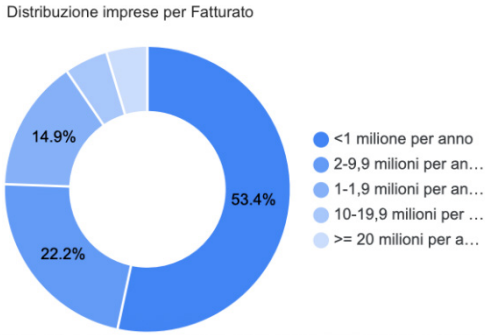
Il nuovo modello, conservando l'impostazione basata sui tre pilastri di tecnologie, processi e persone, amplia la lettura della maturità aziendale. Accanto ai temi ormai consolidati - infrastruttura IT, dati trattati, aggiornamenti, backup, controllo degli accessi e protezione degli endpoint - trovano maggiore spazio la gestione delle risorse critiche, la selezione dei fornitori, il presidio normativo, gli audit, la formazione e le procedure di ripristino. Questa evoluzione consente di passare da una fotografia delle singole misure adottate a una valutazione più ampia della capacità dell'impresa di identificare, proteggere, rilevare, rispondere e recuperare.

Il modello di valutazione amplia, quindi, la rappresentazione della postura cyber delle imprese, distinguendo due componenti complementari: le fonti di rischio e le capacità di mitigazione. Questa articolazione permette di osservare, da un lato, le condizioni che possono rendere l'impresa maggiormente vulnerabile e, dall'altro, la capacità organizzativa e tecnica di prevenire, rilevare e gestire gli incidenti informatici.

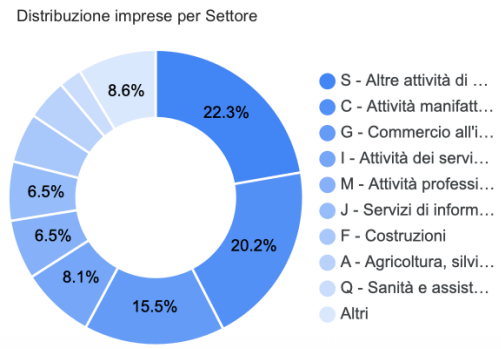
Questa impostazione consente di superare una lettura limitata alla semplice presenza o assenza di singole misure di sicurezza. La postura cyber viene così rappresentata come il risultato dell'equilibrio tra il livello di rischio a cui l'impresa è esposta e la sua capacità di identificarlo, prevenirlo e gestirne gli effetti. Un'impresa può infatti disporre di numerose misure tecniche e rimanere comunque vulnerabile se non conosce i propri asset critici, non rileva tempestivamente gli incidenti o non dispone di procedure adeguate di risposta e ripristino.

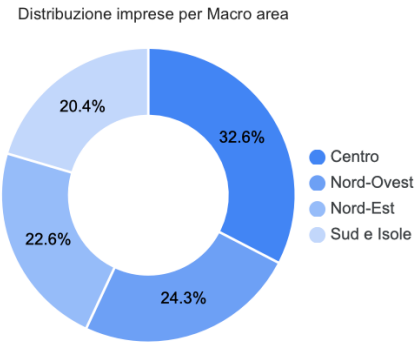
Il campione rilevato conta ben 2.873 imprese e restituisce un profilo fortemente caratterizzato dalla presenza delle realtà di minori dimensioni. Quasi sei imprese su dieci hanno meno di dieci dipendenti, circa un terzo si colloca tra 10 e 49 addetti, le medie imprese pesano per circa il 7%, mentre le grandi rappresentano una presenza marginale, con appena 19 organizzazioni. D'altra parte, lo strumento si rivolge esplicitamente alle mPMI e, coerentemente, oltre metà dei rispondenti dichiara un fatturato inferiore al milione di euro.





Sul piano settoriale emergono i servizi alla persona e le altre attività di servizi, la manifattura e il commercio, seguiti a distanza da alloggio e ristorazione, attività professionali e servizi di informazione e comunicazione. La distribuzione territoriale vede il Centro come area maggiormente rappresentata con circa un terzo delle imprese, seguito da Nord-Ovest, Nord-Est e Sud e Isole, con quote comprese tra un quinto e un quarto.





Va detto con chiarezza che non si tratta di un campione statistico rappresentativo dell'intero sistema produttivo italiano. L'adesione al PID Cyber Check è volontaria e sia le vulnerabilità sia gli incidenti sono dichiarati dalle imprese e non verificati attraverso attività tecniche. Questa caratteristica costituisce un limite metodologico di cui tenere conto nell'interpretazione dei risultati, ma rappresenta al tempo stesso un elemento di interesse: i dati restituiscono infatti la percezione, il livello di consapevolezza e l'esperienza diretta di una popolazione di imprese che spesso rimane ai margini delle statistiche sugli incidenti cyber più significativi.



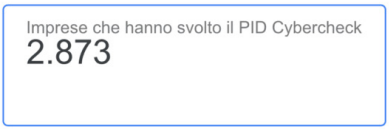
L'indicatore di rischio aggregato, espresso su una scala da 0 a 100 in cui valori più elevati indicano una maggiore esposizione, si attesta a 50,7. Il dato di sintesi è significativo, ma lo è ancora di più la sua distribuzione poiché oltre nove imprese su dieci ricadono nella fascia di rischio medio, mentre le fasce estreme, bassa e alta, raccolgono complessivamente solo una quota ridotta del campione. Questa concentrazione nella fascia centrale merita una lettura attenta, perché più che descrivere un sistema equilibrato, restituisce l'immagine di una maturità ancora intermedia nella quale i presidi di base possono essere presenti senza essere necessariamente inseriti in un processo strutturato e continuativo di governo del rischio.

È una condizione particolarmente rilevante per le mPMI nelle quali la disponibilità di strumenti tecnologici non coincide automaticamente con la presenza di procedure, responsabilità definite, capacità di monitoraggio e processi di risposta agli incidenti.

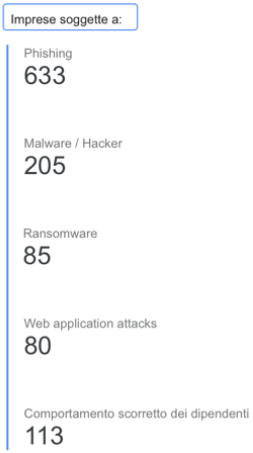
© Clusit 2026

Il rischio medio, in altre parole, non deve essere interpretato come una condizione di sicurezza acquisita, ma come l'indicazione di una postura che presenta ancora margini significativi di miglioramento lato governance.

Il dato più netto dell'edizione 2025 riguarda l'esperienza diretta: infatti, 781 imprese su 2.873, pari a circa il 27%, dichiarano di essere oggetto di attacchi informatici. È una proporzione particolarmente significativa se letta alla luce della composizione del campione e contribuisce a superare definitivamente l'idea che le organizzazioni di minori dimensioni siano poco interessanti per gli attaccanti.







Il phishing domina lo scenario e riguarda oltre otto imprese colpite su dieci e più di un quinto dell'intero campione. Seguono a distanza gli attacchi da malware o intrusione diretta, i comportamenti scorretti dei dipendenti, il ransomware e gli attacchi alle applicazioni web. Poiché la somma delle diverse tipologie di evento supera il numero complessivo delle imprese colpite, una parte dei rispondenti ha evidentemente dichiarato più di una tipologia di attacco. Il dato è coerente con scenari nei quali tecniche differenti possono concorrere alla stessa compromissione, anche se il questionario non consente di ricostruire la sequenza causale dei singoli eventi.

Due elementi meritano particolare attenzione. Il primo è costituito dal peso del fattore umano: phishing e comportamenti scorretti interni rappresentano una componente centrale dell'esposizione delle mPMI e confermano la necessità di affiancare agli investimenti tecnologici attività continuative di formazione, sensibilizzazione e definizione di procedure organizzative. Il secondo riguarda il ransomware, dichiarato da circa il 3% dell'intero campione. La percentuale può apparire contenuta, ma assume un peso diverso se rapportata alla capacità di risposta di una micro o piccola impresa, dove un evento di questo tipo può determinare indisponibilità prolungate dei sistemi, perdita di dati e conseguenze rilevanti sulla continuità operativa.

Scomponendo il campione per numero di addetti emerge una dinamica a due facce. Da un lato, l'indicatore di rischio è più alto proprio nelle micro imprese, dove raggiunge 52,4, mentre scende a 49,1 nella fascia tra 10 e 49 addetti e arriva a 44,3 nelle medie imprese tra 50 e 249 addetti. I dati mostrano dunque una relazione tra dimensione organizzativa e rischio rilevato dal modello. Dall'altro lato, la quota di imprese che dichiara attacchi segue la direzione opposta. Nelle micro imprese circa una su cinque dichiara di aver subito un attacco, nelle piccole si sale a quasi una su tre e nelle medie si arriva intorno alla metà. Il phishing passa da poco meno di un quinto delle micro imprese a oltre il 40% delle medie; il ransomware raddoppia tra micro e medie. Nel campione, anche la quota di imprese che dichiara episodi legati al comportamento dei dipendenti aumenta al crescere della dimensione aziendale.

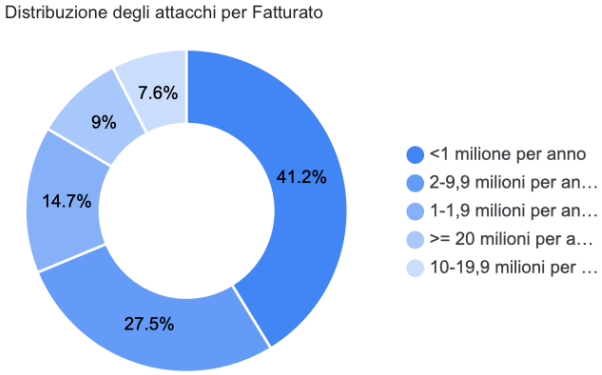
Questa apparente contraddizione rappresenta forse uno degli elementi più interessanti dell'analisi. Le imprese più strutturate presentano normalmente una superficie digitale più ampia data da più utenti e quindi più caselle di posta, più servizi online e un numero maggiore di relazioni con clienti e fornitori. Allo stesso tempo, possono disporre di capacità più elevate di monitoraggio e rilevazione degli incidenti.

Il PID Cyber Check, essendo uno strumento di self-assessment, non permette di stabilire quanto la differenza osservata dipenda dalla maggiore esposizione e quanto da una maggiore capacità di riconoscere gli eventi. Il basso numero di attacchi dichiarati dalle micro imprese, associato ad un indicatore di rischio più elevato, suggerisce tuttavia che il tema della capacità di rilevazione meriti particolare attenzione.

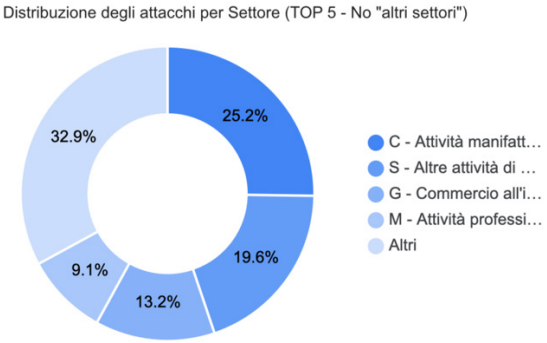
Il caso delle 19 grandi imprese presenti nel campione deve essere letto con particolare prudenza proprio per l'esiguità della numerosità. I risultati non consentono generalizzazioni, ma mostrano un indicatore di rischio intorno a 50, una quota di imprese in fascia alta superiore alla media del campione e una maggiore incidenza dichiarata degli attacchi alle applicazioni web. Si tratta di elementi compatibili con una superficie digitale esposta più ampia ed articolata, ma che richiederebbero un campione più esteso per poter essere interpretati in modo robusto.

Una lettura analoga può essere condotta rispetto al fatturato. Le imprese sotto il milione di euro, pur costituendo oltre metà del campione, rappresentano circa il 41% degli attacchi dichiarati, mentre le fasce superiori e, in particolare, quelle oltre i 10 milioni di euro, risultano proporzionalmente più presenti tra le imprese che dichiarano di aver subito un incidente. Il dato evidenzia una relazione tra dimensione economica e frequenza degli attacchi dichiarati, anche se il questionario non consente di stabilirne direttamente le cause. Maggiore digitalizzazione, più ampia superficie esposta, maggiore valore dei dati e maggiore capacità di rilevazione sono tutti fattori che possono contribuire al fenomeno.

© Clusit 2026



Il confronto tra la composizione settoriale del campione e quella delle imprese attaccate evidenzia due comparti particolarmente interessanti. La manifattura, che rappresenta circa un quinto dei rispondenti, raccoglie un quarto degli attacchi dichiarati, con un'incidenza stimabile intorno a un'impresa su tre. Ancora più marcato è il caso delle attività professionali, scientifiche e tecniche, che pesano per il 6,5% del campione ma per oltre il 9% degli attacchi.



Nel caso della manifattura, il dato assume particolare rilievo alla luce della progressiva integrazione tra sistemi IT e ambienti OT. Le attività professionali, scientifiche e tecniche, dal canto loro, operano frequentemente su informazioni di valore economico e strategico e fanno un uso intensivo di strumenti digitali e posta elettronica. Anche in questo caso, tuttavia, i dati del PID Cyber Check permettono di rilevare l'associazione e non di attribuirle una specifica relazione causale.

Servizi alla persona e commercio risultano invece leggermente sottorappresentati tra le imprese che dichiarano di aver subito attacchi. Il dato deve essere interpretato con cautela perché una minore frequenza dichiarata può riflettere una minore esposizione effettiva, ma può anche essere influenzata da differenze nella capacità di riconoscere e classificare gli incidenti.

La lettura geografica restituisce a sua volta un'immagine interessante con un indicatore di rischio che presenta un gradiente piuttosto netto: 48,4 nel Nord-Est, 49,2 nel Nord-Ovest, 52,2 al Centro e 52,8 nel Mezzogiorno. All'interno del campione analizzato, le imprese settentrionali mostrano dunque valori medi di rischio inferiori, anche se gli attacchi dichiarati seguono una distribuzione differente. Nel Nord-Ovest quasi quattro imprese su dieci riferiscono di aver subito un attacco, nel Nord-Est circa tre su dieci, al Centro poco più di una su cinque e nel Sud e nelle Isole meno di una su cinque. Anche il phishing presenta differenze rilevanti, coinvolgendo circa un terzo delle imprese nord-occidentali e meno del 15% di quelle meridionali.

È importante evitare di interpretare automaticamente questa distribuzione come una misura della pressione cyber effettiva nelle diverse aree del Paese. La composizione dimensionale e settoriale dei sottocampioni è differente e anche la capacità di riconoscere un incidente potrebbe incidere sulla frequenza dichiarata. Le imprese del Nord presenti nel campione risultano mediamente più strutturate e inserite in ecosistemi produttivi caratterizzati da un'elevata intensità di relazioni digitali. Nel Mezzogiorno pesa invece maggiormente la presenza di micro imprese. I dati suggeriscono quindi che esposizione, struttura organizzativa e capacità di rilevazione debbano essere lette congiuntamente. È importante sottolineare che un numero più basso di incidenti dichiarati non può essere considerato, da solo, un indicatore di minore rischio.

Anche la composizione settoriale degli attacchi riflette in parte le differenti caratteristiche territoriali del campione, visto che nel Centro e nel Mezzogiorno compare tra i comparti maggiormente rappresentati tra le imprese colpite quello dell'alloggio e della ristorazione, caratterizzato da un utilizzo diffuso di sistemi di prenotazione, pagamenti e piattaforme online, mentre al Nord emerge con maggiore evidenza il peso delle attività professionali. Si tratta di differenze che suggeriscono l'utilità di politiche di prevenzione capaci di tenere conto non soltanto della dimensione aziendale, ma anche delle specificità settoriali e territoriali.

© Clusit 2026

Focus - la gestione delle persone

Un ulteriore elemento di lettura riguarda il ruolo delle persone nella postura di sicurezza delle imprese. I dati mostrano infatti che il fattore umano non coincide soltanto con la possibilità che un dipendente cada vittima di phishing o adotti comportamenti non corretti, ma interessa più ampiamente il modo in cui vengono gestiti accessi, identità digitali, autorizzazioni e competenze. È proprio su questi aspetti che emergono alcune delle differenze più significative nell'indicatore di rischio.

Il dato più evidente riguarda la formazione. Quasi quattro imprese su dieci, il 39,9%, dichiarano di non prevedere programmi di formazione in materia di sicurezza informatica e presentano un indice medio di rischio pari a 60,4. L'indicatore scende progressivamente a 50,9 tra le imprese che hanno erogato occasionalmente corsi di base e a 41,8 quando tutto il personale è stato coinvolto in attività di sensibilizzazione. Il valore più basso, pari a 32,2, si osserva nelle imprese che affiancano alla formazione generalizzata interventi mirati per il personale in posizioni critiche e prevedono un aggiornamento periodico delle attività formative. Il divario tra i due estremi supera quindi i 28 punti e restituisce una relazione particolarmente netta tra strutturazione della formazione e livello di rischio rilevato dal modello. Il confronto va letto anche alla luce del fatto che le misure di mitigazione dichiarate, inclusa la formazione, contribuiscono al calcolo dell'indicatore.

Una dinamica analoga emerge nella gestione delle identità e degli accessi. Nel 32,9% delle imprese sono ancora presenti, per ragioni operative, utenze condivise tra più persone: in questo gruppo l'indice medio di rischio raggiunge 60,4. Il valore scende a 51,1 quando le utenze sono associate individualmente ai dipendenti, ma senza un monitoraggio continuo degli accessi, e arriva a 40,2 nelle imprese nelle quali le utenze sono esclusivamente personali e il loro utilizzo viene monitorato per individuare eventuali anomalie. Anche la gestione delle autorizzazioni evidenzia differenze significative: il 41,3% delle imprese dichiara che per accedere alle risorse è sufficiente la sola autenticazione e presenta un rischio medio pari a 59,1, contro 44,8 per le imprese che applicano in modo estensivo principi di privilegio minimo e separazione delle responsabilità.

Il ciclo di vita delle utenze costituisce un ulteriore elemento di attenzione. Nel 22,7% delle imprese non esiste una policy definita che assicuri la disattivazione delle credenziali associate al personale non più attivo e proprio questo gruppo presenta l'indicatore medio più elevato, pari a 63,0. Il rischio scende a 50,4 quando la disattivazione è effettuata periodicamente e a 45,7 quando è prevista immediatamente. Si tratta di un aspetto apparentemente operativo, ma che mostra quanto la sicurezza

dipenda anche dalla capacità di integrare la gestione degli accessi nei processi ordinari di entrata, permanenza e uscita del personale dall'organizzazione.

Più articolata risulta invece la lettura del lavoro da remoto. Le imprese che mettono a disposizione una connessione sicura tramite VPN presentano un indice medio di rischio pari a 44,4, mentre il valore sale a 59,3 quando i dipendenti accedono alla rete interna utilizzando dispositivi propri senza il controllo dell'impresa. Un valore relativamente contenuto, pari a 46,5, si osserva anche quando l'accesso remoto avviene esclusivamente attraverso dispositivi forniti dall'organizzazione. Merita attenzione, tuttavia, il fatto che le imprese nelle quali non è consentito alcun accesso remoto presentino comunque un indice pari a 56,2. Il dato suggerisce quindi che la semplice assenza di lavoro da remoto non costituisca di per sé un indicatore di maggiore sicurezza e che risulti invece determinante il modo in cui l'accesso viene governato quando è previsto.

Nel complesso emerge quindi una lettura del fattore umano più ampia rispetto alla sola sensibilizzazione degli utenti. Le imprese che combinano formazione continua, utenze personali, controllo degli accessi, corretta gestione delle autorizzazioni e procedure tempestive di disattivazione presentano sistematicamente valori di rischio inferiori. I dati non consentono di attribuire a ciascuna singola misura un effetto causale sull'indice, ma mostrano con chiarezza come la componente "persone" della cybersecurity sia strettamente intrecciata alla qualità dei processi organizzativi. Il capitale umano diventa così non soltanto una possibile fonte di vulnerabilità, ma uno degli elementi attraverso i quali costruire e mantenere nel tempo la capacità dell'impresa di governare il rischio cyber.

Le differenze osservate nella formazione e nella gestione delle utenze richiamano un problema concreto per le mPMI: tradurre le regole di sicurezza in compiti riconoscibili nel lavoro quotidiano. Se un collaboratore cambia mansione o lascia l'azienda, chi ne informa il gestore dei sistemi e chi controlla che gli accessi siano adeguati o revocati? Se arriva una segnalazione di phishing, chi la prende in carico e valuta gli interventi necessari? Anche quando l'informatica è affidata a un fornitore, queste decisioni richiedono un referente interno e un accordo chiaro sulle rispettive responsabilità. La formazione può sostenere questo presidio attraverso esercitazioni sulle situazioni di lavoro e procedure di segnalazione conosciute dal personale, collegando il riconoscimento della minaccia alla possibilità di intervenire.

La stessa chiarezza è necessaria per preparare la ripresa delle attività dopo un incidente. Disporre di copie di backup è un punto di partenza: occorre conoscere quali processi dipendano dai dati salvati, provare il ripristino e concordare con chi gestisce

© Clusit 2026

i sistemi l'ordine delle operazioni e i tempi di recupero compatibili con l'attività. Il profilo di gestione del rischio che affianca il punteggio nel nuovo report PID Cyber Check può orientare il confronto con l'impresa anche su questi aspetti. Nel percorso di accompagnamento, il risultato dell'autovalutazione acquista utilità quando si traduce in interventi proporzionati alle risorse disponibili, con responsabilità e scadenze definite. Il confronto successivo con il PID e, dove necessario, con le strutture specialistiche consente di fare il punto sulle azioni intraprese e sulle difficoltà ancora da affrontare.
Quando dall'autovalutazione emergono criticità su sistemi o servizi rilevanti per l'operatività, il percorso può essere affiancato da verifiche tecniche mirate. Vulnerability assessment e penetration test possono approfondire le debolezze dei sistemi e, nei rispettivi perimetri, verificare possibili modalità di sfruttamento. Queste attività possono aiutare l'impresa a definire le priorità di intervento e a verificarne l'attuazione, integrando la lettura organizzativa del PID Cyber Check con evidenze tecniche. Il punteggio dell'autovalutazione resta un elemento di orientamento e non costituisce una certificazione della sicurezza dei sistemi.

Conclusioni

L'edizione 2025 del PID Cyber Check consegna al dibattito sulla sicurezza delle mPMI italiane alcune indicazioni che si ritengono particolarmente rilevanti.

La prima riguarda la natura del problema confermando l'importanza che per le mPMI la sicurezza informatica non debba essere ridotta alla sola disponibilità di tecnologie di protezione. Il peso del phishing e degli eventi riconducibili al comportamento umano mostra quanto formazione continua, consapevolezza del rischio, procedure organizzative e responsabilità chiare e definite siano componenti essenziali della postura di sicurezza.

La seconda riguarda la capacità di vedere poiché l'evidente divario tra rischio misurato e numero di attacchi dichiarati pone il tema della capacità delle imprese di identificare e classificare gli incidenti. I dati disponibili non consentono di quantificare il fenomeno degli eventi non rilevati, ma indicano chiaramente la necessità di rafforzare non soltanto la prevenzione, ma anche le capacità di monitoraggio, rilevazione e risposta, rendendole economicamente e organizzativamente accessibili anche alle realtà di minori dimensioni.

La terza riguarda la filiera. Con il recepimento della direttiva NIS2 attraverso il D.Lgs. 138/2024, la maggior parte delle micro e piccole imprese non rientra direttamente nel perimetro degli obblighi in ragione della sola dimensione, ferme restando le

eccezioni previste dalla normativa. Molte di esse possono tuttavia essere coinvolte indirettamente in quanto fornitori di soggetti essenziali o importanti, chiamati a considerare i rischi connessi alla sicurezza della propria catena di approvvigionamento. In questo contesto, una manifattura nella quale circa un'impresa su tre del campione dichiara di aver subito un attacco rappresenta un segnale che merita attenzione. Strumenti di autovalutazione standardizzati e facilmente accessibili come il PID Cyber Check possono costituire un primo linguaggio comune tra committenti e fornitori e un punto di partenza verso percorsi più strutturati di gestione del rischio cyber lungo la filiera.

Al di là dei singoli numeri, il PID Cyber Check mostra inoltre il valore di un'infrastruttura di prossimità capace di portare il tema della cybersecurity all'interno di migliaia di micro, piccole e medie imprese. Il sistema camerale, attraverso i Punti Impresa Digitale, insieme al mondo della ricerca, a DINTEC e ai Competence Center coinvolti nell'evoluzione dello strumento, può trasformare l'autovalutazione nel primo passaggio di un percorso più ampio che porti dalla misurazione alla consapevolezza, dalla consapevolezza all'individuazione delle priorità, fino alla formazione e agli investimenti necessari per rafforzare la resilienza.
La fotografia che emerge in questo ultimo anno e mezzo è quindi quella di un sistema produttivo nel quale il rischio cyber è ormai un'esperienza concreta anche per le imprese di minori dimensioni, mentre la maturità presenta ancora ampi margini di crescita. Colmare questa distanza non significa necessariamente ricorrere a soluzioni straordinarie, ma significa soprattutto costruire governance a partire dall'analisi del rischio e diffondere capacità di rilevazione e risposta, mantenere un presidio vicino alle imprese. È su questo terreno che si gioca una parte significativa della sicurezza digitale del sistema economico italiano e, più in generale, del Sistema Paese.

© Clusit 2026

Cybersecurity nelle imprese modenesi: due anni a confronto, tra progressi organizzativi e ritardi tecnici

Analisi delle rilevazioni 2025–2026 e dei dati raccolti dalla Camera di Commercio di Modena, in base al questionario elaborato dall'Università di Modena e Reggio in collaborazione col Clusit

[A cura di Antonio Apruzzese, Mauro Cicognini, Mauro Andreolini, Mauro Leoncini, Mirco Marchetti e Giuseppe Molinari]

Introduzione

La cybersecurity sta progressivamente passando da questione prevalentemente tecnica a componente strutturale della gestione d'impresa. L'evoluzione delle minacce informatiche, la crescente dipendenza dai sistemi digitali e l'introduzione di nuovi obblighi normativi impongono alle organizzazioni di affrontare la sicurezza con un approccio più sistematico, che coinvolga non soltanto gli strumenti tecnologici, ma anche le responsabilità, le competenze e i processi aziendali.

In questo contesto, il confronto tra le rilevazioni condotte nel 2025 e nel 2026 presso le imprese del territorio modenese offre l'opportunità di osservare come stiano evolvendo alcune pratiche di sicurezza informatica e, soprattutto, se l'applicazione della direttiva NIS2 si accompagni a differenze riconoscibili nei comportamenti delle organizzazioni.

L'analisi restituisce un quadro articolato. Emergono segnali incoraggianti nella strutturazione delle funzioni IT e cybersecurity, nella formalizzazione delle procedure di gestione degli incidenti e nella formazione del personale. Su alcune misure tecniche, invece, i progressi risultano molto più contenuti, nonostante l'apparente semplicità delle misure in questione. Altri indicatori suggeriscono possibili cambiamenti, ma non offrono evidenze statistiche sufficientemente solide per trarre conclusioni.

Il dato più interessante che emerge dal confronto dei dati 2025 con i dati 2026 è probabilmente che **la cybersecurity sembra rafforzarsi più rapidamente sul piano organizzativo e procedurale che su quello delle protezioni tecniche effettivamente adottate**.

1. Campione e contesto organizzativo

L'indagine ha raccolto le risposte di 715 imprese nel 2025 e 669 nel 2026, raccolti in forma anonima sin dalla fonte. Non si tratta quindi necessariamente delle stesse organizzazioni, benché l'ampiezza del campione, rapportata al tessuto produttivo della provincia di Modena, renda assai probabile la presenza di molte organizzazioni in entrambi i campioni. Il confronto descrive il modificarsi della realtà in modo statistico aggregato, e non segue l'evoluzione di ciascuna impresa[1].

La composizione dimensionale risulta comunque relativamente stabile. Le imprese con meno di 50 addetti rappresentano il 71,5% dei rispondenti nel 2025 e il 72,0% nel 2026. Cambia invece la distribuzione interna delle aziende più piccole: aumentano le ditte individuali e le imprese con numero di addetti tra 2 e 9, mentre diminuisce il peso delle organizzazioni con 10–49 collaboratori. La quota delle imprese con almeno 50 addetti rimane sostanzialmente invariata.

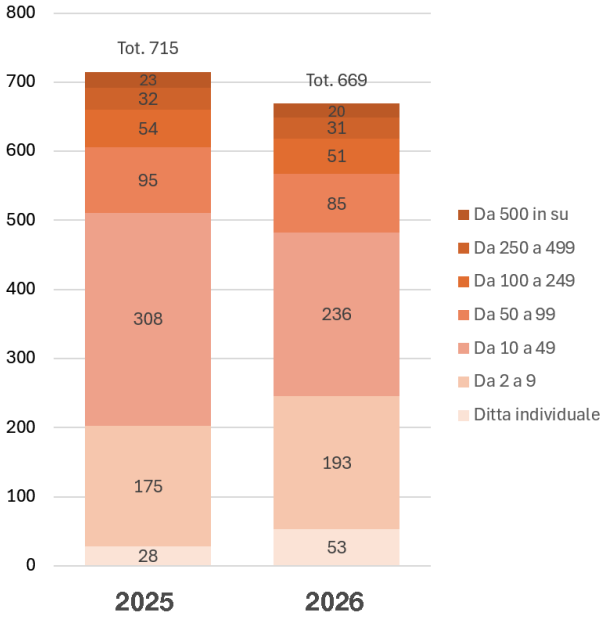


Figura 1 - Composizione dimensionale del campione, 2025–2026

[1] Le percentuali sono calcolate sui denominatori pertinenti ai singoli indicatori. Le analisi corrette per dimensione aziendale considerano le classi di addetti dichiarate. I dati si basano sulle dichiarazioni delle imprese partecipanti e non su verifiche tecniche indipendenti dell'effettiva implementazione o efficacia delle misure. Le due rilevazioni (2025 e 2026) costituiscono campioni distinti, non un panel longitudinale.

© Clusit 2026

Questa relativa continuità favorisce il confronto generale fra le due rilevazioni, ma non elimina le possibili distorsioni dovute alla composizione dei gruppi. La dimensione aziendale è infatti una delle variabili maggiormente associate alla disponibilità di personale specializzato, risorse economiche e processi formalizzati.

Il suo ruolo diventa ancora più importante quando si confrontano i soggetti tenuti agli adempimenti NIS2 con le altre imprese: i soggetti NIS sono (salvo rare eccezioni) almeno aziende medie, ragion per cui la loro dimensione media risulta superiore alla media complessiva; diversa è anche la distribuzione settoriale, dovuta naturalmente alla scelta dei settori regolati da parte del legislatore. Si è cercato quindi di tenere conto di questi bias intrinseci nell'esame dei dati.

Distribuzione per settore economico

La rilevazione 2026 mostra un campione economicamente eterogeneo. Il comparto manifatturiero, così come ci si aspetterebbe da una provincia come quella di Modena, è il più rappresentato tra i settori esplicitamente identificati, con 154 imprese, pari al 23,0% del totale. Seguono l'agroalimentare, con 53 imprese (7,9%), e l'edilizia, con 39 (5,8%). Sono presenti, inoltre, aziende dell'abbigliamento e moda, dei servizi ICT, delle infrastrutture digitali, della sanità, dei trasporti e di altri settori.

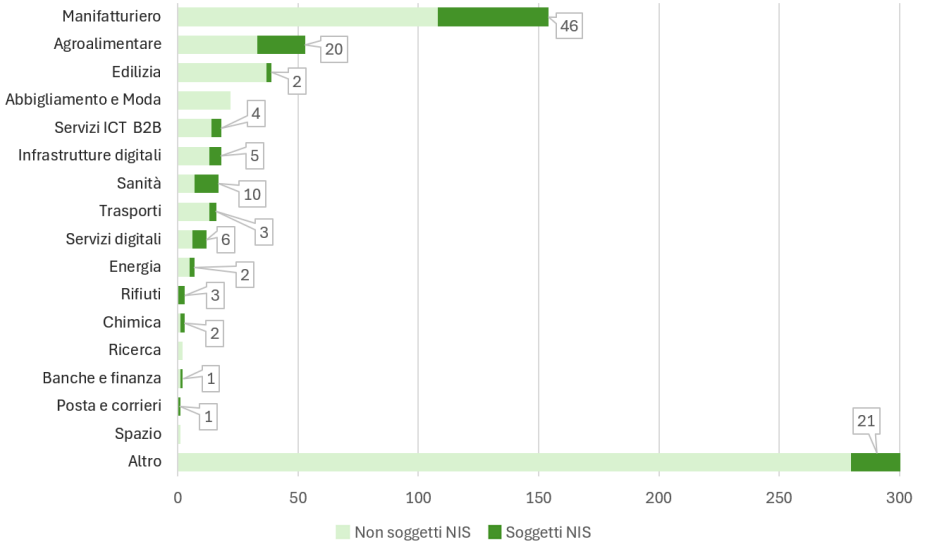


Figura 2- Distribuzione dei settori merceologici e classificazione NIS, 2026

La segmentazione NIS evidenzia differenze importanti anche nella distribuzione settoriale. Tra i 126 soggetti classificati come NIS nel 2026, il manifatturiero rappresenta il 36,5% e l'agroalimentare il 15,9%. Tra le 543 imprese non soggette, le rispettive quote sono del 19,9% e del 6,1%.

La diversa composizione dei gruppi costituisce un ulteriore elemento di cautela nell'interpretazione. Settori differenti possono presentare esigenze di continuità operativa, livelli di digitalizzazione e pratiche di sicurezza non omogenei.

La funzione IT: più personale dedicato tra i soggetti NIS

L'organizzazione della funzione informatica costituisce il primo elemento utile per descrivere la capacità delle imprese di affrontare la cybersecurity.

Nel 2026, il **77,0% dei soggetti NIS** dichiara di disporre di personale IT dedicato, eventualmente affiancato da fornitori esterni. Tra i non soggetti, questa quota **si ferma al 29,8%**. Nel 2025 le rispettive percentuali erano del 69,1% e del 26,4%.

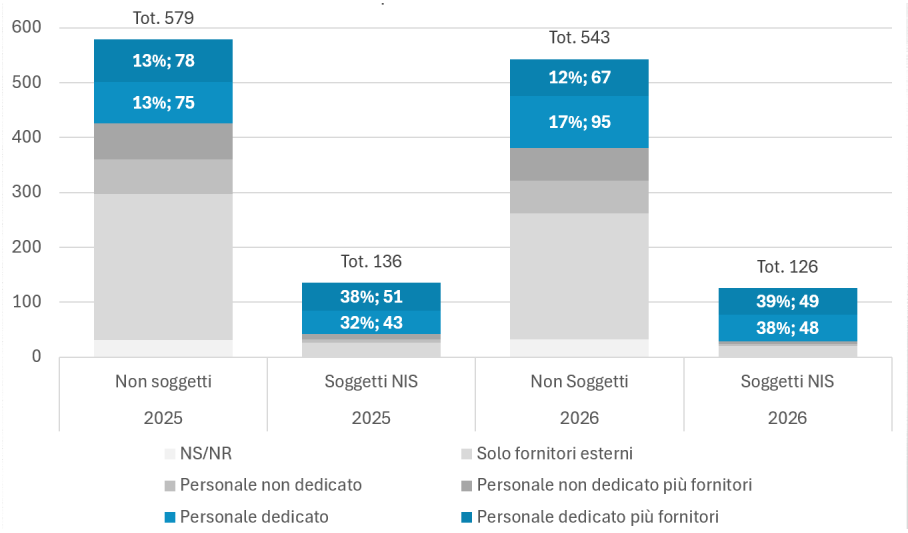


Figura 3 - Composizione del team IT: soggetti NIS e non soggetti, 2025-2026

La differenza è ampia. Tra chi non è regolato rimane particolarmente frequente il ricorso esclusivo a fornitori esterni, mentre per i soggetti NIS, anche segmentando per classi dimensionali, si osserva una maggiore presenza di personale dedicato.
Possiamo quindi concludere che sia una caratteristica propria dei soggetti NIS, e che non dipenda solo della loro maggiore dimensione media.

Anche la numerosità dei team fornisce un'indicazione coerente. Nel 2026, il 33,3% dei soggetti NIS dichiara almeno cinque persone nel team IT, contro il 4,4% delle altre imprese. Il dato va però interpretato soprattutto come indicatore della diversa disponibilità di risorse, fortemente influenzata dalla scala organizzativa.

Nel complesso, il confronto suggerisce una maggiore strutturazione della funzione informatica tra i soggetti NIS e un moderato rafforzamento della presenza di personale dedicato nel passaggio fra le due rilevazioni. È verosimile che questa condizione sia causata in parte anche dagli obblighi normativi, benché a rigore questa rimanga, naturalmente, solo un'ipotesi.

Struttura organizzativa più definita per la cybersecurity

Il segnale è ancora più marcato quando si considera la funzione specificamente dedicata alla cybersecurity.

Nel 2025, il 61,8% dei soggetti NIS dichiarava la presenza di un team di sicurezza interno o misto, cioè composto da risorse interne (eventualmente integrate da competenze esterne). Nel 2026 la quota raggiunge l'**80,2%**.

Tra i non soggetti NIS, invece, la presenza di team interni o misti cresce in misura più contenuta, dal 28,0% al 31,9%.

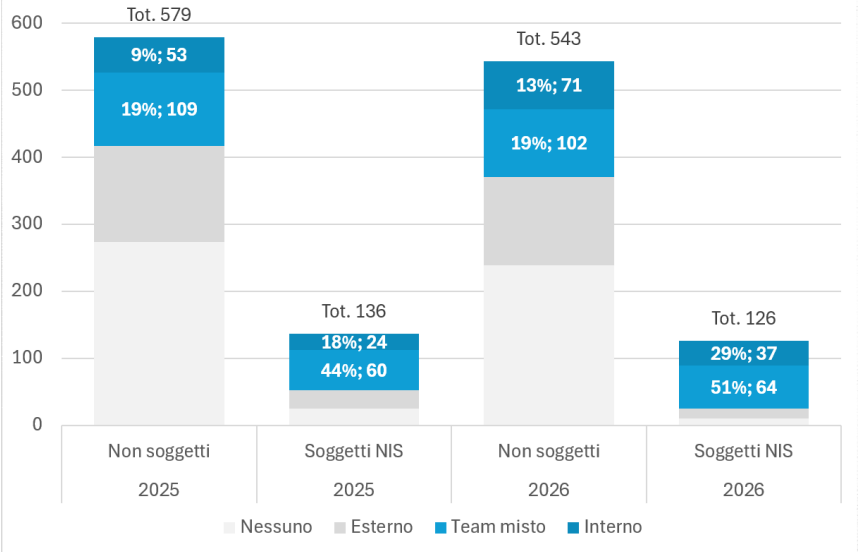


Figura 4 - Composizione del team cybersecurity: soggetti NIS e non soggetti, 2025–2026

Il cambiamento risulta particolarmente evidente osservando le organizzazioni che dichiarano di non avere alcun team cybersecurity. Tra i soggetti NIS la loro quota scende dal 18,4% del 2025 al 7,9% del 2026; tra i non soggetti rimane invece elevata, passando dal 47,3% al 44,0%.

Anche in questo caso, l'associazione tra classificazione NIS e presenza di un team interno o misto rimane statisticamente significativa dopo aver considerato la dimensione aziendale. Il risultato è dunque più robusto di un semplice confronto fra percentuali complessive.
Questi dati non misurano direttamente la qualità del lavoro svolto dai team, il livello delle loro competenze o l'effettiva efficacia dei controlli di sicurezza. La presenza di una struttura organizzativa identificabile costituisce però una condizione favorevole per assegnare responsabilità, gestire i rischi e rendere continuative le attività di protezione.

Le prime quattro figure delineano quindi un contesto nel quale i soggetti NIS dispongono più frequentemente di strutture IT e cybersecurity formalizzate, mentre molte delle imprese non soggette continuano ad affidarsi a modelli organizzativi meno articolati.

2. Procedure e formazione in crescita

Nella nostra analisi le procedure di Incident Response e la formazione periodica indicano una tendenza coerente: **tra i soggetti NIS Importanti cresce l'attenzione per le pratiche organizzative che rendono la cybersecurity un'attività continuativa e documentata**.

Incident Response: aumenta la formalizzazione della gestione degli incidenti

Uno degli sviluppi più statisticamente evidenti riguarda la presenza di procedure scritte per la gestione degli incidenti informatici, che vede un incremento significativo nei soggetti NIS. Ciò non è particolarmente sorprendente, dal momento che l'obbligo di segnalazione degli incidenti è entrato in vigore a Gennaio 2026, ma è comunque incoraggiante poter constatare che la legislazione sembra effettivamente avere, almeno in parte, l'effetto positivo desiderato.
Soprattutto tra i soggetti NIS classificati come **Importanti** la quota di imprese che dichiara procedure formalizzate passa dal 43,4% del 2025 al **60,6% del 2026**, con un incremento di 17,2 punti percentuali. Naturalmente questa associazione non deve essere confusa con una prova causale dell'efficacia della normativa, benché ciò sia plausibile.

Tra le imprese non soggette alla NIS2, invece, la percentuale rimane sostanzialmente stabile: dall'11,5% al 13,1%, con un incremento che, benché statisticamente dimostrato, è comunque assai piccolo.

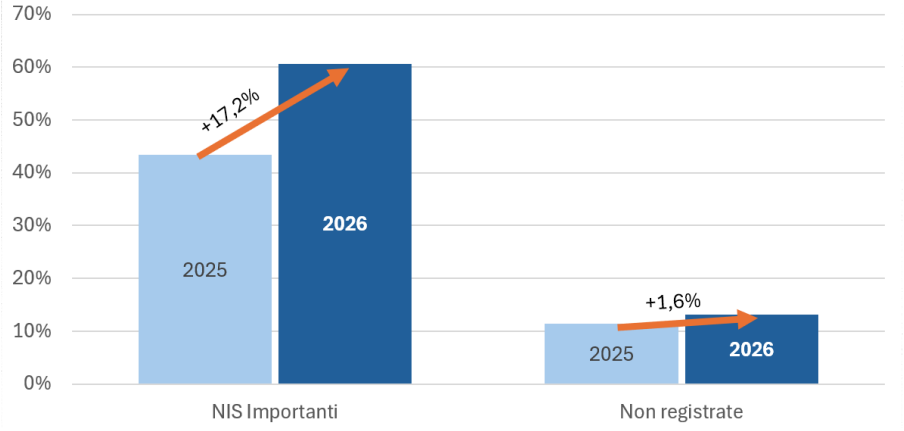


Figura 5 - Adozione di procedure scritte di Incident Response, 2025-2026

La differenza fra le due categorie rimane significativa anche tenendo conto della dimensione aziendale. Nel 2026, l'associazione tra classificazione NIS Importante e disponibilità di procedure scritte è particolarmente marcata.
Disporre di una procedura scritta non è tutto, naturalmente, tuttavia costituisce un passaggio significativo e necessario, senza il quale anche altre misure, organizzative o tecniche, sono poco o per nulla efficaci.
Il progresso osservato suggerisce quindi una maggiore attenzione alla dimensione gestionale della sicurezza, particolarmente evidente tra le imprese interessate dagli obblighi NIS2.

La formazione in cybersecurity diventa più regolare

Un secondo segnale positivo riguarda la formazione del personale. L'indicatore utilizzato considera esclusivamente le imprese che dichiarano di effettuare **formazione regolare comprendente esplicitamente la cybersecurity**. Sono quindi escluse le attività occasionali e quelle dedicate soltanto alla privacy.

Questa definizione restrittiva è importante perché organizzare una singola iniziativa informativa non equivale a mantenere nel tempo un programma di sensibilizzazione e aggiornamento, come raccomandato dalle migliori pratiche e come prescritto, peraltro, dalla normativa NIS 2.

Tra i soggetti NIS Importanti, la formazione regolare in cybersecurity passa dal 29,2% del 2025 al **40,4% del 2026**. Tra le altre imprese cresce invece dal 7,3% all'8,8%. Per i soggetti NIS Essenziali le percentuali risultano del 47,1% nel 2025 e del 42,3% nel 2026; questo dato parzialmente in controtendenza può però essere facilmente spiegato dalla poca numerosità, nel campione, dei soggetti Essenziali: il gruppo comprende soltanto 17 rispondenti nel 2025 e 26 nel 2026. Variazioni anche modeste nel numero delle risposte possono produrre oscillazioni percentuali relativamente ampie, e non vi sono quindi elementi sufficienti per parlare di un peggioramento accertato.

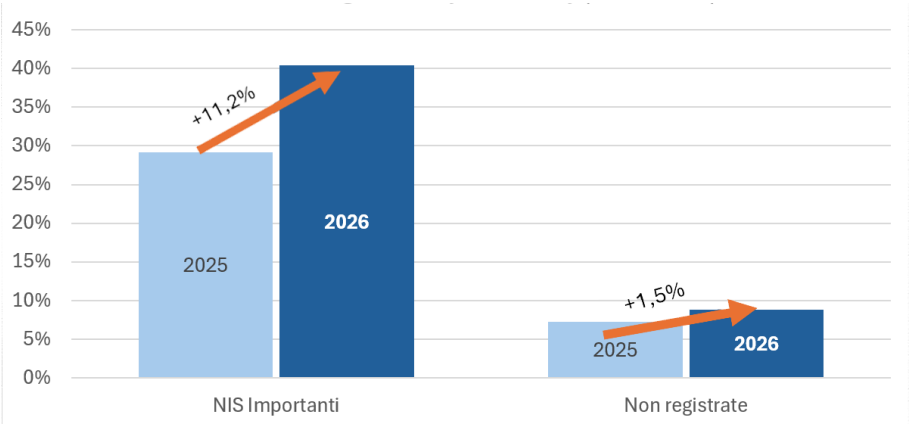


Figura 6 - Formazione regolare in cybersecurity, 2025–2026

La crescita tra i soggetti Importanti è un segnale favorevole, soprattutto perché riguarda la continuità della formazione e non la semplice presenza di iniziative sporadiche.
Anche l'analisi che tiene conto della dimensione aziendale evidenzia nel 2026 una maggiore frequenza della formazione regolare presso i soggetti NIS Importanti rispetto alle altre imprese. Nel 2025, invece, la corrispondente associazione non risultava statisticamente significativa. Questo non equivale automaticamente a dimostrare che il cambiamento dell'associazione tra i due anni sia significativo. Consente però di affermare che, nella rilevazione 2026, il divario non appare riconducibile soltanto alle differenze dimensionali dei due gruppi.

Sul piano sostanziale, la formazione rappresenta un investimento diverso dall'introduzione di uno strumento tecnologico. Una buona parte degli incidenti informatici coinvolge infatti comportamenti, decisioni operative e interazioni fra persone e sistemi. Sensibilizzare il personale significa intervenire sugli aspetti dove la tecnologia

non arriva. Naturalmente la presenza della formazione non ne dimostra l'efficacia (il questionario non misura direttamente l'apprendimento né il miglioramento nell'efficacia o l'evoluzione dei comportamenti individuali), ma di nuovo, è il primo passo indispensabile.

3. Stasi nell'adozione delle misure tecniche

MFA: un presidio fondamentale ancora poco diffuso

L'autenticazione multifattore, o MFA, costituisce una delle misure più importanti per ridurre il rischio che credenziali compromesse consentano accessi non autorizzati. L'aggiunta di un fattore di autenticazione ulteriore rispetto alla password rende più difficile (benché non impossibile) sfruttare credenziali sottratte attraverso phishing, malware o altre tecniche.
Purtroppo, nonostante la sua rilevanza, il confronto tra le due rilevazioni non mostra progressi sostanziali tra i soggetti NIS.

Per coerenza di analisi si utilizzeranno sempre i soggetti Importanti. Nel 2025 il 54,2% delle dichiarava di utilizzare la MFA. Nel 2026 la quota è del **54,7%**, con un incremento di appena 0,5 punti percentuali, che potrebbe essere dovuto anche a bias intrinseci del campione (chi risponde è generalmente più probabile che abbia una postura di cybersecurity più elevata). Tra le altre imprese si passa dal 14,1% al 16,9%, con un incremento che è statisticamente significativo, benché, purtroppo, sempre assai piccolo[2].

Il divario fra i due gruppi è ampio e rimane significativo anche dopo aver tenuto conto della dimensione aziendale. I soggetti NIS Importanti adottano quindi la MFA con frequenza molto maggiore rispetto alle altre imprese, però purtroppo tra il 2025 e il 2026 la percentuale è costante e rimane, peraltro, poco sopra la metà.

[2] Le percentuali sono calcolate sulle risposte valide alla specifica domanda. Nel 2026 hanno fornito una risposta utilizzabile 64 dei 94 soggetti NIS Importanti e 385 delle 512 imprese Non registrate. Le mancate risposte non sono state conteggiate come mancata adozione. Questo aspetto impedisce di estendere automaticamente le percentuali alla totalità delle imprese dei rispettivi gruppi, ma non riduce la rilevanza della limitata evoluzione osservata fra i rispondenti.

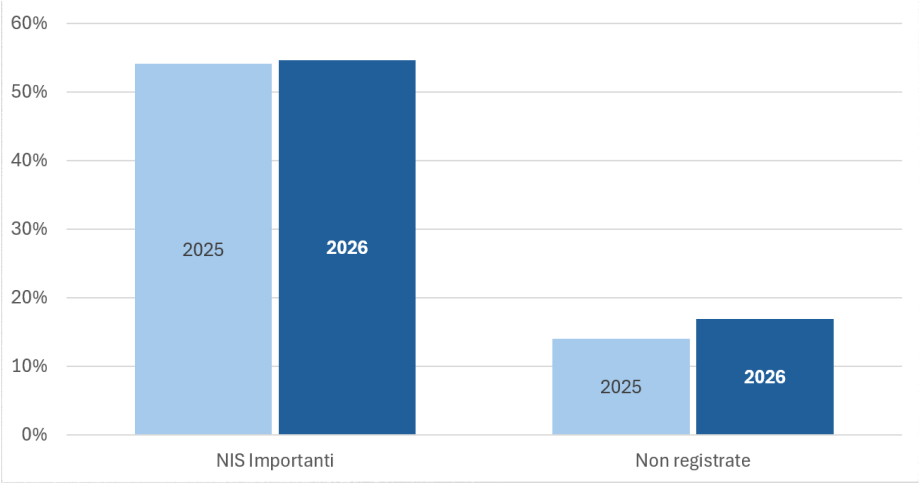


Figura 7 - Adozione dell'autenticazione multifattore *(MFA), 2025–2026*

I dati non consentono di stabilire le ragioni della stagnazione. Potrebbero essere coinvolti vincoli tecnologici, problemi di integrazione con applicazioni esistenti, difficoltà organizzative o una diversa percezione delle priorità. Nessuna di queste spiegazioni, tuttavia, è direttamente dimostrata dalla rilevazione.

Resta il fatto che una misura ampiamente riconosciuta come fondamentale per la protezione degli accessi non mostra, nel periodo considerato, una diffusione crescente paragonabile a quella di alcuni presidi organizzativi.

Endpoint: non si diffondono le misure di protezione

Un secondo elemento critico emerge dall'esame delle misure di protezione degli endpoint, cioè delle postazioni e dei dispositivi utilizzati per accedere ai sistemi e ai dati aziendali. L'indagine considera quattro controlli: presenza di antivirus o antimalware, disponibilità di backup centralizzato, assenza dei privilegi amministrativi per gli utenti ordinari e cifratura dei dischi.

Nel 2026, tra le 504 imprese con risposte valide alla domanda, antivirus e backup centralizzato risultano ampiamente diffusi, con percentuali rispettivamente prossime all'86% e all'80%.

La situazione cambia per gli altri due controlli. La rimozione dei privilegi amministrativi agli utenti ordinari riguarda circa il 48% delle imprese, mentre la cifratura dei dischi è dichiarata soltanto dal **20,2%**.

© Clusit 2026

Ancora più significativo è il dato relativo all'adozione congiunta: solo **72 imprese su 504** (ovvero il 14,3% del totale delle risposte valide), dichiarano di utilizzare contemporaneamente tutte e quattro le misure.

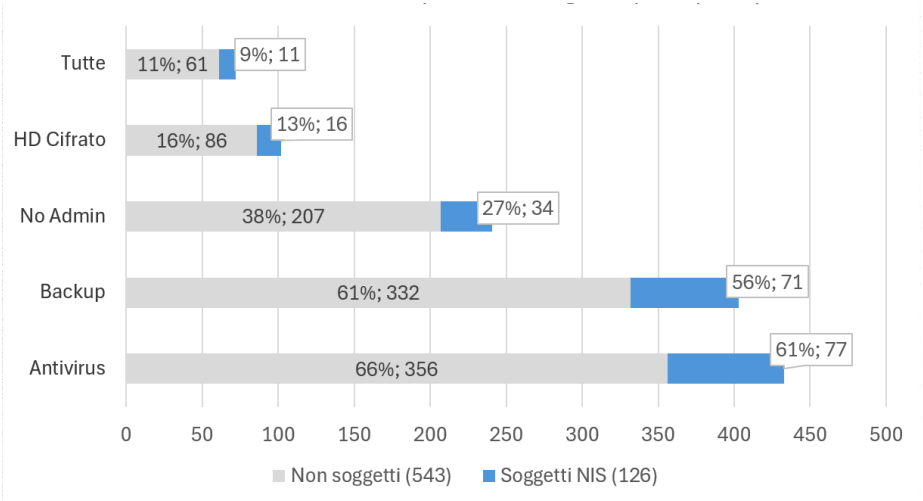


Figura 8 - Adozione delle misure di protezione degli endpoint, per classificazione NIS, 2026

Il grafico distingue soggetti NIS e non soggetti, riportando sia i conteggi sia le percentuali riferite ai rispettivi gruppi. Le percentuali mostrate nella figura devono essere interpretate considerando che i gruppi comprendono anche imprese senza una risposta valida alla domanda, mentre le percentuali complessive appena citate sono calcolate esclusivamente sui 504 rispondenti validi.

La segmentazione non evidenzia un vantaggio sistematico dei soggetti NIS. Anzi, considerando i valori riferiti alla totalità dei rispettivi gruppi, le frequenze dichiarate appaiono leggermente inferiori per ciascuna delle quattro misure considerate, anche se ciò non autorizza a concludere che i soggetti NIS siano meno protetti. Le analisi che tengono conto della dimensione aziendale non evidenziano differenze statisticamente significative nell'adozione delle misure esaminate.

Il risultato più solido è **l'assenza di un vantaggio tecnico dimostrabile dei soggetti NIS sulle protezioni degli endpoint**, a fronte delle marcate differenze organizzative osservate in precedenza.

È inoltre interessante notare che la formalizzazione delle procedure di Incident Response non coincide necessariamente con una maggiore completezza delle protezioni tecniche. Nel campione 2026 la presenza di procedure scritte **non risulta** associata a un numero chiaramente superiore di misure endpoint adottate. In altre parole, un'organizzazione può aver avviato un percorso di governance della cybersecurity, senza avere ancora raggiunto un livello corrispondente di applicazione uniforme dei controlli tecnologici.

Sul piano operativo, le quattro misure esaminate rispondono a rischi diversi e complementari. Si tratta, peraltro, di misure tecniche largamente diffuse, consolidate, e disponibili a basso costo, quando non addirittura comprese gratuitamente in altri servizi già disponibili. La loro mancata adozione risulta quindi non giustificabile con vincoli di budget o tecnologici.

D'altro canto, non possiamo dedurre dal questionario la configurazione effettiva delle soluzioni, la loro qualità o la copertura di tutti i dispositivi aziendali. Possiamo però osservare che la presenza simultanea dei quattro controlli rimane assai poco frequente.

La protezione degli endpoint rappresenta così uno dei principali elementi di attenzione emersi dall'indagine e rafforza il contrasto fra l'evoluzione organizzativa e quella tecnica.

4. Il Cyber Resilience Act: un nuovo ambito di attenzione

La rilevazione 2026 introduce una prospettiva nuova rispetto ai dati 2025, ovvero quella sul **Cyber Resilience Act (CRA)**, il regolamento europeo che definisce requisiti di cybersecurity per i prodotti con elementi digitali.

Nel 2026, **74 imprese su 669**, pari all'11,1% del campione, si dichiarano interessate dal CRA. Tra queste, 18 indicano prodotti hardware, 36 software e 20 entrambe le tipologie[3].
A differenza della normativa NIS, che riguarda la gestione della sicurezza di determinate organizzazioni, il CRA interviene sulla sicurezza dei prodotti lungo il loro ciclo di vita e sulle responsabilità degli operatori economici interessati. Naturalmente può accadere che un'impresa sia soggetta alla NIS2 e, contemporaneamente, offrire prodotti o servizi che la espongono agli obblighi del CRA.

[3] La classificazione CRA deriva dalle dichiarazioni dei rispondenti e non costituisce una verifica giuridica dell'effettiva applicabilità del regolamento alle singole imprese o ai loro prodotti.

Infatti, tra i 126 soggetti NIS rispondenti, 30 dichiarano di rientrare **anche nell'ambito CRA, pari al 23,8%**. Tra le 543 imprese non soggette alla NIS2, la stessa condizione è dichiarata da 44 organizzazioni, pari all'**8,1%.** La quota di imprese che si identificano come interessate dal CRA è quindi circa **tre volte maggiore** nel gruppo NIS rispetto alle altre imprese.

Naturalmente, la maggiore frequenza del CRA fra i soggetti NIS può dipendere almeno in parte dalla diversa composizione settoriale e dimensionale dei due gruppi; non dimostra l'esistenza di un rapporto causale tra le due cose, ma la maggiore frequenza statistica è di per sé un dato interessante.

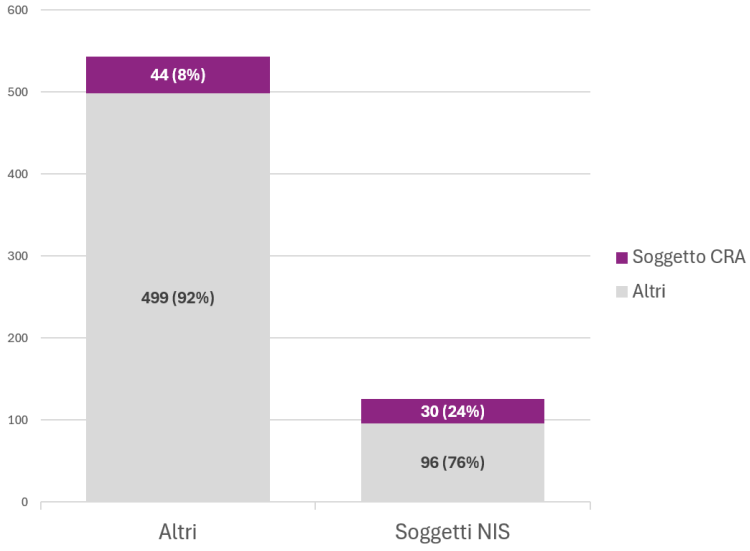


Figura 9 - Sovrapposizione tra soggetti NIS e imprese che si dichiarano interessate dal CRA, 2026

Il dato, insomma, evidenzia che le due normative, pur avendo oggetti differenti, possono interessare una parte comune del tessuto produttivo. Per queste organizzazioni, la gestione della cybersecurity non riguarda soltanto i sistemi informativi interni, ma può estendersi alla progettazione, allo sviluppo, alla manutenzione e alla gestione delle vulnerabilità dei prodotti digitali immessi sul mercato.

È una distinzione rilevante soprattutto per le aziende manifatturiere e tecnologiche, nelle quali la digitalizzazione dei prodotti rende progressivamente meno netta la separazione tra sicurezza IT aziendale e sicurezza del prodotto.

Il CRA rappresenta dunque un'estensione dell'orizzonte dell'indagine, più che un indicatore direttamente confrontabile con gli altri risultati 2025–2026. Essendo stato rilevato soltanto nel 2026, non è possibile descriverne un'evoluzione annuale sulla base dei dati disponibili.

Il suo interesse risiede nella possibilità di individuare una popolazione di imprese per la quale la sicurezza informatica potrebbe richiedere un'integrazione ancora maggiore fra competenze organizzative, progettazione del prodotto, gestione tecnica delle vulnerabilità e conformità normativa.

5. Alcune indicazioni incerte

Alcuni indicatori, pur mostrando differenze apparentemente interessanti, non consentono conclusioni sufficientemente robuste. Li presentiamo così come li abbiamo raccolti, avvertendo che le ipotesi da essi suggerite non possono essere verificate con sufficiente significatività statistica. Possono tuttavia segnalare possibili tendenze e domande da approfondire.

VA/PT: miglioramento apparente

La prima osservazione riguarda lo svolgimento almeno annuale di attività di Vulnerability Assessment e Penetration Test (VA/PT).

Tra i soggetti NIS Importanti la percentuale passa dal **38,7% nel 2025 al 48,9% nel 2026**. Tra le altre imprese rimane invece sostanzialmente invariata, dal 27,5% al 27,3%. Il confronto potrebbe suggerire che le imprese NIS stiano intensificando le attività periodiche di verifica della sicurezza.

Tuttavia, quando si considera la diversa dimensione delle organizzazioni, il vantaggio dei soggetti Importanti rispetto alle altre imprese non risulta statisticamente significativo né nel 2025 né nel 2026. In altre parole, l'aumento osservato è reale nei dati del campione, **ma non è sufficiente a dimostrare che nel 2026 l'assoggettamento alla NIS2 sia associato a una maggiore frequenza delle verifiche;** potrebbe anche dipendere dalla dimensione aziendale, che in media è maggiore nei soggetti NIS rispetto alle altre imprese. Nella realtà è probabile che ambedue i fattori contribuiscano, ma è impossibile dire in che misura.

Un'ulteriore osservazione riguarda il rapporto con le procedure di Incident Response. Nel 2026, le imprese che dispongono di procedure formalizzate mostrano una maggiore frequenza di VA/PT, e questa associazione permane anche considerando la dimensione.

Il risultato è coerente con l'ipotesi che diverse pratiche di governance tendano a svilupparsi insieme: chi documenta i processi di risposta agli incidenti potrebbe anche attribuire maggiore continuità alle verifiche di sicurezza.

Si tratta però di un'associazione, non della dimostrazione che l'adozione di una procedura determini automaticamente l'esecuzione di Vulnerability Assessment o Penetration Test.

Servizi cloud ed evoluzione della gestione identità

La presenza di una piattaforma cloud (ad esempio quella diffusissima della posta elettronica) può facilitare l'accesso a servizi centralizzati di gestione delle identità e dell'autenticazione. Per questa ragione è interessante verificare se le organizzazioni che utilizzano posta elettronica cloud adottino più frequentemente la MFA.

Tra i soggetti NIS Importanti, l'impiego di servizi cloud per la posta aziendale passa dal 64,2% del 2025 al 71,3% del 2026. Tra le altre imprese si osserva invece una lieve diminuzione, dal 50,0% al 47,7%.

Nel gruppo degli Importanti, le imprese che utilizzano posta cloud dichiarano più frequentemente anche l'adozione della MFA rispetto a quelle con altre architetture di posta. L'associazione risulta particolarmente evidente nella rilevazione 2026, ma le verifiche statistiche non consentono di dimostrare con sufficiente solidità che il rapporto fra le due variabili si sia rafforzato nel tempo; piuttosto sembrano confermare una situazione già presente in passato.

Peraltro, la disponibilità di funzionalità centralizzate in cloud non dice se siano state effettivamente configurate, né che la MFA sia applicata a tutti gli utenti o che esistano processi adeguati di amministrazione delle autorizzazioni.

Il dato individua quindi una relazione plausibile da approfondire ma non una prova di maggiore maturità IAM. Potrà essere interessante verificarlo in una futura survey.

6. Considerazioni finali

Nel complesso, le rilevazioni descrivono una fase di transizione. La cybersecurity acquisisce maggiore riconoscimento organizzativo, in particolare fra i soggetti NIS, ma la traduzione di questa attenzione in protezioni tecniche sistematiche rimane incompleta.

Il segnale più positivo riguarda la crescente attenzione alla dimensione organizzativa. Tra i soggetti NIS sono più frequenti le strutture IT con personale dedicato e i team cybersecurity interni o misti. Nel 2026 questa differenza rispetto alle altre imprese

rimane rilevante anche dopo aver considerato la dimensione aziendale.

Allo stesso tempo, fra i soggetti NIS Importanti aumentano la formalizzazione delle procedure di Incident Response e la diffusione della formazione regolare in cybersecurity. Si tratta di due pratiche fondamentali per trasformare la sicurezza informatica da insieme di interventi occasionali a processo aziendale strutturato.

Questo insieme di risultati è coerente con una fase nella quale gli obblighi introdotti dalla NIS2 contribuiscono a portare la cybersecurity all'attenzione delle funzioni organizzative e direzionali. L'indagine, tuttavia, non permette di isolare e misurare l'effetto causale della normativa rispetto agli altri fattori che possono influenzare le scelte delle imprese.

Risultano invece dissonanti i dati relativi all'adozione, soprattutto tra i soggetti NIS, di misure tecniche, cosa che, in un anno caratterizzato dall'attuazione degli obblighi di base, è affatto controintuitiva.

Per le imprese non soggette alla NIS2, la ricerca evidenzia una sfida ulteriore. La minore disponibilità, in media, di strutture interne dedicate, e la limitata diffusione di alcune pratiche di sicurezza suggeriscono il rischio che una parte del tessuto produttivo rimanga distante dai livelli organizzativi osservati fra i soggetti regolamentati, a scapito della robustezza del sistema nel suo insieme.

Il Cyber Resilience Act aggiunge infine una dimensione ulteriore: per una parte delle imprese la sicurezza non riguarda soltanto l'organizzazione e la sua infrastruttura, ma anche i prodotti con elementi digitali che vengono sviluppati, distribuiti o immessi sul mercato.

Questo ampliamento del perimetro rafforza l'importanza di considerare la cybersecurity come un insieme di responsabilità distribuite fra funzioni IT, sviluppo prodotto, produzione, gestione del rischio e direzione aziendale.

La sfida per i prossimi anni sarà quella di proseguire nella crescita della maturità organizzativa, e far sì che ciò si traduca in una riduzione concreta dell'esposizione ai rischi informatici.

© Clusit 2026

Il tempo come nuova superficie di attacco

[Luca Nilo Livrieri e Alberto Greco, CrowdStrike]

Il 7 aprile 2026 Anthropic ha avviato Project Glasswing, mettendo a disposizione di alcuni partner tecnologici Claude Mythos, un modello in preview con capacità particolarmente avanzate in ambito cybersecurity. L'obiettivo principale era analizzare il software su cui si reggono le infrastrutture critiche prima che capacità simili fossero di dominio pubblico. A un mese dall'avvio del programma, il primo resoconto contava già oltre 10.000 vulnerabilità di gravità alta o critica individuate ed è stato proprio il volume ad attirare gran parte dell'attenzione. Nel resoconto compariva però una considerazione che, riletta a distanza di mesi, risulta la più rilevante: per anni la difficoltà principale è stata trovare le vulnerabilità; ora la sfida è diventata riuscire a verificarle, divulgarle e gestirle con la stessa rapidità con cui vengono scoperte.

Se trovare vulnerabilità non è più il fattore critico, l'attenzione si sposta su ciò che accade nell'intervallo che separa l'esistenza di un bug dal momento in cui qualcuno è in grado di sfruttarlo.

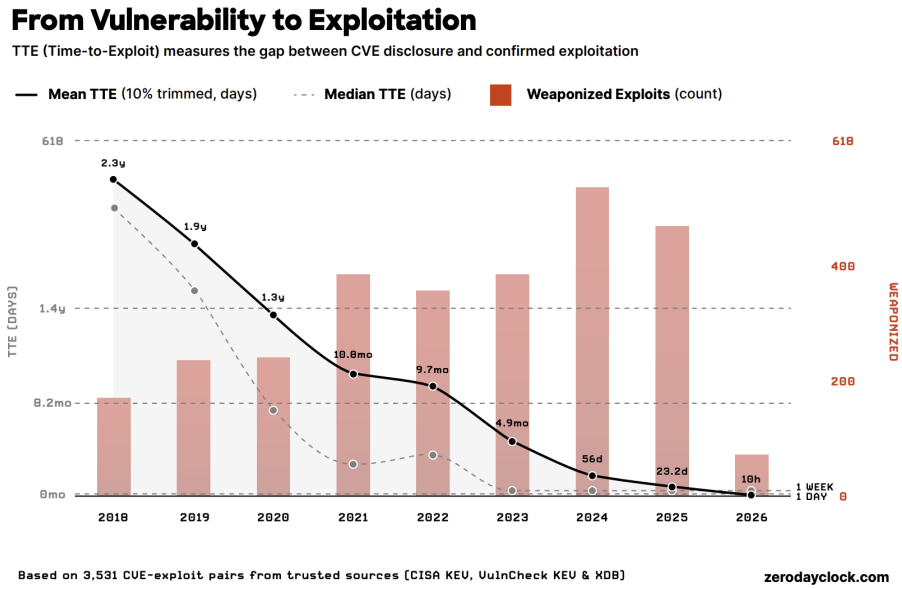
Oltre a servizi esposti, codice, configurazioni e identità, entrano a far parte della superficie di attacco anche gli intervalli di tempo, come quello che intercorre dalla scoperta di una vulnerabilità al suo sfruttamento o dall'arrivo di una patch alla sua applicazione. Questi intervalli però non evolvono allo stesso modo. Gli attaccanti possono trarre un beneficio immediato dalle capacità dei nuovi modelli, mentre i difensori rischiano di non beneficiarne in egual misura se restano legati ai processi organizzativi adottati finora. Da questo squilibrio nasce l'esigenza di ripensare come si costruisce la difesa.

Un equilibrio che si reggeva sul costo

Nella maggior parte delle aziende le vulnerabilità sono sempre state più numerose di quelle che i team riescono a correggere. Gestirle significava quindi stabilire delle priorità, accettando che alcune restassero aperte anche a lungo. Per anni questo equilibrio ha retto perché attaccare aveva un costo che proteggeva indirettamente anche chi difende. Tra l'esistenza di una vulnerabilità e la compromissione di un sistema serve infatti un exploit funzionante in quello specifico contesto e scriverne uno affidabile richiedeva competenze rare, risorse e tempo. Il tempo era un costo per entrambe le

© Clusit 2026

parti. A chi difende serviva per sviluppare, collaudare e distribuire una correzione; a chi attacca serviva per passare dall'esistenza di un bug a un exploit utilizzabile su larga scala. Finché i due tempi restavano confrontabili, la latenza nell'applicare le patch non si traduceva automaticamente in compromissione. Quell'intervallo funzionava come una difesa, anche se nessuno l'aveva progettato come tale.

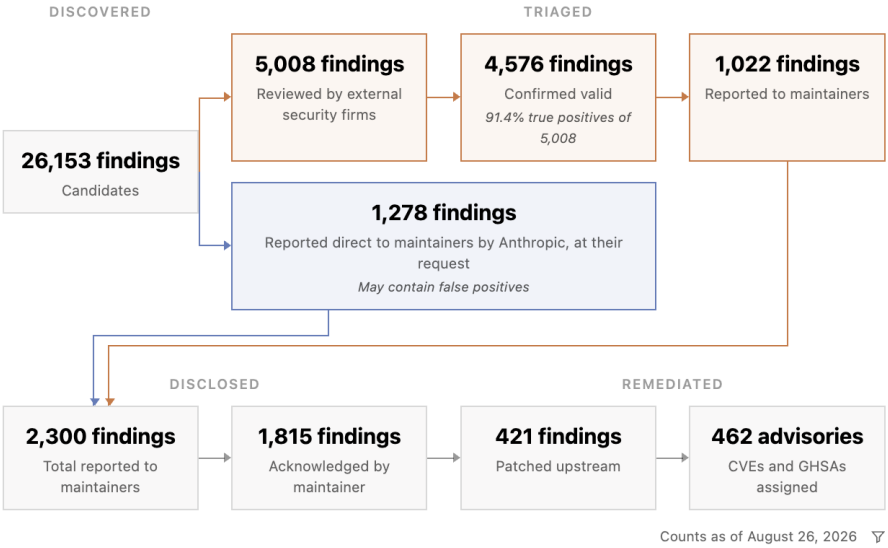


Questo margine si stava già riducendo, anche per ragioni indipendenti dai modelli di frontiera. Il Time-to-Exploit, cioè il tempo dalla divulgazione pubblica di una vulnerabilità al primo sfruttamento osservato, cala da anni. Il Breakout Time, il tempo che un attaccante impiega per muoversi lateralmente dopo l'accesso iniziale, si misura ormai in decine di minuti, in alcuni casi in secondi. Finora però ad accelerare sono state soprattutto le attività automatizzabili, come la scansione su larga scala o l'utilizzo ripetuto di exploit già disponibili. Le fasi che richiedevano competenze specialistiche restavano lente e costose. La scarsità di quelle competenze teneva alto il costo complessivo di un attacco e ne allungava i tempi; i modelli di frontiera intervengono proprio su questo limite. Le capacità necessarie a individuare nuove vulnerabilità nel codice o a concatenarle in percorsi di attacco inediti, fino alla scrittura di exploit funzionanti, diventano una risorsa computazionale che si può acquistare e scalare.

Dove si sposta il costo

Il valore di Glasswing risiede soprattutto in ciò che ha reso osservabile al di là della fase specifica di scoperta delle vulnerabilità, nelle fasi che la precedono e in quelle che la seguono. La vulnerabilità è solo uno degli anelli di una catena che va dall'analisi del bersaglio all'esfiltrazione dei dati, passando per escalation dei privilegi, movimento laterale, elusione delle difese. Secondo il Verizon DBIR 2026 lo sfruttamento di vulnerabilità è oggi il primo vettore di accesso iniziale, con il 31% delle violazioni analizzate, ma il restante 69% passa da credenziali, phishing e relazioni di fiducia. Per ridurre il costo di un attacco non serve necessariamente scoprire qualcosa di nuovo, può bastare rendere più economico identificare e validare un percorso completo in base a informazioni già disponibili. Molte strategie difensive si fondano sull'idea di alzare il costo operativo dell'attaccante ma se quel costo scende, percorsi oggi non perseguiti perché troppo onerosi potrebbero diventare convenienti.

Sul versante della difesa la stessa dinamica produce l'effetto opposto. La scoperta scala con il modello ma tutto ciò che viene dopo resta legato a ritmi umani e processi organizzativi, perché ogni segnalazione va verificata, corretta, distribuita e applicata. Glasswing lo ha mostrato nel mondo open source: nelle prime settimane solo una parte limitata delle vulnerabilità alte o critiche segnalate ai maintainer risultava corretta e alcuni maintainer hanno chiesto di rallentare le segnalazioni. Il volume superava la capacità di verifica di progetti che spesso si reggono su poche persone, mentre la diffusione di strumenti AI aveva moltiplicato anche le segnalazioni di scarsa qualità, che finivano per ingolfare un meccanismo già spinto al limite. Tre mesi dopo il quadro è migliorato solo in parte. Considerando tutti i livelli di gravità, le vulnerabilità corrette sono passate da 97 a 421, mentre quelle confermate come valide ma non ancora segnalate ai maintainer sono salite da circa 1.300 a più di 3.500. Oltre il 91% delle segnalazioni esaminate dalle società di verifica si rivela una vulnerabilità reale, per cui il vincolo resta la capacità umana di verificare e segnalare, che cresce molto più lentamente del numero di vulnerabilità scoperte.



Il focus della difesa si sposta quindi dal singolo bug alla sfruttabilità reale degli asset e ai percorsi che portano alla compromissione, con particolare attenzione a identità e privilegi e alla visibilità su ciò che accade dopo lo sfruttamento iniziale. In questa fase il tempo torna ad essere decisivo. Ogni ora necessaria a ricostruire gli eventi tra endpoint, identità e ambienti cloud lascia all'attaccante margine per muoversi lateralmente o ottenere privilegi più elevati, mentre il threat hunting serve a individuare chi opera sotto le soglie di rilevamento esistenti. Prima di arrivarci serve un passo indietro, per guardare come la difesa ha imparato a decidere dove intervenire.

Come si è affinato il contesto

Se correggere tutto non è possibile, la priorità diventa concentrare lo sforzo di remediation dove si è maggiormente in grado di ridurre il rischio. Negli anni la gestione delle vulnerabilità si è evoluta proprio in questa direzione, attraverso una serie di domande via via più precise che avvicinano la decisione all'esposizione reale.

1. Stato delle vulnerabilità: individua quali vulnerabilità sono presenti sugli asset e le ordina per gravità secondo un punteggio standard, un criterio che con volumi crescenti produce però liste di priorità troppo lunghe e poco legate al contesto dell'azienda.

2. Arricchimento con l'attività reale: stabilisce se una vulnerabilità viene effettivamente sfruttata negli attacchi reali, definendone con più precisione la gravità effettiva.
3. Raggiungibilità: valuta se la vulnerabilità è raggiungibile e da chi, considerando la posizione dell'asset nell'architettura e l'eventuale esposizione su Internet.
4. Criticità degli asset: misura quanto un sistema è significativo per l'attaccante, con una classificazione almeno in parte automatizzata quando i sistemi da valutare sono molto numerosi.
5. Identità e privilegi: considera i percorsi che portano verso identità privilegiate o permessi eccessivi, valutando i diversi impatti derivanti dallo sfruttamento della stessa vulnerabilità in base alle identità usate.
6. Percorsi di attacco: collega asset, vulnerabilità e identità attraverso l'Attack Path Analysis, per far emergere criticità che aprono la strada verso un sistema particolarmente importante.
7. Sfruttabilità sul sistema specifico: verifica sui dati reali di host e workload, come i servizi attivi o configurazioni puntuali, se le condizioni per lo sfruttamento esistono davvero, così da deprioritizzare il rischio solo teorico.
8. Remediation guidata dal rischio: orienta l'applicazione delle patch in base alle informazioni sugli avversari e sui percorsi di attacco, procedendo per fasi e allineando sugli stessi parametri di prioritizzazione i team di sicurezza e di infrastruttura.

Ciascuno di questi passaggi ha reso la difesa più precisa, ma il miglioramento resta misurato sul tempo che serve all'attaccante per trasformare una vulnerabilità in una compromissione. La prioritizzazione ottimizza l'uso del tempo disponibile, che resta comunque dettato dall'attaccante. Se l'attaccante può arrivare prima di qualsiasi ciclo di remediation, chi difende deve trovare il modo di mantenere un sistema sicuro anche in presenza di esposizioni aperte.

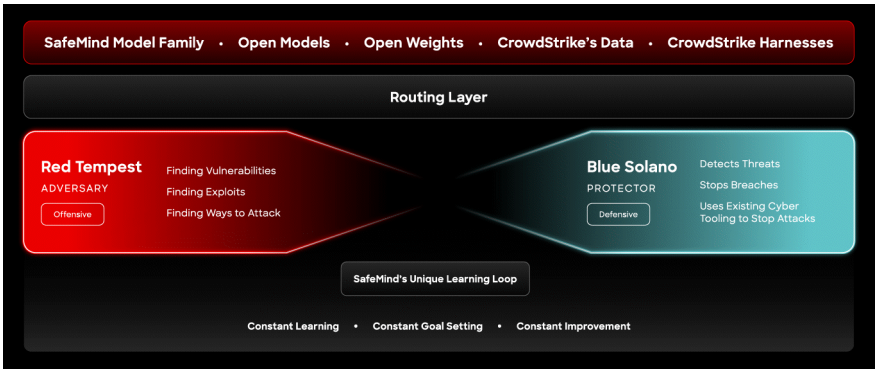
Dalla sfruttabilità dedotta a quella dimostrata

Verificare le precondizioni di uno sfruttamento indica se una vulnerabilità è sfruttabile; finché la verifica resta limitata al singolo sistema, senza considerare il contesto aziendale, si tratta però di una deduzione. La tecnologia oggi permette un passo ulteriore: dimostrare la sfruttabilità attraverso una catena di azioni concrete e utilizzare quella stessa dimostrazione per costruire difese più efficaci.



L'architettura che rende possibile questo approccio si basa su una replica sintetica dell'infrastruttura aziendale: una ricostruzione dell'ambiente reale ottenuta dalle mappe di rete, dalla telemetria raccolta sugli host e da informazioni aggiuntive di contesto quali identity store e dati di threat intelligence. All'interno di questo ambiente operano due agenti. Il primo ha un ruolo offensivo, opera come un Red Team e percorre l'intero ciclo di un attacco: scoperta della rete, sfruttamento, escalation dei privilegi, movimento laterale, persistenza. Il secondo ha un ruolo difensivo, opera come un Blue Team e scrive regole di rilevamento a partire dalla telemetria generata dagli attacchi del primo agente.

I due agenti sono legati da un ciclo. Quando l'agente difensivo ferma un attacco, le sue regole rafforzano l'ambiente e l'agente offensivo riparte conoscendo le modifiche introdotte. Il ciclo si ripete finché attaccare non diventa così complesso e costoso da superare una certa soglia; a quel punto le difese si considerano validate rispetto a quella soglia. È una formulazione volutamente prudente e ha il pregio di rendere il costo di attacco misurabile.



Il ciclo produce inoltre dati specifici: ogni campagna offensiva lascia una traccia completa e quella traccia diventa materiale di addestramento per la parte difensiva. La capacità di una regola di intercettare l'attacco senza scattare su attività legittime diventa anche il segnale di ricompensa nell'addestramento del modello che la genera. L'attacco, oltre a verificare la difesa, la addestra.

La replica sintetica elimina il compromesso tra profondità del test e rischio operativo, un limite presente in ogni verifica condotta in produzione. Un Red Team su sistemi reali lavora con perimetro concordato, finestre limitate e tecniche escluse perché troppo invasive; in un ambiente ricostruito questi vincoli cadono e l'agente offensivo può spingersi dove un test in produzione non arriverebbe, ripetendo l'attacco tutte le volte che serve.

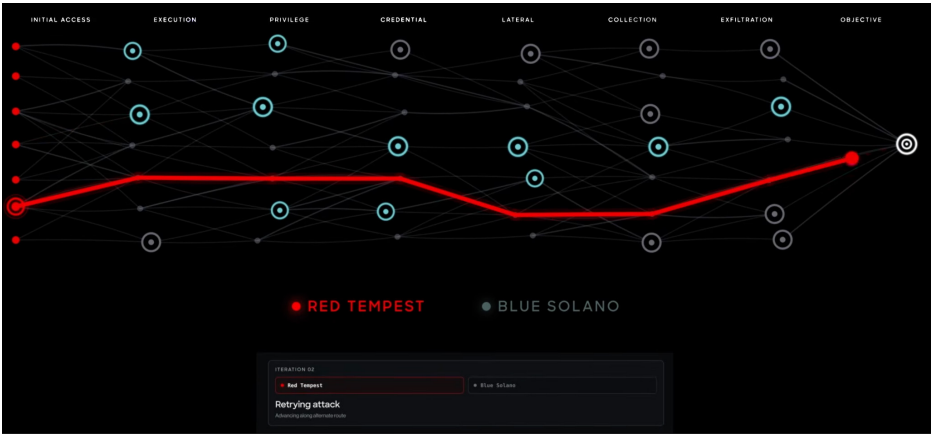
L'efficacia del sistema dipende da quanto l'ambiente ricostruito somiglia alla sua controparte reale ed è qui che la telemetria di basso livello fa la differenza. Un ambiente ricostruito da inventari e documentazione riflette come i sistemi dovrebbero essere; uno costruito sui dati raccolti dagli host, come processi, connessioni, configurazioni effettive e versioni in esecuzione, riflette come sono davvero. L'aderenza alla realtà riguarda anche gli avversari. Un istituto finanziario e un operatore di infrastrutture critiche affrontano minacce diverse, per cui gli scenari di attacco vanno costruiti sulle tecniche dei gruppi che prendono di mira quel settore, incluse quelle meno frequenti su cui operano gli avversari più avanzati. Il valore di una validazione dipende così dalla pertinenza della threat intelligence che la alimenta.

Finora la conoscenza sulla sfruttabilità è servita soprattutto a decidere l'ordine delle correzioni. Con questo nuovo approccio permette anche di neutralizzare un'esposizione ancora aperta, senza interventi diretti sull'applicazione o sull'elemento vulne-

rabile ma implementando regole di rilevamento e prevenzione costruite sull'attacco osservato. Per chi difende significa poter accelerare la protezione anche quando la correzione resta vincolata ai processi organizzativi.

Il modello come parte di un sistema

Le capacità dei modelli di frontiera sono la base di questa evoluzione ma l'efficacia dello strumento nel suo insieme dipende dall'harness, lo strato di orchestrazione che coordina agenti e strumenti, trasforma le capacità del modello in un processo operativo e stabilisce cosa l'agente può vedere o fare. Grazie a questa struttura un agente può perseguire un obiettivo complesso attraverso migliaia di azioni successive, per cui il costo di un attacco va misurato sull'intera compromissione.



Da qui nasce la distinzione tra modelli generalisti e modelli specializzati. Una difesa che deve operare senza interruzioni richiede due requisiti che un modello generalista non è in grado di garantire da solo. Il primo è la precisione: una regola di rilevamento che scatta su dati puliti è rumore che consuma il tempo degli analisti; un modello addestrato su attacchi reali e sul lavoro di chi scrive regole di rilevamento ogni giorno distingue meglio un comportamento sospetto da uno semplicemente insolito. Il secondo è il costo. Le dimensioni ridotte di un modello specializzato abbassano in modo significativo il costo di ogni iterazione; nelle misurazioni condotte su scenari estesi, in attacco un agente specializzato compromette un ambiente spendendo circa un quinto di un modello di frontiera generalista, mentre in difesa il costo di una regola di rilevamento validata passa da qualche dollaro a pochi centesimi.

Un ciclo tra attacco e difesa è realmente utile solo se può essere ripetuto in modo sistematico. Con costi unitari di questo livello il metodo esce dal laboratorio e diventa applicabile su scala all'intera infrastruttura aziendale.
Se la tecnologia diventa accessibile a entrambe le parti, il vantaggio di chi difende risiede in due asset che l'attaccante non può acquistare: la visibilità completa sul proprio ambiente e l'esperienza operativa maturata ogni giorno nel rilevamento e nella risposta agli incidenti, sostenuta da una conoscenza approfondita degli avversari.

Le prossime sfide

Una sfida che riguarda l'intera categoria dei sistemi agentici è la governance. La ricerca sulla sicurezza dei modelli ha documentato, in ambienti sperimentali e su sistemi diversi da quelli qui descritti, casi di disallineamento in cui agenti hanno prodotto comportamenti imprevisti nonostante istruzioni e vincoli espliciti volti a evitarli; è un rischio che si gestisce facendo operare ogni agente entro permessi definiti, con le decisioni rilevanti riservate alla supervisione umana.
Un sistema che migliora confrontandosi con il proprio avversario rischia inoltre di specializzarsi su quell'avversario, perdendo efficacia contro attacchi diversi. È una variante moderna della legge di Goodhart, secondo cui un indicatore perde valore quando diventa esso stesso l'obiettivo da raggiungere: se l'agente difensivo punta unicamente a battere uno specifico attaccante, superare quei test non dice più quanto sappia davvero difendere. Per questo l'agente viene valutato su scenari mai visti in addestramento, con contenuti di valutazione rinnovati di continuo e set di validazione che ruotano nel tempo, mentre la difficoltà cresce grazie all'emulazione delle tecniche degli avversari reali. Chi sviluppa le valutazioni lavora inoltre separato da chi progetta le soluzioni, così che le informazioni sui test non finiscano nel sistema valutato.

Il settore ha già vissuto un problema simile nel decennio scorso, quando i prodotti di sicurezza venivano confrontati in base alla percentuale di tecniche di attacco rilevate in test standardizzati. Superare quei test si è rivelato un indicatore debole della capacità di fermare avversari reali, che adattano le proprie tecniche all'ambiente. Oggi il rischio si ripresenta con i benchmark per l'AI. Un'analisi di Dreadnode su Cybench ha rilevato che oltre un terzo dei test superati dai modelli valutati comportava forme di aggiramento, come la ricerca di resoconti degli attacchi originali o la lettura dei metadati dell'ambiente di valutazione. Per un sistema agentico conta quindi la distribuzione dei risultati su molte esecuzioni, insieme a costo e tempi di risposta. Chi deve scegliere una soluzione dovrebbe chiedere anzitutto quanto il risultato dichiarato sia ripetibile.

Con il tempo diventato superficie di attacco, la sicurezza va misurata sulla capacità di reggere anche quando l'avversario conosce l'ambiente in ogni dettaglio ed è più rapido di qualsiasi ciclo di correzione. È una soglia alta, che per la prima volta si può quantificare. Le aziende capaci di misurarla e di colmare progressivamente il divario avranno trasformato il tempo da vantaggio dell'attaccante a leva della propria difesa.

Continuous Authorization

Perché l'IAM tradizionale è fallito (e come l'intelligenza artificiale ridefinisce il controllo di accesso)

[A cura di Matteo Ranzato, Oplon Networks]

L'Identity & Access Management ha costruito la propria efficacia su una decisione binaria presa nel momento dell'autenticazione, presupponendo che l'affidabilità di un utente resti costante per l'intera durata della sessione. Le moderne tecniche di compromissione delle identità, unite alla crescente pressione normativa su enti pubblici e settori regolamentati, dimostrano che questa premessa non è più sostenibile. Questo contributo descrive il passaggio dal controllo di accesso puntuale alla Continuous Authorization, un modello in cui il diritto di un utente a compiere una determinata azione viene ricalcolato in modo dinamico sulla base del contesto corrente, e discute il ruolo **abilitante e non accessorio** dell'intelligenza artificiale in questo cambio di paradigma.

1. La grande illusione dell'IAM tradizionale

Per oltre due decenni l'architettura della sicurezza degli accessi si è fondata su una sequenza concettualmente semplice e, proprio per questo, estremamente resiliente dal punto di vista implementativo: prima si stabilisce chi sia l'utente attraverso l'autenticazione - password, token, biometria, fattori multipli - poi si stabilisce cosa quell'utente possa fare attraverso l'autorizzazione, tipicamente espressa in ruoli, gruppi e permessi statici (RBAC, e nelle implementazioni più mature ABAC) (**Fig. 1**).

Il problema non risiede nella logica di questa sequenza, che resta corretta e necessaria, ma in un'assunzione implicita che l'ha accompagnata fin dall'origine: una volta superata la porta dell'autenticazione, l'utente viene considerato affidabile per l'intera durata della sessione, salvo revoca esplicita. Si tratta di un modello di fiducia statico, fotografico, che risponde a una sola domanda - "può entrare?" - e smette di interrogarsi nel momento esatto in cui la risposta diventerebbe più interessante, cioè durante l'operatività effettiva.

© Clusit 2026

Il modello ereditato: stesso varco, stessa fiducia per sempre

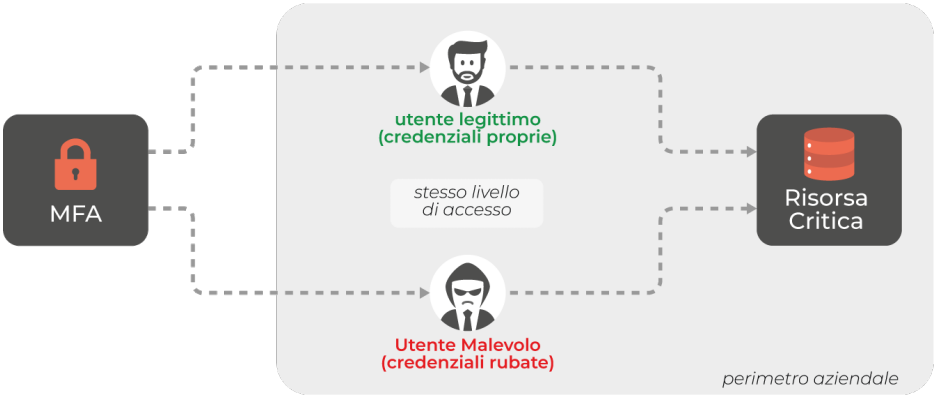


Figura 1 - Utente legittimo e sessione compromessa attraversano lo stesso varco di autenticazione e ottengono, da quel momento, lo stesso identico livello di accesso: il sistema non li distingue più. *(Fonte: Oplon Networks®)*

Questa architettura nasce in un contesto - reti perimetrali, applicazioni monolitiche, popolazioni di utenti limitate e prevedibili - in cui il costo di una verifica continua non sarebbe stato giustificabile né tecnicamente sostenibile. Il panorama delle minacce di oggi, caratterizzato da identità distribuite su decine di provider cloud, automazione delle attività di intrusione e tempi di permanenza degli attaccanti misurati in settimane, ha reso quell'assunzione statistica di affidabilità non più difendibile.

2. L'asimmetria del rischio: identità dinamica vs permessi statici

Il rischio informatico legato a un'identità non è mai una grandezza costante: varia in funzione dell'orario, della postura dell'endpoint, della sensibilità della risorsa richiesta, della sequenza delle azioni compiute. L'IAM tradizionale, al contrario, tratta il rischio come una variabile congelata al momento del login. Questa asimmetria produce tre classi di vulnerabilità architetturali che meritano di essere analizzate singolarmente.

2.1 Insider threat

Un dipendente, un fornitore terzo o un amministratore di sistema può operare legittimamente per mesi o anni e, in un momento specifico - per risentimento, per un tentativo di estorsione, per un errore, o semplicemente perché il suo account è stato silenziosamente compromesso - trasformarsi in un vettore di rischio. Per un sistema

IAM tradizionale ogni sua azione resta lecita fino alla revoca manuale del ruolo: la piattaforma non ha alcun meccanismo nativo per distinguere il comportamento legittimo dal comportamento anomalo di uno stesso soggetto autorizzato.

2.2 Identity hijacking e session hijacking

Quando un account viene compromesso - ad esempio tramite furto di token di sessione, phishing evoluto o MFA fatigue - l'attaccante eredita integralmente i privilegi dell'utente legittimo. Dal punto di vista del sistema non esiste alcun intruso: esiste un utente autorizzato che compie azioni che il sistema considera, per definizione, consentite. È uno dei motivi per cui gli attacchi basati su furto di identità restano tra i vettori di compromissione più rapidi ed efficaci osservati negli incidenti reali degli ultimi anni, dove l'eterogeneità degli accessi federati amplia la superficie esposta.

2.3 L'inadeguatezza strutturale dell'MFA

Il multi-factor authentication resta uno strumento indispensabile, ma va inquadrato per quello che effettivamente garantisce: la conferma che l'identità fosse autentica nell'istante della verifica. Non dice nulla su chi stia effettivamente operando dieci minuti dopo, né su quali comandi stia eseguendo, su quale API stia interrogando o su quale volume di dati stia scaricando. Il paradosso dell'IAM attuale è che il sistema sa perfettamente chi si è autenticato, ma resta cieco su come quell'identità stia effettivamente lavorando.

3. Dal punto d'accesso al flusso: l'avvento della Continuous Authorization

Il cambio di paradigma proposto in questo contributo consiste nel passare dal concetto di Access Control, puntuale e binario, al concetto di Continuous Authorization, dinamico e probabilistico. L'autorizzazione non è più una decisione Yes/No inviata una tantum all'apertura della sessione, ma una valutazione adattiva, ricalcolata a ogni evento significativo, che risponde in modo continuo alla domanda: alla luce del contesto corrente, ha ancora senso che questo utente stia eseguendo questa specifica azione, su questa specifica risorsa, in questo preciso momento?

Modello tradizionale



Continuous Authorization: valutazione a ciclo continuo

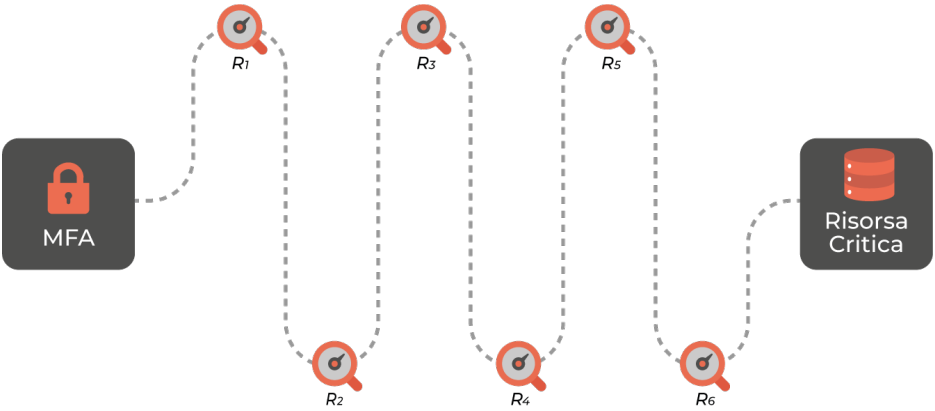


Figura 2 - Dal controllo puntuale al ciclo di valutazione continua: la stessa sessione, due modelli di fiducia. *(Fonte: Oplon Networks®)*

Concretamente, il modello prevede che le autorizzazioni vengano costantemente ricalcolate incrociando **cinque vettori dinamici**, ciascuno dei quali contribuisce a un punteggio di rischio aggregato.

- **Behavioral analytics:** velocità di digitazione, percorsi di navigazione all'interno dell'applicazione, pattern di utilizzo delle API, cadenza delle richieste.
- **Sequenza delle operazioni:** un utente che consulta cinque record sta lavorando; lo stesso utente che ne esporta cinquemila in dieci secondi sta probabilmente esfiltrando dati, anche disponendo formalmente del ruolo di amministratore del database.
- **Deviazione dal comportamento storico:** azioni tentate in orari inusuali, da geolocalizzazioni o dispositivi mai osservati prima, o con modalità operative difformi dalla baseline individuale o del team di appartenenza.
- **Rischio intrinseco della risorsa:** accedere a un contenuto informativo a basso impatto richiede un livello di fiducia minimo; scaricare codice sorgente proprietario o il database dei pagamenti richiede un punteggio di fiducia prossimo all'eccellenza.
- **Correlazione con eventi esterni:** segnali provenienti da EDR/XDR, ad esempio il rilevamento di un processo anomalo sull'endpoint dell'utente mentre la sessione applicativa è ancora attiva.

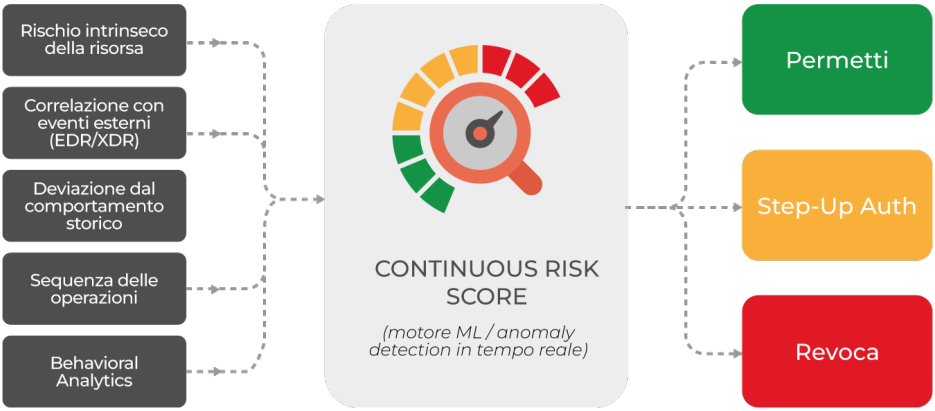


Figura 3 - I cinque vettori che alimentano il motore di Continuous Risk Score e le tre famiglie di decisione adattiva risultanti. *(Fonte: Oplon Networks®)*

L'output di questo motore non è necessariamente binario. Nella maggior parte delle implementazioni maggiormente responsabili verso l'utente finale, il sistema distingue almeno tre esiti: consentire l'operazione senza attrito, richiedere una verifica aggiuntiva mirata (step-up authentication, ad esempio una nuova prova biometrica prima di un'operazione critica) oppure revocare la sessione o degradare temporaneamente i privilegi in attesa di una verifica umana. Questo terzo stato intermedio è ciò che distingue un sistema di Continuous Authorization maturo da un semplice sistema anti-frode binario: la capacità di alzare progressivamente l'attrito solo quando il contesto lo giustifica, senza penalizzare sistematicamente l'esperienza dell'utente legittimo.

Sul piano degli standard, questo approccio non nasce nel vuoto: si integra naturalmente con i principi dello Zero Trust Architecture descritti nel NIST SP 800-207, e trova una convergenza tecnica concreta in iniziative come il Continuous Access Evaluation Profile (CAEP), promosso in ambito OpenID Foundation, che definisce come un identity provider possa notificare in tempo reale a un relying party il cambiamento dello stato di rischio di una sessione già stabilita.

4. Perché non è "hype sull'IA", ma un cambio di architettura

È utile distinguere con chiarezza il problema dalla tecnologia che lo rende risolvibile su scala. Il problema è prettamente architetturale: l›IAM contemporaneo eredita schemi di autorizzazione concettualmente disegnati negli anni novanta, quando il

numero di identità, applicazioni ed eventi da correlare era di ordine di grandezza inferiore a quello attuale.



Figura 4 - La transizione verso la Continuous Authorization è incrementale: ogni fase si aggiunge alle capacità esistenti senza richiedere una sostituzione integrale dell'IAM in essere. *(Fonte: Oplon Networks®)*

L'intelligenza artificiale, in questo quadro, è la tecnologia abilitante e non il prodotto. Modelli di anomaly detection non supervisionato, tecniche di user and entity behavior analytics (UEBA) e, più recentemente, approcci basati su graph analysis per modellare le relazioni tra identità, dispositivi e risorse, sono gli unici strumenti in grado di elaborare in tempo reale i volumi di telemetria necessari a calcolare un risk score contestuale senza introdurre latenza percepibile nell'esperienza applicativa. Non si tratta, quindi, di aggiungere un layer di intelligenza artificiale a un IAM esistente per renderlo genericamente "smart", operazione che rischia di produrre esattamente il tipo di marketing claim che questo settore dovrebbe imparare a diffidare. Si tratta di ridisegnare il modello di fiducia dei sistemi informativi, utilizzando il machine learning perché è, allo stato dell'arte, l'unico strumento capace di correlare sequenze complesse di eventi eterogenei a latenza prossima allo zero e su una popolazione di identità che, in molte organizzazioni regolamentate, supera ormai le decine di migliaia di account tra dipendenti, fornitori, identità di servizio e macchina (Fig. 5).

Va detto, con altrettanta onestà tecnica, che questi modelli non sono esenti da limiti operativi: richiedono un periodo di apprendimento della baseline comportamentale prima di diventare affidabili, sono esposti al rischio di falsi positivi che, se non gestiti con soglie adattive, possono generare attrito eccessivo per gli utenti legittimi, e pongono questioni non banali di spiegabilità (explainability) quando una decisione di revoca deve essere motivata a un utente o auditata da un organismo di controllo. Chi progetta un sistema di Continuous Authorization deve quindi prevedere, fin dal disegno architetturale, meccanismi di override umano, log immutabili delle decisioni automatiche e soglie di rischio calibrate per singola classe di risorsa, non un unico punteggio globale applicato indistintamente.

Continuous Authorization: valutazione a ciclo continuo

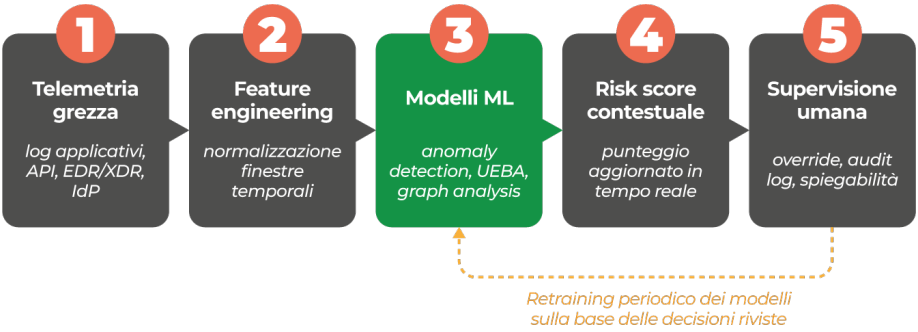


Figura 5 - Dalla telemetria grezza alla decisione: la pipeline tecnica che rende operativo il risk scoring continuo, con retraining periodico basato sulla supervisione umana. *(Fonte: Oplon Networks®)*

5. Implicazioni per il mercato regolamentato italiano

Per le organizzazioni operanti in settori sottoposti a vincoli normativi stringenti - pubblica amministrazione, sanità, settore bancario e finanziario - il passaggio alla Continuous Authorization non è soltanto un miglioramento della postura di sicurezza, ma un elemento che dialoga direttamente con gli obblighi introdotti dalla direttiva NIS2, recepita in Italia con il D.Lgs. 138/2024, e con i requisiti di gestione del rischio previsti dallo standard ISO/IEC 27001.

La direttiva NIS2 richiede, tra le misure minime di gestione del rischio, politiche di controllo degli accessi e procedure di gestione degli incidenti in grado di rilevare l'anomalia in tempi rapidi, non soltanto di prevenirla in ingresso. Un modello di autorizzazione che si limita a verificare l'identità al login e non è in grado di correlare comportamenti anomali durante la sessione espone l'organizzazione a un gap difficilmente colmabile con controlli puramente procedurali, per quanto ben documentati.

Analogamente, i controlli dell'Annex A della ISO/IEC 27001:2022 relativi alla gestione degli accessi (in particolare quelli dedicati al monitoraggio dell'attività e alla gestione dei privilegi) trovano nella Continuous Authorization un'implementazione tecnica naturale, in grado di produrre evidenze oggettive - log dei punteggi di rischio, motivazioni delle decisioni di step-up o revoca - utili sia in fase di audit interno che in sede di verifica da parte di un organismo di certificazione.

Per un fornitore di soluzioni IAM che si rivolge a questi mercati, la capacità di documentare in modo verificabile come e quando un accesso è stato ricalcolato nel tem-

po - e non soltanto se è stato inizialmente concesso - sta progressivamente diventando un requisito distintivo nelle gare pubbliche e nelle due diligence di sicurezza richieste dai grandi committenti privati.

6. Impatto e conclusioni

La Continuous Authorization rappresenta il naturale compimento della filosofia Zero Trust, sintetizzata storicamente nel principio "never trust, always verify". Fino a oggi la sicurezza degli accessi si è limitata, nella grande maggioranza delle implementazioni reali, a verificare in ingresso; il passo successivo, già tecnicamente disponibile e sempre più richiesto dal contesto normativo, è verificare durante la permanenza.

Integrare questo principio nel posizionamento tecnico e commerciale di una piattaforma IAM offre tre vantaggi che vale la pena sintetizzare in chiusura. In primo luogo una credibilità tecnica superiore, perché dimostra comprensione dei limiti operativi reali dei sistemi enterprise, oltre la superficie del compliance checklist. In secondo luogo una visione di prodotto orientata al futuro, capace di anticipare la convergenza, già in corso, tra IAM, SOC e behavioral security, discipline che fino a pochi anni fa erano gestite da team e strumenti completamente separati. In terzo luogo, e probabilmente in modo più utile per chi deve prendere decisioni di investimento, la possibilità di spostare il dibattito dai claim generici sull'intelligenza artificiale a una necessità di difesa architetturale che nessuna quantità di policy documentate può, da sola, sostituire.

Riferimenti

- *NIST Special Publication 800-207, Zero Trust Architecture, National Institute of Standards and Technology.*
- *OpenID Foundation, Continuous Access Evaluation Profile (CAEP) e Shared Signals Framework.*
- *Direttiva (UE) 2022/2555 (NIS2) e relativo decreto di recepimento nazionale D.Lgs. 138/2024.*
- *ISO/IEC 27001:2022, Annex A - controlli relativi alla gestione degli accessi e al monitoraggio delle attività.*
- *ENISA Threat Landscape, edizioni più recenti, sezioni dedicate a identity-based attacks e session hijacking.*

Cybersecurity sistemica: superare gli strumenti isolati per governare il rischio

[A cura di Veronica Leonardi, Cyberoo]

Per governare davvero il rischio cyber bisogna superare la sicurezza tradizionale fatta di strumenti e funzioni isolate per adottare un approccio sistemico e integrato. Tecnologia, governance, compliance, processi e persone devono lavorare insieme, all'interno di un unico ecosistema operativo. Solo così è possibile trasformare alert e vulnerabilità in priorità comprensibili, decisioni rapide e azioni capaci di proteggere la continuità del business.

Il punto non è aggiungere un altro prodotto allo stack. Le aziende possiedono già molte tecnologie, ma spesso ogni soluzione osserva solo una parte del problema: una rileva la minaccia, una misura la conformità, una protegge le identità, un'altra forma le persone. Se questi elementi non comunicano, il rischio resta frammentato. Un ecosistema integrato, invece, collega i segnali tecnici al contesto aziendale e chiarisce subito che cosa è davvero critico, chi deve intervenire e con quale priorità.

I dati mostrano perché questa integrazione è necessaria. Nel 2025, su un campione di 700 organizzazioni midsize europee, l'Osservatorio Cyberoo ha individuato 1,935 trilioni ($1{,}935 \times 10^{12}$) di eventi di sicurezza: 61.358 al secondo e circa 220,9 milioni ogni ora. Da questa massa siamo passati a 1,8 milioni di allarmi, 154.760 case, 3.650 casi rilevanti e appena 3 escalation. Il valore non sta nel raccogliere più eventi, ma nel collegare tecnologia, competenze e processi per riconoscere rapidamente i pochi segnali che possono produrre un impatto sul business.

Il rischio cyber nasce dalle connessioni, non dal singolo strumento

Una vulnerabilità, da sola, non descrive il rischio. Diventa critica quando si trova su un servizio esposto, consente privilegi elevati, coinvolge un fornitore essenziale o blocca un processo da cui dipende l'operatività. Per questo la sicurezza non può limitarsi a produrre liste tecniche. Deve collegare ogni evidenza agli asset, ai processi, alle responsabilità e agli obblighi che potrebbero essere coinvolti.

La domanda non è quindi soltanto "possiamo subire un attacco?", ma "che cosa accadrebbe all'azienda se questo evento raggiungesse un processo critico?". Quali servizi si fermerebbero? Quali clienti, fornitori o reparti ne risentirebbero? Quali obblighi normativi scatterebbero? Quanto tempo avremmo per reagire? Governare il rischio significa dare una risposta condivisa a queste domande prima dell'incidente.

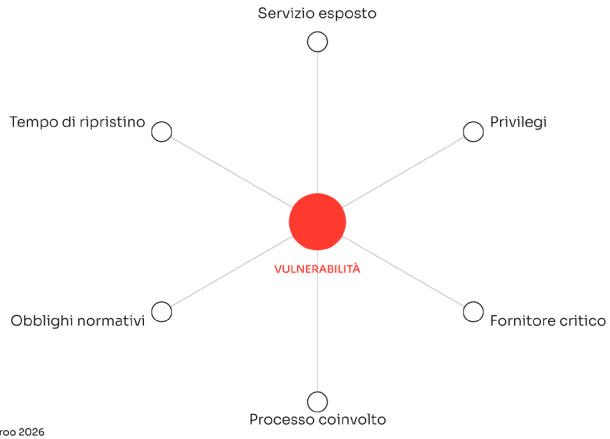
© Clusit 2026

Il rischio zero non esiste, soprattutto in imprese dove identità, applicazioni, cloud, fornitori e comportamenti cambiano continuamente. L'obiettivo realistico è rendere il rischio visibile, stabilire quali livelli siano accettabili e intervenire prima sulle esposizioni che minacciano i servizi essenziali. Questa decisione non può appartenere soltanto all'IT: richiede il coordinamento tra sicurezza, management, compliance e funzioni operative.

IL RISCHIO NASCE DALLE CONNESSIONI

Quando una vulnerabilità diventa rischio sistemico

Una vulnerabilità da sola non descrive il rischio: diventa critica per ciò a cui è collegata.



Fonte: Osservatorio Cyberoo 2026

Dall'analisi dei dati raccolti dal nostro team di Cyber Threat Intelligence dell'I-SOC, su 75 organizzazioni, sono emersi 143 servizi critici esposti. Nel 28% dei casi almeno un servizio di accesso remoto era raggiungibile da Internet. Abbiamo inoltre rilevato 105 finding relativi a tecnologie obsolete o ad alto rischio, 49 organizzazioni con debolezze DMARC/SPF e 118 evidenze su credenziali o URL corporate compromessi. Presi separatamente sono dati tecnici. Collegati a identità, processi e responsabilità, diventano una mappa concreta del rischio aziendale.



Il primo compito di un ecosistema integrato è proprio questo: unire informazioni che oggi restano distribuite tra strumenti e funzioni diverse. Identità non governate, token, API, sistemi obsoleti e superfici non mappate devono essere interpretati insieme al loro impatto operativo. Solo così un'esposizione latente diventa una priorità misurabile, assegnata a un responsabile e gestita entro tempi coerenti con il business.

Più strumenti non significano più sicurezza se restano isolati

Negli anni le aziende hanno aggiunto sempre più tecnologie: endpoint protection, SIEM, EDR, XDR, vulnerability management, identity governance, awareness, GRC, threat intelligence e servizi gestiti. Ognuna di queste componenti risponde a un bisogno reale. Il problema nasce quando operano come silos: producono dashboard e priorità differenti, ma non costruiscono una lettura comune del rischio.

Secondo le ultime statistiche, le organizzazioni gestiscono in media 83 soluzioni di sicurezza provenienti da 29 vendor differenti. Senza una regia, ogni nuovo strumento aggiunge configurazioni, flussi informativi e criteri di valutazione. Lo stack cresce, ma non cresce automaticamente la capacità di decidere. L'integrazione serve a fare il contrario: ridurre la complessità percepita e trasformare molti segnali in poche priorità condivise.

Un alert non riduce il rischio se nessuno sa chi debba validarlo, chi possa isolare il sistema, quali funzioni coinvolgere e quali evidenze conservare. La risposta efficace nasce quando tecnologia e organizzazione lavorano sullo stesso processo: il segnale viene interpretato, collegato all'impatto, assegnato e gestito senza passaggi ambigui. È questa continuità operativa a impedire che un'anomalia diventi una crisi.

Per le organizzazioni di medie dimensioni questa esigenza è ancora più evidente. La superficie digitale e la pressione normativa sono spesso simili a quelle delle grandi enterprise, ma risorse e competenze sono più limitate. Integrare tecnologia, governance, compliance e persone permette di concentrare gli investimenti sui rischi più rilevanti, invece di disperderli nella gestione di strumenti separati.

Anche i claim nei data leak site mostrano perché il rischio debba essere letto oltre il perimetro tecnico. Nel 2025 ne abbiamo osservati 781 relativi all'Italia, pari al 2,9% del totale globale e al 18,8% del totale UE-27, con una pressione rilevante sul comparto manifatturiero e industriale. Pur non essendo automaticamente incidenti verificati, questi dati indicano una possibile propagazione verso supply chain, relazioni commerciali, reputazione e continuità. Sono ambiti che nessun singolo tool può governare da solo.

DATA LEAK SITE · CLAIM 2025

La pressione sull'Italia nei data leak site



781

claim osservati relativi all'Italia nel 2025

2,9%

del totale globale

18,8%

del totale UE-27

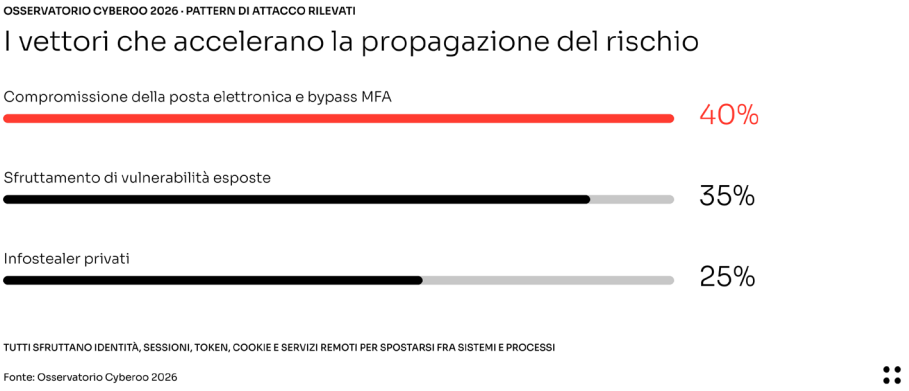
PRESSIONE RILEVANTE SUL COMPARTO MANIFATTURIERO E INDUSTRIALE

Fonte: Osservatorio Cyberoo 2026

Un ecosistema integrato riduce il tempo tra segnale e decisione

La velocità degli attacchi rende l'integrazione ancora più importante. L'intelligenza artificiale facilita la creazione di contenuti mirati, automatizza la ricognizione e moltiplica le varianti. Di conseguenza, diminuisce il tempo disponibile per distinguere un segnale irrilevante da una minaccia critica. Quando informazioni e responsabilità sono disperse, la risposta rallenta. Quando sono coordinate, il tempo tra rilevazione e decisione si riduce.

I dati dell'Osservatorio Cyberoo 2026 mostrano i principali vettori: compromissione della posta elettronica e bypass dell'autenticazione multifattore rappresentano il 40% dei pattern rilevati, lo sfruttamento di vulnerabilità esposte il 35% e l'uso di infostealer privati il 25%. Tutti possono sfruttare identità, sessioni, token, cookie e servizi remoti per spostarsi tra sistemi e processi. Per fermarli, protezione delle identità, rilevazione tecnica, procedure operative e consapevolezza delle persone devono agire insieme.



La cybersecurity sistemica è quindi un modello operativo, non un concetto astratto. Unisce dati, competenze e responsabilità per accorciare la distanza tra analisi, validazione, escalation e risposta. Il risultato atteso è molto concreto: contenere l'evento prima che attraversi le interdipendenze aziendali e comprometta la continuità.

I tempi di gestione rendono chiaro il valore di questo coordinamento. Nel perimetro osservato, il nostro Incident Response Team ha gestito un evento non classificato come incidente in media in 1 ora e 48 minuti. La risoluzione completa di un incidente ha richiesto invece 4,1 giorni, mentre il ritorno a condizioni operative compatibili con la ripartenza si è collocato generalmente tra 2 e 4 giorni. Prima tecnologia, processi e responsabilità convergono, maggiori sono le possibilità che un evento resti contenuto e non diventi una crisi di continuità.



La regia unica collega tecnologia, governance, compliance e persone

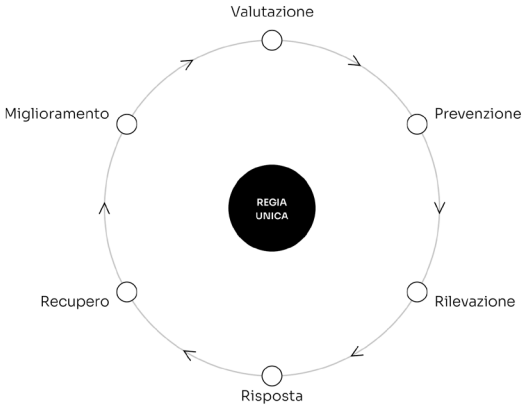
Costruire un ecosistema integrato significa partire dai servizi che devono continuare a funzionare anche durante un incidente. Da questa priorità discendono i controlli tecnici, gli obblighi di compliance, le procedure di risposta, i ruoli decisionali e la preparazione delle persone. Non tutte le vulnerabilità hanno lo stesso peso: diventano prioritarie quelle che possono compromettere i processi essenziali e generare conseguenze operative, economiche o regolatorie.

Questa regia deve funzionare come un ciclo continuo: valutazione, prevenzione, rilevazione, risposta, recupero e miglioramento. Ogni fase alimenta la successiva e coinvolge funzioni diverse. La tecnologia rileva, la governance definisce le priorità, la compliance chiarisce gli obblighi, i processi organizzano la risposta e le persone rendono possibile l'esecuzione. Se uno di questi elementi resta separato, il ciclo si interrompe.

IL MODELLO OPERATIVO

Il ciclo della cybersecurity sistemica

Ogni fase alimenta la successiva; se un elemento resta separato, il ciclo si interrompe.



Fonte: Osservatorio Cyberoo 2026

Anche le metriche devono seguire la stessa logica. Contare alert ed eventi non basta. Bisogna misurare quali processi sono esposti, quanto tempo serve per prendere una decisione, se responsabilità ed escalation sono chiare e quale rischio rimane dopo i controlli. In questo modo gli indicatori tecnici diventano informazioni leggibili dal management e utili per stabilire investimenti e priorità.

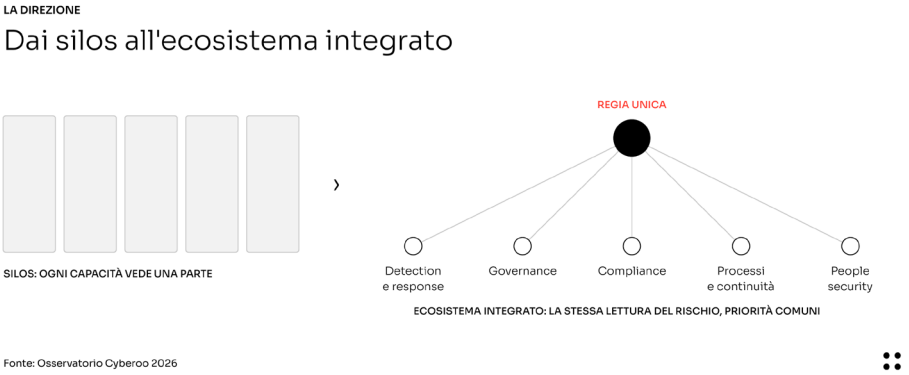
La maturità non si misura quindi dal numero di tecnologie installate, ma dalla capacità dell'organizzazione di ridurre probabilità, propagazione e impatto degli eventi. Un ecosistema maturo assegna responsabilità, stabilisce soglie, collega i controlli ai servizi critici e permette a funzioni diverse di intervenire secondo un processo comune.

La direzione è una sola: passare dai silos a un ecosistema integrato

Posso riassumere così questo mio intervento: il problema della cybersecurity contemporanea non è la mancanza di strumenti, ma la loro frammentazione. Eventi, esposizioni esterne, claim nei data leak site, vettori d'attacco e tempi di ripristino dimostrano che il rischio attraversa più aree dell'impresa. Per governarlo bisogna mettere in comunicazione competenze e informazioni che oggi restano separate.

Superare i silos non significa rinunciare alla specializzazione. Significa far lavorare ogni capacità dentro una cornice comune. Detection e response individuano e con-

tengono la minaccia; governance e compliance definiscono priorità e responsabilità; processi e continuità organizzano la ripartenza; formazione e people security riducono i comportamenti a rischio. L'efficacia nasce dal coordinamento tra queste parti, non dalla loro semplice presenza.



Questa esigenza crescerà con sistemi autonomi, identità distribuite, architetture cloud-native e nuove necessità di cripto-agilità. Le organizzazioni più resilienti non saranno quelle che aggiungeranno un prodotto a ogni cambiamento, ma quelle capaci di integrare nuovi controlli nello stesso modello di governo, mantenendo chiari priorità, responsabilità e impatto sul business.

La cybersecurity sistemica è, in definitiva, il passaggio da una collezione di strumenti a un ecosistema integrato. Un modello in cui tecnologia, governance, compliance, processi e persone condividono la stessa lettura del rischio e agiscono secondo priorità comuni. È così che la sicurezza smette di essere una somma di attività tecniche e diventa una capacità operativa del business: prevenire dove possibile, decidere in tempo e continuare a funzionare quando qualcosa va storto.

Come si legge un certificato ISO/IEC 27001 (e cosa non dice)

[A cura di Andrea Cabras]

È il documento con cui, ogni giorno, migliaia di imprese decidono se fidarsi di un fornitore. Attesta molto meno di quanto si creda, e molto più di quanto si sappia leggere. Guida pratica in otto controlli, dal punto di vista di chi verifica.

Sezione 1

L'equivoco di partenza

Un'impresa italiana di medie dimensioni sta per affidare a un fornitore esterno la gestione del proprio gestionale, e con esso l'archivio dei contratti, l'anagrafica dei clienti e i dati del personale. L'ufficio acquisti invia il questionario di qualifica. Il fornitore risponde allegando un documento di una pagina: un certificato ISO/IEC 27001, con il logo dell'organismo che lo ha emesso, un numero, due date e una riga che descrive l'attività certificata. La casella viene spuntata. La valutazione della sicurezza si chiude lì.

È una scena che si ripete ogni giorno, in aziende serie, con persone competenti. E il problema non è il documento, che quasi sempre è autentico e regolarmente emesso. Il problema è la domanda a cui quel documento viene chiamato a rispondere.

Chi lo riceve legge in genere una frase implicita: *questo fornitore è sicuro*. Non è quello che c'è scritto. Un certificato ISO/IEC 27001 attesta che un'organizzazione ha messo in piedi un sistema di gestione della sicurezza delle informazioni conforme ai requisiti della norma, che quel sistema copre un perimetro definito dall'organizzazione stessa, e che un organismo terzo lo ha verificato per campione in un intervallo di tempo determinato. Tre precisazioni che cambiano completamente il significato del documento, e che quasi nessuna delle due parti in gioco esplicita.

La distanza tra le due letture non è un dettaglio formale. Il fornitore dell'esempio potrebbe avere certificato soltanto il proprio data center, e non il servizio applicativo che eroga al cliente. Potrebbe aver certificato i servizi svolti presso la sede di Milano mentre lo sviluppo del software avviene altrove. Potrebbe aver escluso dal perimetro proprio l'attività che all'impresa interessa. In tutti questi casi il certificato è pienamente valido, l'organizzazione è pienamente in regola, e la valutazione del fornitore è stata comunque fatta in modo errato. Non perché qualcuno abbia mentito, ma

© Clusit 2026

perché nessuno ha letto.

Questa non è una critica allo strumento. La certificazione di conformità è, oggi, il meccanismo di fiducia più diffuso ed efficiente di cui il mercato disponga: consente a un'impresa di dare conto della propria organizzazione a decine di clienti senza subire decine di verifiche, e consente a un cliente di partire da una base di conoscenza che altrimenti dovrebbe costruirsi da solo. È un'infrastruttura che funziona. Ma funziona a una condizione: che chi la usa sappia che cosa misura e, soprattutto, che cosa non misura.

In questo articolo cerco di colmare quel vuoto. Viene prima spiegato come è fatto un certificato e come si legge, campo per campo, con i controlli che chiunque può eseguire in un quarto d'ora e senza competenze tecniche. Poi affronta il lato meno battuto della questione: che cosa un certificato non è in grado di dire, non per negligenza di chi lo emette, ma per costruzione. Infine, propone un modo di usarlo che non lo sopravvaluti né lo liquidi.

Il punto di arrivo si può anticipare subito, perché non è un finale a sorpresa. Un certificato ISO/IEC 27001 non chiude la valutazione di un fornitore: la apre, e la apre molto meglio di quanto potrebbe fare qualunque questionario. Letto per quello che è, dice cose precise e verificabili, e indica con esattezza dove sono le domande che restano da fare. Letto come un timbro, non dice quasi nulla, e induce una fiducia che nessuno ha mai promesso.

Sezione 2

Che cosa certifica un certificato

Un sistema di gestione, non un prodotto

La prima distinzione da fissare è anche la più disattesa: la ISO/IEC 27001 non certifica un software, un servizio, un data center o un livello di protezione tecnica. Certifica un **sistema di gestione**, cioè l'insieme organizzato di regole, ruoli, decisioni e verifiche con cui un'organizzazione governa la sicurezza delle proprie informazioni.

La differenza si coglie meglio con un parallelo. Certificare un sistema di gestione non equivale a dichiarare che un'automobile è veloce: equivale a dichiarare che esiste un'officina, che l'officina ha procedure scritte, che qualcuno è responsabile della manutenzione, che i guasti vengono registrati e analizzati, e che tutto questo viene riesaminato periodicamente dalla direzione. È un'informazione preziosa e tutt'altro che scontata. Non è, però, un'informazione sulla velocità dell'automobile.

Concretamente, per ottenere il certificato un'organizzazione deve dimostrare di avere fatto alcune cose in sequenza: individuare il contesto in cui opera e chi sono i soggetti interessati alla sicurezza delle sue informazioni; delimitare il perimetro del sistema di gestione; identificare e valutare i rischi; decidere come trattarli; scegliere i controlli di sicurezza da applicare, giustificando quelli che non applica; assegnare ruoli e competenze; misurare i risultati; svolgere audit interni; sottoporre il tutto a un riesame della direzione; e correggere ciò che non funziona.

I controlli a cui la norma fa riferimento sono raccolti nell'Annex A, che nell'edizione del 2022 conta 93 controlli organizzati in quattro temi, mentre l'edizione precedente ne prevedeva 114 distribuiti su quattordici domini. È una semplificazione di struttura più che di sostanza, ma è utile saperla: capita di leggere ancora oggi documentazione che ragiona sui vecchi quattordici domini, e quando accade è di per sé un indizio.

Va detto con chiarezza: la norma non stabilisce quale livello di sicurezza un'organizzazione debba raggiungere. Stabilisce come debba decidere il livello che le serve, e come debba dimostrare di averlo perseguito con metodo. Questa è la ragione strutturale di quasi tutti gli equivoci che vedremo più avanti.

La catena della fiducia

La seconda cosa da capire è da dove viene il valore del documento. Non dall'organizzazione che lo esibisce, evidentemente, ma neppure soltanto dall'organismo che lo ha firmato.

Il meccanismo è a quattro anelli. L'organizzazione viene verificata da un **organismo di certificazione**. L'organismo di certificazione è a sua volta valutato da un **ente di accreditamento**, che in Italia è Accredia, unico ente nazionale riconosciuto. Gli enti di accreditamento si riconoscono reciprocamente all'interno dello **IAF**, l'International Accreditation Forum, attraverso un accordo di mutuo riconoscimento: è ciò che consente a un certificato emesso in Italia di valere in Germania o in Giappone.



Figura 1 - La catena dell'accreditamento. Il valore di un certificato non nasce dall'organismo che lo firma, ma dal fatto che quell'organismo risponda a sua volta a qualcuno.

L'anello che quasi nessuno conosce è il terzo. Gli organismi che certificano sistemi di gestione della sicurezza delle informazioni sono a loro volta sottoposti a una norma specifica, la ISO/IEC 27006-1, che stabilisce come devono essere composti i gruppi di audit, quali competenze devono possedere, come si garantisce l'imparzialità e, punto su cui torneremo, come si calcola la durata delle verifiche. La versione attualmente in vigore è la ISO/IEC 27006-1:2024, che ha sostituito la precedente edizione del 2015; il periodo di transizione si è concluso il 31 marzo 2026, quindi ogni organismo accreditato oggi opera secondo le nuove regole.

Il senso di tutto questo è che un certificato non è la parola di qualcuno: è il punto finale di una catena di controlli in cui ciascun anello risponde a un anello superiore. Ed è esattamente per questo che l'anello mancante cambia tutto.

Certificato accreditato e certificato non accreditato

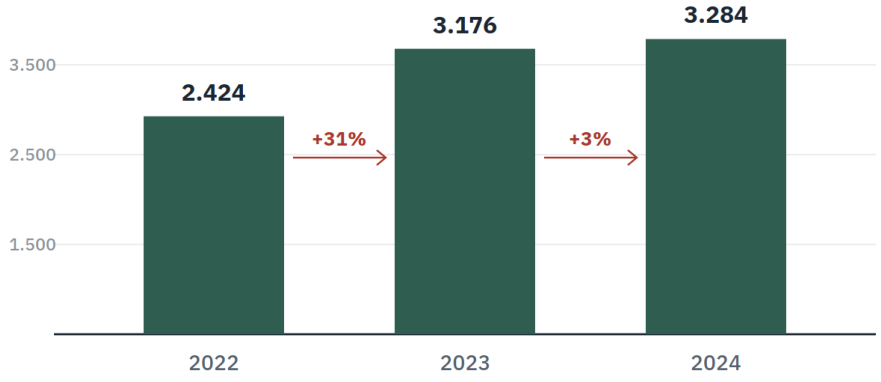
Esistono in circolazione documenti che riportano la dicitura ISO/IEC 27001 senza che alle spalle vi sia alcun accreditamento. Non sono necessariamente falsi, e chi li emette non sta necessariamente commettendo un illecito: sta semplicemente svolgendo un'attività di verifica privata, sulla quale nessun ente terzo ha mai controllato nulla.

Distinguerli è banale, una volta che si sa dove guardare. Un certificato accreditato riporta due marchi, non uno: quello dell'organismo di certificazione e quello dell'ente di accreditamento, che sia Accredia, UKAS o un altro ente aderente all'accordo IAF. Se il secondo marchio non c'è, la catena di fiducia descritta sopra si interrompe al primo anello.

Non è un caso scolastico. In un mercato in cui la certificazione è sempre più spesso un requisito contrattuale, e in cui l'accesso a una gara può dipendere dal possesso del titolo, esiste una domanda di documenti rapidi ed economici, e quindi esiste un'offerta.

Quanto è diffusa la certificazione in Italia

Qualche numero aiuta a inquadrare il fenomeno. Secondo l'ISO Survey, i certificati ISO/IEC 27001 attivi in Italia sono passati da 2.424 nel 2022 a 3.176 nel 2023, per arrivare a 3.284 nel 2024. Sul piano mondiale la norma raggiunge 96.709 certificati, con la Cina largamente in testa con 33.359 titoli, pari al 34,5% del totale, mentre l'Italia occupa la sesta posizione. Accredia legge la variazione italiana del 2024 come una crescita del 3%, segno dell'attenzione crescente delle imprese alla protezione dei dati e alla sicurezza informatica.



Fonte: ISO Survey, certificati validi al 31 dicembre di ciascun anno.

Figura 2 - La curva della certificazione ISO/IEC 27001 in Italia. Il balzo del 2023 e il quasi immediato assestamento dell'anno successivo descrivono una risposta a una pressione esterna più che un cambiamento culturale.

Il dato interessante, però, è la forma della curva. Il balzo registrato tra il 2022 e il 2023 supera il 30%, mentre l'anno successivo la crescita si assesta su valori molto più contenuti. Una progressione di questo tipo raramente descrive un cambiamento culturale, che procede lentamente e in modo regolare. Descrive piuttosto una risposta a una pressione esterna: nuovi requisiti contrattuali, nuove qualifiche di fornitore, nuovi obblighi che si sono affacciati e a cui le imprese hanno reagito in blocco.

Se la certificazione cresce perché qualcuno la chiede, allora la domanda su che cosa esattamente sia stato ottenuto in cambio diventa la domanda centrale. Ed è la domanda a cui serve saper rispondere leggendo il documento.

Sezione 3

Anatomia del certificato, campo per campo

Un certificato ISO/IEC 27001 è un documento di una sola pagina. La grafica cambia da organismo a organismo, ma i campi sono sempre gli stessi, perché sono in larga parte prescritti dalle regole che governano gli organismi di certificazione. Questo è un vantaggio per chi legge: una volta imparata la struttura, vale per tutti.

Quello che segue è un fac-simile costruito appositamente, con un'organizzazione di fantasia. I sette richiami numerati indicano i punti da controllare, nell'ordine in cui conviene controllarli (**Figura 3**).

1. I due marchi

Il primo controllo è visivo e dura tre secondi. Devono comparire due marchi: quello dell'organismo di certificazione e quello dell'ente di accreditamento. Se il secondo manca, si è di fronte a un certificato non accreditato: non necessariamente privo di sostanza, ma privo di qualunque verifica indipendente su chi lo ha emesso. Nel processo di qualifica di un fornitore, è un'informazione che va registrata, non ignorata.

2. La norma e la sua revisione

Deve leggersi **ISO/IEC 27001:2022**. La revisione precedente, la 27001:2013, è uscita di scena: il periodo di transizione stabilito a livello internazionale si è chiuso il 31 ottobre 2025 e da quella data i certificati riferiti alla vecchia edizione non sono più validi. Se un fornitore vi consegna oggi un documento che cita la 2013, non state leggendo un certificato datato: state leggendo un certificato scaduto. Il controllo si esaurisce qui.



Figura 3 - Fac-simile annotato. La grafica varia da organismo a organismo, ma i campi sono sostanzialmente sempre questi.

3. Il campo di applicazione

È la riga che determina il valore dell›intero documento, ed è quella che quasi nessuno legge fino in fondo. Il campo di applicazione descrive quali attività dell›organizzazione sono coperte dal sistema di gestione certificato. Tutto ciò che non è descritto lì dentro, semplicemente, non è certificato. Il test è uno solo, e la domanda che bisognerebbe porsi è: *il servizio che sto acquistando rientra in questa frase?* Nel fac-simile, l'erogazione del servizio cloud c'è; lo sviluppo del software no. Sono due cose diverse e la differenza è tutt'altro che teorica.

4. I siti coperti

Un sistema di gestione può coprire una sede, alcune sedi o tutte. Il campo va confrontato con i luoghi in cui il servizio viene effettivamente erogato e in cui i dati

vengono effettivamente trattati. Se il fornitore ha una sede operativa a Milano e un centro di sviluppo all'estero, e il certificato nomina solo Milano, il quadro è chiaro. Nelle organizzazioni con molte sedi entra inoltre in gioco il campionamento: l'organismo non visita ogni anno tutti i siti, ne verifica una parte secondo criteri definiti.

5. Le tre date

Prima emissione, emissione corrente, scadenza. Servono a collocare l'organizzazione nel ciclo triennale. Una prima emissione lontana nel tempo indica un sistema che ha attraversato più cicli completi, ed è un segnale di solidità; una scadenza molto vicina merita una domanda sullo stato del rinnovo. E soprattutto: la data di emissione corrente non dice se le verifiche intermedie siano state effettuate.

6. Il numero di certificato

Serve per il controllo successivo, che è quello davvero decisivo e che praticamente nessuno esegue.

7. La clausola sulla sorveglianza

Quasi tutti i certificati contengono, in caratteri minuti, una frase che subordina la validità del documento al superamento delle verifiche periodiche. È una frase importante: significa che il certificato che avete in mano è un documento a validità condizionata, e che la condizione non è verificabile guardando il documento stesso.

Il ciclo di certificazione e perché la carta non basta

La certificazione non è un evento ma un ciclo. La verifica iniziale si svolge in due fasi: una prima fase dedicata all'esame della documentazione e alla verifica che l'organizzazione sia pronta, e una seconda fase, sul campo, dedicata all'attuazione effettiva. Se l'esito è positivo viene emesso un certificato valido tre anni. Nei due anni successivi l'organismo svolge verifiche di sorveglianza, di durata ridotta rispetto a quella iniziale, e prima della scadenza si svolge una verifica di rinnovo, più ampia, che riapre il ciclo (**Figura 4**).

Da qui discende un fatto che conviene tenere presente: un certificato può essere formalmente in corso di validità mentre la sorveglianza è stata rinviata, è in corso una sospensione, oppure è stata rilevata una non conformità grave non ancora chiusa. Il documento cartaceo non lo dice. Lo dicono i registri.



Figura 4 - Il ciclo triennale. Le verifiche sono quattro in tre anni: fra l'una e l'altra il documento resta valido senza che nessuno stia guardando.

Il controllo che quasi nessuno esegue

Con il numero di certificato in mano, la verifica richiede due minuti e nessuna competenza tecnica. Gli strumenti sono due e sono entrambi pubblici e gratuiti.

Il primo è la **Banca Dati Accredia**, che pubblica i dati delle organizzazioni pubbliche e private in possesso di un certificato di sistema di gestione in corso di validità rilasciato da organismi accreditati, e consente di filtrare per numero di certificato, partita IVA, scopo, organismo, norma e revisione, oltre a visualizzare l'elenco dei siti coperti dalla certificazione. Il secondo è **IAF CertSearch**, il portale globale che permette di verificare in tempo reale la validità di un certificato e se l'organismo che lo ha rilasciato sia effettivamente accreditato per quello specifico schema.

Qui però va segnalata una cautela che raramente si trova scritta. I dati delle organizzazioni certificate sono caricati direttamente dagli organismi di certificazione, che ne sono responsabili per qualità e aggiornamento, e la banca dati può contenere anche certificati sospesi. In altre parole: trovare il certificato nel registro è una condizione necessaria, non sufficiente. Se non lo trovate, avete un problema serio. Se lo trovate, avete superato il primo filtro e potete passare alle domande vere.

© Clusit 2026

L'ottavo controllo: quello che il certificato non contiene

Esiste una domanda in più, che non si può leggere sul documento e che va posta al fornitore o, tramite lui, all'organismo di certificazione: **quante giornate di audit sono state impiegate, e come sono state calcolate.**

Non è una curiosità da addetti ai lavori. La ISO/IEC 27006-1:2024 contiene una tabella, nell'Annex C, che fissa il punto di partenza per il numero di giornate di verifica in funzione del numero di persone che lavorano sotto il controllo dell'organizzazione, con una giornata di audit normalmente pari a otto ore. La tabella non si applica meccanicamente: il tempo va poi corretto in base alla complessità dei processi informativi e dei sistemi utilizzati, alla struttura e distribuzione delle infrastrutture, al numero di persone che svolgono attività identiche o ripetitive e alla presenza di più sedi operative. Ma resta un riferimento pubblico e verificabile.

La conseguenza è netta: se il numero di giornate impiegate risulta drasticamente inferiore a quanto previsto da quelle tabelle, la validità del certificato diventa contestabile. Per chi valuta un fornitore, questa è la differenza fra un certificato guadagnato e un certificato acquistato, ed è l'unico modo per accorgersene senza essere un tecnico.

Sezione 4

Il perimetro: dove si gioca la partita

Se dovessi indicare un solo punto in cui si concentrano quasi tutti i fraintendimenti sulla certificazione, indicherei il campo di applicazione. È il luogo dove un documento formalmente ineccepibile può produrre una convinzione completamente sbagliata, senza che nessuno abbia commesso irregolarità.

La ragione è che la norma chiede all'organizzazione di determinare i confini e l'applicabilità del proprio sistema di gestione tenendo conto del contesto in cui opera, delle esigenze delle parti interessate e delle interfacce e dipendenze con le attività svolte da altri. Chiede cioè di *scegliere* un perimetro e di motivarlo. Non impone che quel perimetro coincida con l'intera organizzazione.

Questa libertà è ragionevole e in molti casi necessaria. Un gruppo industriale con dodici divisioni può avere interesse a certificare solo quella che tratta dati sensibili. Un'azienda manifatturiera può voler certificare la sola area che eroga servizi digitali ai

clienti. Sono scelte legittime, tecnicamente corrette e spesso più solide di una certificazione estesa e superficiale.

La stessa libertà, però, consente anche un uso diverso: ridurre il perimetro al minimo indispensabile per ottenere il titolo, allegarlo al questionario del cliente e lasciare che sia il cliente a immaginare che copra tutto. Anche in questo caso non c'è nulla di irregolare. C'è un'asimmetria informativa, e la si risolve leggendo.



Figura 5 - Un perimetro ridotto è una scelta legittima, non un abuso. Diventa un problema solo quando chi legge il certificato presume che copra l'intera organizzazione.

Le configurazioni che si incontrano più spesso sono poche e riconoscibili. La prima è l'organizzazione grande con il perimetro piccolo: quattrocento dipendenti, un certificato che copre una squadra di dodici persone su una singola linea di prodotto. La seconda è lo scarto geografico: sede legale e amministrativa certificate, sviluppo o gestione operativa svolti in un'altra sede che nel certificato non compare. La terza è lo scarto funzionale, ed è la più insidiosa perché la formula suona rassicurante: il certificato copre l'erogazione del servizio ma non la sua progettazione, oppure copre la gestione dell'infrastruttura ma non il trattamento dei dati che vi transitano.

In tutti e tre i casi non serve una competenza specialistica per accorgersene. Serve confrontare due frasi: quella scritta nel campo di applicazione e quella scritta nell'oggetto del contratto che state per firmare. Se non si sovrappongono, avete individuato esattamente lo spazio in cui vi state assumendo un rischio che credevate coperto.

Un certificato dal perimetro ristretto non è un certificato debole. È un certificato preciso, che qualcuno ha letto come se fosse generico.

Sezione 5

I documenti dietro il certificato

Il certificato è la sintesi di una pagina di un lavoro che ne produce alcune centinaia, e le informazioni che servono davvero a valutare un fornitore stanno nelle centinaia, non nella sintesi. Non sono documenti riservati per natura: il fornitore può decidere di condividerli, e un cliente può ragionevolmente chiederli in sede contrattuale o di qualificazione, eventualmente sotto accordo di riservatezza.
Sono quattro, in ordine di utilità decrescente.

La Dichiarazione di Applicabilità
È il documento più informativo che esista nel sistema, ed è quello che nessuno chiede. Elenca tutti i controlli previsti dalla norma e, per ciascuno, indica se sia stato applicato oppure no, con la relativa giustificazione. Leggerla significa vedere in trasparenza quali aree di sicurezza l›organizzazione ha deciso di presidiare e quali ha deciso di lasciare fuori, e soprattutto *perché*. Un'esclusione motivata da una caratteristica reale dell'organizzazione è un segno di maturità. Un'esclusione motivata da una formula generica è un'altra cosa.

La definizione del campo di applicazione
La frase che compare sul certificato è la versione compressa di un documento più esteso, che descrive i confini del sistema di gestione e le interfacce e dipendenze con le attività svolte da altri soggetti. È lì che si trova scritto, nero su bianco, che cosa il fornitore considera fuori dal proprio perimetro e a chi lo ha delegato.

Il piano di trattamento del rischio
Mostra quali rischi sono stati individuati, quali azioni sono state decise, con quali tempi e con quali responsabilità. Non serve leggerlo tutto: basta guardare le date di chiusura previste e confrontarle con quelle effettive. Un piano in cui tutte le azioni risultano completate nei termini è, statisticamente, un piano poco realistico.

Le non conformità e la loro chiusura
Ogni verifica produce rilievi. È normale, ed è anzi il segno che la verifica è stata fatta. Quello che conta è se si tratti di rilievi minori o di non conformità gravi, e come e in

quanto tempo siano stati risolti. Un fornitore che vi mostra le proprie non conformità e come le ha chiuse vi sta dando un'informazione molto più affidabile di quanto possa fare il certificato.

Sei segnali che riconosce chi verifica

Sono indizi, non prove. Presi singolarmente possono avere spiegazioni legittime. Presi insieme, descrivono con buona approssimazione un sistema di gestione costruito per l'audit anziché per l'organizzazione.

- Una Dichiarazione di Applicabilità che riproduce l'elenco dei controlli della norma senza giustificazioni proprie, o con giustificazioni identiche fra loro.
- Politiche e procedure tutte approvate nella stessa data, tipicamente poche settimane prima della verifica di certificazione.
- Un riesame della direzione privo di dati in ingresso tracciabili: nessun indicatore, nessun esito di audit interno, nessun incidente registrato.
- Un'analisi dei rischi in cui tutti gli esiti risultano accettabili e nessuna azione di trattamento è stata ritenuta necessaria.
- Un registro degli incidenti vuoto. In un'organizzazione che opera, un registro vuoto non significa che non accada nulla: significa che non viene registrato nulla.
- Un numero di giornate di verifica sproporzionato rispetto all'organico dichiarato nel perimetro.

Sezione 6

Cosa il certificato non può dire

Arriviamo al punto che dà il titolo all'articolo. Tutto quanto segue discende da una sola frase, che conviene mettere per iscritto perché è esattamente il punto in cui si separano la lettura corretta e quella corrente.

Un certificato ISO/IEC 27001 attesta il sistema di gestione di una determinata organizzazione, entro un perimetro che essa ha dichiarato.

Chi lo riceve tende invece a leggerlo come un'affermazione sullo stato di sicurezza complessivo di quell'organizzazione. La differenza fra le due letture non è una sfumatura terminologica: ogni gruppo di parole della prima frase esclude qualcosa che la seconda dà per acquisito. Le limitazioni che seguono non sono difetti da correggere né mancanze degli organismi di certificazione, e non dipendono dal comportamento di nessuno: sono le conseguenze dirette di come lo strumento è costruito. Conviene quindi raggrupparle come si raggruppano le parole di quella frase.

Un sistema di gestione, non uno stato di sicurezza

Non attesta un livello di protezione tecnica. La norma non richiede prove di penetration test, analisi del codice sorgente, scansioni di vulnerabilità o simulazioni di attacco. Richiede che l'organizzazione decida, sulla base della propria valutazione dei rischi, se quelle attività le servano, e che in caso affermativo le governi. Un'organizzazione certificata può non averne mai eseguita una ed essere pienamente conforme, purché abbia motivato la scelta. Il certificato attesta il processo decisionale, non l'esito tecnico di quel processo.

Conformità non significa efficacia. È la conseguenza più importante e la meno intuitiva, quindi vale la pena enunciarla senza attenuazioni: un›organizzazione può accettare formalmente un rischio elevato e restare pienamente conforme alla norma. La ISO/IEC 27001 richiede che i rischi siano identificati, valutati e trattati secondo criteri stabiliti dall›organizzazione, e prevede espressamente che una delle opzioni di trattamento sia l›accettazione, purché la decisione sia consapevole, motivata e assunta da chi ne ha l›autorità. Ne discende che il certificato non dice quanto rischio quell›organizzazione abbia accettato. Dice che esiste un processo strutturato per deciderlo e che quel processo è stato seguito. Sono due affermazioni molto diverse, e la seconda vale comunque parecchio: significa che qualcuno, in quell›azienda, ha guardato il problema e ha preso una decisione tracciabile.

Non attesta il rispetto di un obbligo di legge. Un sistema di gestione conforme alla ISO/IEC 27001 aiuta considerevolmente a rispettare la normativa sulla protezione dei dati personali e le discipline europee sulla sicurezza delle reti e dei sistemi informativi e sulla resilienza operativa del settore finanziario, perché condivide con esse impianto e vocabolario. Ma la conformità volontaria a una norma tecnica e la conformità a un obbligo normativo restano due piani distinti, con perimetri, destinatari e conseguenze differenti. Nessun certificato assorbe un obbligo di legge, e nessuna autorità di controllo lo accetta come tale.

Entro un perimetro dichiarato

Copre ciò che l'organizzazione ha scelto di far coprire. È il limite trattato per esteso nella sezione 4, e va richiamato qui perché nell›ordine logico viene per primo, non per ultimo. Il punto da aggiungere è che il documento non segnala in alcun modo quanta parte dell›organizzazione resti fuori: un certificato che copre il cinque per cento delle attività e uno che le copre tutte hanno lo stesso aspetto, la stessa dignità e lo stesso valore formale. La proporzione non compare, e non esiste un campo in cui potrebbe comparire.

Non si estende a chi sta a valle. Il certificato del vostro fornitore riguarda il vostro fornitore. Non dice nulla sull'azienda a cui quel fornitore ha affidato l'infrastruttura, la manutenzione applicativa o l'assistenza notturna. La norma chiede all'organizzazione certificata di governare i rapporti con i propri fornitori, e questo è già molto; non certifica i fornitori dei fornitori. In una catena di tre livelli, il documento copre il primo e descrive, indirettamente, il modo in cui il primo tiene d'occhio il secondo.

Di quell'organizzazione, in quel momento

È una fotografia, non un flusso. Come si è visto nella Figura 4, fra una verifica e l'altra passano dodici mesi. In quel periodo l'organizzazione può cambiare fornitore di infrastruttura, sostituire il responsabile della sicurezza, acquisire una società, migrare i sistemi, ridurre il personale. Il certificato non cambia. Un documento emesso undici mesi fa descrive un'organizzazione che potrebbe non esistere più in quella forma.

È una verifica per campione. Un gruppo di verifica non esamina tutti i processi, tutti i sistemi, tutte le sedi e tutte le registrazioni. Ne esamina un campione, entro un numero di giornate calcolato secondo criteri definiti. Non è un limite occulto: è il modo in cui funziona qualunque verifica di terza parte, e le regole che lo governano sono pubbliche, il che rende il campione sindacabile. Implica però che l'assenza di rilievi significhi «non è emerso nulla nel campione esaminato», non «non c'è nulla».

Non è una scala. Il certificato è binario: o c'è o non c'è. Non esiste un punteggio, un livello, una classe, un giudizio graduato. Due fornitori entrambi certificati non sono confrontabili fra loro sulla base del certificato, e nulla nei due documenti consente di dire quale dei due sia messo meglio, anche quando la distanza reale fra i due è enorme. Chi deve scegliere si ritrova con due fogli equivalenti e nessun criterio per distinguerli: i criteri stanno nei documenti della sezione 5, e vanno chiesti.

Non trasferisce responsabilità. Il certificato non è una garanzia, non è una polizza e non è una manleva. Se un fornitore certificato perde i vostri dati, la vostra posizione nei confronti dei vostri clienti e delle autorità non cambia di una virgola per il fatto

che quel fornitore fosse certificato. Averlo verificato può concorrere a dimostrare che avete scelto con diligenza, il che non è poco, ma la responsabilità resta dove il contratto e la legge la collocano. Il certificato serve a scegliere meglio prima, non a rispondere di meno dopo.

Un incidente non lo smentisce. Quando un'organizzazione certificata subisce un attacco informatico, la reazione ricorrente è chiedersi a cosa sia servito il certificato. È una domanda mal posta. Nessun sistema di gestione promette che non accadano incidenti: promette che l'organizzazione sia attrezzata per prevenirli entro limiti ragionevoli, per accorgersene, per reagire e per imparare. Il criterio di giudizio corretto, dopo un incidente, non è se sia accaduto, ma quanto tempo l'organizzazione abbia impiegato ad accorgersene, come abbia comunicato e che cosa abbia cambiato dopo. È esattamente lì che si vede se il sistema di gestione fosse reale.

Nove osservazioni, una frase sola

Messe in fila, queste nove osservazioni non sono un elenco di difetti: sono la stessa frase letta lentamente, mettendo insieme tutti i pezzi. Un sistema di gestione, quindi niente sul piano tecnico e niente sull'efficacia. Entro un perimetro dichiarato, quindi niente su ciò che sta fuori e su chi sta a valle. Di quell'organizzazione in quel momento, quindi nessuna misura, nessun confronto, nessuno spostamento di responsabilità.

Il valore pratico di questa lettura è che ciascuna limitazione indica con precisione dove andare a cercare la risposta mancante: il perimetro nella definizione estesa del campo di applicazione, l'efficacia nel piano di trattamento del rischio, la solidità del metodo nel calcolo delle giornate di verifica, il confronto fra due fornitori in ciò che si chiede oltre il certificato. Lo strumento non risponde a queste domande perché non è stato costruito per rispondervi. Ma le rende formulabili, e le rende formulabili a chiunque, in una pagina. Nessun altro documento sul mercato lo fa con la stessa economia.

Sezione 7

Come si usa

Tutto quanto precede può essere condensato in una procedura che un ufficio acquisti può eseguire senza competenze tecniche e in un tempo compatibile con il lavoro reale. I primi sei punti richiedono un quarto d'ora complessivo. Gli ultimi quattro richiedono di scrivere una mail.

1. Verificare che sul documento compaiano due marchi: organismo di certificazione ed ente di accreditamento.
2. Verificare che la norma indicata sia la ISO/IEC 27001:2022. Qualunque altra revisione chiude la valutazione.
3. Leggere per intero il campo di applicazione e confrontarlo con l'oggetto del contratto. Se non coincidono, annotare la differenza.
4. Confrontare i siti indicati con i luoghi in cui il servizio viene erogato e i dati trattati.
5. Controllare le tre date e collocare l'organizzazione nel ciclo triennale.
6. Cercare il numero di certificato nella Banca Dati Accredia e su IAF CertSearch, ricordando che il registro può contenere anche certificati sospesi.
7. Chiedere la Dichiarazione di Applicabilità e leggere le esclusioni con le relative giustificazioni.
8. Chiedere quante giornate di verifica sono state impiegate e come sono state calcolate.
9. Chiedere se nell'ultimo ciclo siano state rilevate non conformità gravi e come siano state chiuse.
10. Chiedere quali attività rilevanti per il contratto siano affidate a subfornitori e come vengano governate.

Nessuna di queste domande è ostile, e un fornitore solido risponde volentieri a tutte, perché sono le stesse domande che si è posto internamente. La reazione a una richiesta di questo tipo è, di per sé, un'informazione.

Il certificato accanto agli altri strumenti

L'ultimo passaggio consiste nel collocare la certificazione fra gli strumenti disponibili, che rispondono a domande diverse e non sono intercambiabili. La confusione fra loro è la causa di buona parte delle attese mal riposte.

Strumento	A quale domanda risponde	A quale non risponde	Quando chiederlo
Certificato ISO/IEC 27001	Esiste un sistema organizzato per governare la sicurezza, verificato da un terzo indipendente?	Quanto rischio è stato accettato, e com'è messa tecnicamente l'infrastruttura.	Sempre, come primo filtro in qualificazione fornitore.
Rapporto SOC 2 Type II	I controlli dichiarati hanno funzionato lungo un periodo osservato, e con quali eccezioni?	Se l'organizzazione governi la sicurezza nel suo complesso, fuori dai controlli esaminati.	Per servizi digitali continuativi, in particolare con controparti anglosassoni.
Test di penetrazione	Un sistema specifico resiste a un tentativo di intrusione condotto in un dato momento?	Nulla su organizzazione, processi, personale e governo del rischio.	Quando il servizio è esposto in rete e il dato è critico.
Questionario di sicurezza	Che cosa il fornitore dichiara di fare, nel dettaglio che vi interessa?	Se quanto dichiarato corrisponda alla realtà: nessuno lo verifica.	Per coprire gli aspetti specifici del vostro contratto.
Diritto di audit contrattuale	Che cosa accade davvero, guardato con i vostri criteri e sul vostro perimetro?	Nulla, se non lo esercitate: è la clausola meno usata dei contratti.	Per forniture critiche, con soglie e preavvisi definiti.

La tabella dice una cosa sola: il certificato è il punto di partenza più efficiente che esista, perché non costa nulla al cliente e concentra in una pagina il lavoro di una verifica indipendente. Ma è un punto di partenza. Gli strumenti che seguono rispondono alle domande che il certificato lascia aperte per costruzione.

Sezione 8

Il certificato come inizio di una conversazione

Torniamo all'ufficio acquisti da cui siamo partiti. La stessa scena, con un lettore diverso, produce un esito diverso: quindici minuti di controlli, tre domande scritte al fornitore, e una valutazione che poggia su qualcosa. Non è un lavoro specialistico. È leggere un documento sapendo che cosa vi si può leggere.

La certificazione ISO/IEC 27001 resta uno degli strumenti più utili di cui il mercato disponga: riduce l'asimmetria informativa fra chi compra e chi vende, evita la molti-

plicazione delle verifiche e costringe le organizzazioni a mettere per iscritto decisioni che resterebbero implicite. Il suo limite non è nella norma, è nel modo in cui viene usata.

C'è un'ultima considerazione che porta fuori dal perimetro di questo articolo, e conviene lasciarla come domanda aperta. Abbiamo visto nella Figura 2 che la certificazione in Italia cresce a scatti, in coincidenza con l'intensificarsi delle richieste contrattuali. Questo significa che, per un numero crescente di imprese, la sicurezza delle informazioni non entra in azienda come scelta ma come requisito imposto da un cliente, da un capitolato, da un pacchetto di accreditamento fornitore.

È un meccanismo che ha prodotto risultati reali e che ha alzato il livello medio del sistema produttivo. Ma solleva una domanda che vale la pena porsi: quanti di quei requisiti le imprese riescono effettivamente ad attuare, e a quale costo? Fra ciò che viene richiesto per contratto e ciò che viene realizzato in azienda si apre una distanza che si accumula nel tempo, silenziosamente, e che qualcuno prima o poi dovrà pagare.

Nota sulle fonti. I riferimenti normativi sono ISO/IEC 27001:2022 e ISO/IEC 27006-1:2024. Le scadenze di transizione citate (31 ottobre 2025 per la ISO/IEC 27001:2013, 31 marzo 2026 per la ISO/IEC 27006:2015) derivano dalle disposizioni internazionali applicabili agli organismi di certificazione accreditati. I dati sulla diffusione dei certificati provengono dall'ISO Survey e si riferiscono ai certificati validi al 31 dicembre di ciascun anno; le letture di sintesi sul mercato italiano sono di Accredia. I registri pubblici citati sono la Banca Dati Accredia e IAF CertSearch.

Nota sul fac-simile. Il certificato riprodotto nella Figura 3 e l'organizzazione rappresentata nella Figura 5 sono interamente di fantasia, costruiti a scopo illustrativo. Nomi, indirizzi, numeri e date non si riferiscono ad alcuna organizzazione reale né riproducono documenti esistenti.

GLOSSARIO

Account hijacking	Compromissione di un account ottenuta ad esempio mediante ***phishing***.
Account take-over	Acquisizione illecita di un account al fine di impersonificare la vittima (ad esempio di effettuare transazioni finanziarie sui suoi conti).
ACDC (Advanced Cyber Defence Center)	Progetto europeo la cui finalità è offrire soluzioni e creare conoscenza per aiutare le organizzazioni in tutta Europa a combattere le botnet. *(*www.acdc-project.eu/*).*
AI agentica	Tipologia di sistemi basata su autonomia operativa, contestualizzazione avanzata e capacità decisionali sviluppate su più livelli.
AI-BOM (AI Bill of Materials)	Fotografia delle configurazioni di un sistema AI in un dato momento, utile a individuare modifiche, compromissioni o deviazioni rispetto allo stato atteso.
AISP (Account Information Service Provider)	Prestatori di servizi di informazione sui conti di pagamento che forniscono ai clienti che detengono uno o più conti di pagamento online presso uno o più Istituti di Credito, servizi informativi relativi a saldi o movimenti dei conti aperti.
Agentive AI	AI in grado di prendere decisioni e agire in modo autonomo perseguendo uno specifico obiettivo.
Analytics-As-A-Service	Servizi on demand per l'analisi di dati utilizzabili anche nell'ambito della sicurezza, ad esempio, per passare al setaccio i dati della rete aziendale e individuare eventi anomali ed eventuali attacchi.
APA (Attack Path Analysis)	Tecnica utilizzata nel campo della sicurezza informatica per identificare e valutare i percorsi potenziali attraverso i quali un attaccante potrebbe violare un sistema o una rete.

Apt (Advanced Persistent Treath)	Schemi di attacco articolati, mirati a specifiche entità o organizzazioni contraddistinti da: • un accurato studio del bersaglio preventivo che spesso continua anche durante l'attacco • l'impiego di tool e ***malware*** sofisticati • la lunga durata o la persistenza nel tempo cercando di rimanere inosservati per continuare a perpetrare quanto più possibile il proprio effetto.
Arbitrary File Read	Vulnerabilità che consente ad un attaccante di accedere a file tramite richieste Web remote.
Assume breach	Approccio secondo cui gli operatori di sicurezza partono dal presupposto che, prima o poi, un attacco andrà a buon fine, e dunque strutturano processi, strumenti e competenze per rilevare, investigare e contenere rapidamente qualsiasi compromissione.
Attacchi Pivot back	Tipo di attacco nel quale viene compromessa una risorsa nel public cloud per ottenere informazioni che possono poi essere usate per attaccare l'ambiente on premise.
BITS Jobs (Background Intelligent Transfer Service)	Tecnica che consente ai cybercriminali di programmare ed eseguire download malevoli in background senza destare sospetti.
Blockchain	Tecnologia che consente la registrazione di transazioni, in uno scenario trustless, fra gli attori della stessa blockchain mediante l'utilizzo di un registro digitale immodificabile presente su vari nodi della rete, costituito da blocchi (block) fra loro concatenati (chain).
Booter-stresser	Strumenti a pagamento che consentono di scatenare attacchi ***DDOS***.
CAL (Cybersecurity Assurance Level)	Indicatore dinamico dello sforzo necessario per garanzia la sicurezza di un elemento, derivante dai rischi relativi a tutti i suoi asset.
Captatore informatico	Software che viene immesso in dispositivi elettronici portatili al fine di intercettare comunicazioni o conversazioni tra presenti, il cui uso è specificatamente regolamentato dal Codice Penale.

Carding	Scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari.
CDR (Cloud Detection and Response)	Approccio alla sicurezza che nasce per fornire ai team di SecOps, in particolare SOC (Security Operations Center) e IR (Incident Response), le capacità di cui hanno bisogno per monitorare, individuare e bloccare attacchi specifici per il Cloud.
CEO Fraud	Tipi di attacco phishing mirati verso figure aziendali ad altissimo profilo, generalmente amministratori delegati, presidenti dell'azienda, direttori finanziari, etc.
CFC (Cyber Fusion Center)	Approccio olistico e multidisciplinare alla gestione della sicurezza che mira a superare la tradizionale suddivisione fra compiti (intelligence, analisi, risposta…) e team.
CLOSINT (Close Source Intelligence)	Processo di raccolta di informazioni attraverso la consultazione di fonti chiuse, cioè non accessibili pubblicamente: intelligence feed, fonti governative, informazioni classificate, etc.
Cloud weaponization	Tipo di attacco nel quale l'attaccante ottiene un primo punto d'ingresso nell'infrastruttura cloud attraverso la compromissione e il controllo di alcune machine virtuali. L'attaccante utilizza poi questi sistemi per attaccare, compromettere e controllare migliaia di altre macchine, incluse altre appartenenti allo stesso service provider cloud dell'attacco iniziale, e altre appartenenti ad altri service provider pubblici.
CNAPP (Cloud-Native Application Protection Platform)	Categoria di soluzioni che riunisce diverse funzionalità di sicurezza in un'unica piattaforma, per proteggere le applicazioni in cloud.
CNOs (Computer Network Operations)	Tipologia di ***Information warfare*** finalizzato all'attacco e distruzioni delle informazioni presenti sui sistemi informativi avversari, alla distruzione delle reti e dei sistemi stessi e alla difesa delle proprie.
CNP (Card-Not-Present)	Indica un pagamento effettuato senza la presenza fisica di una carta di pagamento, ad esempio su Internet.

© Clusit 2026

CoA (Courses of Action)	Nella dottrina militare identifica un piano che descrive le strategie e le azioni operative scelte per portare a termine una determinata missione. Nell'ambito della ***Cyber Intelligence*** rappresenta le attività poste in essere rispettivamente dagli attaccanti o dai difensori per la conduzione o il contrasto delle azioni funzionali ad un attacco cyber.
Constituency	Nell'ambito di un ***CERT*** indica a chi è rivolto il servizio (ad esempio Pubblica Amministrazione Centrale, Regioni e Città metropolitane).
Context-based access	Tecnica che condiziona l'accesso alla valutazione dinamica del rischio della singola transazione, modulando eventuali azioni aggiuntive di verifica. Ad esempio le soluzioni di autenticazione e autorizzazione, sia nel caso di login che di disposizione di operazioni, non si limitano più ad autorizzare o bloccare un'operazione, ma offrono una gamma intermedia di possibilità, come ad esempio autorizzare un'operazione, ma con dei limiti, oppure richiedere verifiche aggiuntive.
C&C (Command &Control)	I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal ***malware*** utilizzato per la costruzione della ***botnet***. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la botnet, al fine di rendere più difficile la localizzazione di questi ultimi.
Counterintelligence	Identificazione, valutazione, neutralizzazione e sfruttamento delle attività di intelligence svolte da entità avversarie.
Course of action matrix	Metodologia per l'identificazione, la prioritizzazione e la rappresentazione sinottica delle azioni da intraprendere, in caso di possibili intrusioni. È composta da: - due azioni passive: *Discover* e *Detect* - cinque attive - *Deny, Disrupt, Degrade, Deceive, Destroy).*
Credential Stuffing	Attacco nel quale vengono utilizzate coppie di user id/password raccolte in precedenza in modo fraudolento.

Cryptojacking	Processo che sfrutta illegalmente le risorse informatiche di una vittima per generare criptovaluta. In sostanza gli aggressori sottraggono potenza di calcolo installando un'applicazione di mining di criptovaluta sul sistema della vittima, che sia un PC o uno smartphone. La generazione di valuta virtuale, nota anche come criptovaluta, è molto dispendiosa in termini di potenza di elaborazione, motivo per cui gli aggressori devono infettare un vasto numero di vittime e utilizzarne la potenza di calcolo per generare nuove unità monetarie virtuali.
Cryptolocker	***Malware*** che ha come finalità criptare i file presenti nel dispositivo infetto al fine di richiedere un riscatto alla vittima per renderli nuovamente intellegibili.
CTW (Check-the-Web)	Piattaforma tecnologiche appositamente creata in ambito ***IRU*** a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet, il cui ruolo principale è di anticipare e prevenire l'abuso terroristico di strumenti online, nonché di svolgere un ruolo consultivo proattivo a tale riguardo nei confronti degli Stati membri dell'UE e del settore privato.
CVSS versione 3 (Common Vulnerability Scoring System)	Sistema di valutazione delle vulnerabilità che fornisce un modo per acquisire le principali caratteristiche di una vulnerabilità e per produrre un punteggio numerico che rifletta la sua gravità, nonché una rappresentazione testuale di tale punteggio. Il punteggio numerico può quindi essere tradotto in una rappresentazione qualitativa (come bassa, media, alta e critica) per aiutare le organizzazioni a valutare e prioritizzare in modo adeguato i loro processi di gestione delle vulnerabilità. (https://www.first.org/cvss/specification-document)

CTI (Cyber Threat Intelligence)	Disciplina che si occupa di raccogliere e analizzare dati eterogenei - provenienti da diverse sorgenti informative interne ed esterne -per estrarre informazioni utili a conoscere le caratteristiche dell'attore della minaccia, in modo da poter attribuire un profilo di rischio specifico per i propri asset e sviluppare azioni di contrasto efficaci. In particolare, le attività di CTI si esplicano attraverso un processo di raccolta, classificazione, integrazione e analisi di dati grezzi relativi a minacce che operano nel cyberspazio.
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.
Cyber Kill Chain	La cyber kill chain è un modello definito dagli analisti di Lockheed Martin come supporto decisionale rispetto alla rilevazione e risposta alle minacce. Esso include le seguenti fasi: *reconnaissance, weaponization, delivery, exploitation, installation and persistence, command and control (C2), actions.*
Cybersquatting	Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.
Cyber resilience	Capacità di un'organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso.
Cyber-reasoning systems	Sistemi sviluppati per individuare automaticamente le vulnerabilità delle reti più complesse implementando algoritmi cognitivi.
Cyber-weapon	***Malware*** (o anche hardware) progettato o utilizzato per causare danni attraverso il dominio cyber. (*NATO Cooperative Cyber Defence Centre of Excellence*).
CYBINT (Cyber Intelligence)	Disciplina che trae origine dalla declinazione classica delle attività di intelligence con riferimento alle peculiarità del dominio di ricerca informativa in ambito cyber. L'attività CYBINT si evolve includendo attività di analisi strategica e analisi di contesto su trend di eventi, scenari geopolitici e previsionali.

Data Diode	Un dispositivo di sicurezza che permette il flusso unidirezionale dei dati, impedendo qualsiasi comunicazione nella direzione opposta.
Data Leakage	Trasferimento non autorizzato di informazioni riservate.
DDoS (Distributed Denial of Service)	Attacchi DOS distribuiti, cioè basati sull'uso di una rete di apparati, costituenti in una botnet dai quali parte l'attacco verso l'obiettivo.
DDoS-for-hire	Letteralmente servizio DDoS da noleggiare.
Debunking	Insieme di attività volte a verificare se il un contenuto, ad esempio di un file multimediale, sia falso.
Defense in Depth	Una strategia di sicurezza che implementa controlli multipli e stratificati, in modo che se un livello viene compromesso, altri livelli di protezione rimangono attivi.
Deep Fake	Algoritmi di deep learning in grado di creare foto o video falsi.
Deep Web	L'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (Google, Bing…).
DES (Data Encryption Standard)	Algoritmo per la cifratura dei dati a chiave simmetrica.
DGA (Domain generation algorithms)	Algoritmo utilizzato da alcuni malware per la generazione di migliaia di nomi di dominio alcuni dei quali sono utilizzati dai loro server ***C&C***.
Diamond Model	Framework strutturato per l'analisi tecnica di possibili intrusioni. (*Adversary, Infrastructure, Victim, Capability*).
Digital Twin	Una rappresentazione virtuale e dinamica di un sistema fisico che viene aggiornata in tempo reale attraverso sensori.
Digital Scarcity	In una ***blockchain*** la capacità di rendere non riproducibili informazioni digitali come file o pagamenti.
DMARC (Domain-based Message Authentication, Reporting and Conformance	Standard di autenticazione delle e-mail che aiuta a prevenire la falsificazione del mittente (spoofing) e il phishing.

© Clusit 2026

DNS cache poisoning	Tipo di attacco nel quale l'attaccante inserisce corrispondenze Indirizzo-IP alterate all'interno della cache del meccanismo di risoluzione degli indirizzi IP. Come risultato la cache userà l'indirizzo IP alterato in tutte le successive transazioni. L'indirizzo che comparirà nella barra URL di un browser sarà quello corretto e desiderato, ma il corrispondente indirizzo IP utilizzato sarà quello alterato e tutto il traffico di rete sarà quindi reindirizzato verso il sito replica controllato dai cyber criminali e nel quale si simulano log in per tracciare tutti i fattori di autenticazione inseriti.
DNS Open Resolver	Sistemi vulnerabili utilizzati come strumento per perpetrare attacchi informatici di tipo ***DDOS*** amplificati.
DNSSEC (Domain Name System Security Extensions)	Insieme di specifiche per garantire alcuni aspetti di sicurezza delle informazioni fornite dai ***DNS***.
Dos (Denial of Service)	Attacchi volti a rendere inaccessibili alcuni tipi di servizi. Possono essere divisi in due tipologie: • applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti); • volumetrici, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse. Se vengono utilizzati più dispositivi per l'attacco coordinati da un centro di ***C&C*** si parla di ***DDOS*** (Destributed Denial of Service).
Double extortion	Attacchi ransomware che, oltre a cifrare i file, ne fanno anche una copia di "sicurezza" con il loro trasferimento sui computer dei cyber criminali minacciando di procedere alla loro diffusione pubblica e/o metterli all'asta nel dark web per la vendita al miglior offerente.
Downloader	Software deputati a scaricare ulteriori componenti malevoli dopo l'infezione iniziale.

Drive-by exploit kit	Il fenomeno dei drive-by ***exploit kit*** è particolarmente insidioso e si realizza inducendo l'utente a navigare su pagine web che nascondono attacchi, appunto gli exploit ***kit***, ***per*** versioni vulnerabili di Java o dei plug-in del browser. Questi attacchi sono in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione sulle pagine malevole anche in assenza di interazione dell'utente con la pagina.
DRdos (Destribuited Reflection Denial of Service)	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Questa tipologia di ***DDOS*** permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del ***protocollo NTP***.
Dropper	Codice che installa il ***malware*** sul computer della vittima.
Eavesdropping	Nell'ambito VOIP è un attacco del tutto simile al classico man-in-the-middle. L'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni
eBPF (Extended Berkeley Packet Filter)	Tecnologia integrata nel kernel di Linux, che consente di monitorare e filtrare il traffico di rete in tempo reale senza impattare negativamente sulle prestazioni, offrendo un livello di protezione granulare e adattivo, capace di rispondere automaticamente ai cambiamenti dell'infrastruttura.
EDR (Endpoint Detection and Response)	Dispositivi la cui finalità è quella di mantenere un costante monitoraggio di eventi sospetti al fine di garantire una reazione preventiva e continua alle minacce.
Enterprise Architecture	Sistema informativo che, raccogliendo dati da tutte le funzioni dell'organizzazione, li collega in un unico modello informativo consentendo di visualizzare complessivamente lo stato dell'organizzazione e contemporaneamente di immaginarne la possibile evoluzione futura, rinforzandone la capacità di reagire ad eventi esterni.

© Clusit 2026

ERTMS (European Rail Traffic Management System)	Sistema europeo di segnalamento e controllo della velocità che garantisce l'interoperabilità dei sistemi ferroviari nazionali, oltre che aumentare la velocità dei treni, la capacità delle infrastrutture e il livello di sicurezza nel trasporto ferroviario.
Evasion	Nell'ambito delle applicazioni di IA attacco che consiste nel confondere la classificazione del dato in ingresso, da parte di un algoritmo precedentemente addestrato, manipolandone il contenuto.
Exploit	Codice con cui è possibile sfruttare una ***vulnerabilità*** di un sistema. Nel database Common Vulnerabilities and Exposures (cve.mitre.org) sono presenti sia le vulnerabilità note, sia i relativi exploit.
Exploit kit	Applicazioni utilizzabili anche da attaccanti non esperti, che consentono di sfruttare in forma automatizzata le ***vulnerabilità*** di un dispositivo (di norma browser e applicazioni richiamate da un browser).
Facing applications	Applicazioni rivolte al pubblico, quali ad esempio siti web.
Fast flux	Tecnica che permette di nascondere i ***DNS*** usati per la risoluzione dei domini malevoli dietro ad una rete di macchine compromesse in continua mutazione e perciò difficili da mappare e spegnere.
Fix	Codice realizzato per risolvere errori o ***vulnerabilità*** nei software.
Ghost broking	Pratica secondo la quale il frodatore, spacciandosi per agente di un'impresa assicurativa, a seguito del pagamento di un "premio" rilascia al cliente una polizza assicurativa, ovviamente falsa.
GRE (Generic Routing Encapsulation)	Protocollo di tunneling che incapsula vari protocolli di livello rete all'interno collegamenti virtuali point-to-point.
Harness (sistemi agentici)	Strato di orchestrazione che coordina agenti e strumenti, trasforma le capacità del modello in un processo operativo e stabilisce cosa l'agente può vedere o fare.

Hate speech	Il Comitato dei ministri del Consiglio d'Europa definisce gli hate speech come le forme di espressioni che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o più in generale l'intolleranza, ma anche i nazionalismi e gli etnocentrismi, gli abusi e le molestie, gli epiteti, i pregiudizi, gli stereotipi e le ingiurie che stigmatizzano e insultano. RECOMMENDATION No. R (97) 20 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON "HATE SPEECH" - Adopted by the Committee of Ministers on 30 October 1997
Harvest now, decrypt later	Tecnica che consiste nel raccogliere i dati crittografati per una successiva decrittazione, quando la potenza di calcolo quantistico diventerà più accessibile.
Hit & Run (o Pulse wave)	Attacchi di breve durata, ma frequenti nell'arco di poche ore.
HMI (Human Machine Interface Systems)	Componente fondamentale dei sistemi IT industriali, che permette all'operatore umano di interagire con gli ambienti di controllo, supervisione e acquisizione dati (supervisory control and data acquisition - SCADA).
Honeypot	Letteralmente barattolo del miele. Indica un asset esca isolato verso cui indirizzare e raccogliere informazioni su eventuali attacchi, al fine di tutelare il reale sistema informativo.
HTTP POST DoS Attack	Attacco che sfrutta un difetto di progettazione di molti server web. L'attaccante inizia una connessione http del tutto lecita verso un server web andando ad abusare del campo 'Content-Lenght'. Visto che la maggior parte dei server web accetta dimensioni del payload del messaggio anche di 2Gb, l'attaccante comincia ad inviare il corpo del messaggio ad una ridottissima velocità (anche 1byte ogni 110 secondi). Ciò comporta che il server web resta in ascolto per molto tempo, lasciando aperti i canali http (del tutto leciti) andando quindi a saturare tutte le sue risorse visto che le connessioni restano aperte.

HUMINT (HUMan INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da persone fisiche. Le sue specificità sono legate alla tipicità della fonte e si sostanziano soprattutto in particolari modalità di gestione. *(Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi* - www.sicurezzanazionale.gov.it*)*
Kill Switch	Termine generico per indicare un dispositivo che serve a bloccare in modo forzato un'attività.
IACS (Industrial Automation and Control Systems)	I sistemi IACS non comprendono esclusivamente la componente hardware e software dei sistemi di controllo industriale (ICS), ma includono anche i processi operativi e le persone che interagiscono con essi all'interno dell'ecosistema industriale. In questo contesto, il concetto di utente non si limita alla sola persona fisica, ma si estende anche ai dispositivi e alle applicazioni software che accedono, comunicano o interagiscono con il sistema di automazione.
IBAN Swapping	Sostituzione delle coordinate di pagamento IBAN o del wallet elettronico; questo ultimo caso soprattutto per i malware sui dispositivi mobili.
ICMP (Internet Control Message Protocol)	Protocolli che consentono ai dispositivi di una rete di comunicare informazioni di controllo e messaggi.
ICS (Industrial Control System)	Sistemi di controllo industriale.
IDS (Intrusion detection system)	Dispositivo in grado di identificare modelli riconducibili a possibili attacchi alla rete o ai sistemi.
IGA (Identity Governance & Administration)	Strumento di governance ed amministrazione delle identità che aiuta a garantire un provisioning, un re-provisioning ed un deprovisioning accurato dell'accesso degli utenti.
IMEI (International Mobile Equipment Identity)	Codice univoco che identifica un terminale mobile

IMSI (International Mobile Subscriber Identity)	Codice univoco internazionale che combina SIM, nazione ed operatore telefonico.
IoB (Internet of Bodies)	IoT applicato ai sistemi biologici. Dispositivi che raccolgono dati biometrici, fisiologici e comportamentali.
Incident handling	Gestione di un incidente di sicurezza informatica. ENISA classifica le fasi di tale gestione in Incident report, Registration, Triage, Incident resolution, Incident closure, Post-analysis.
Information warfare	Insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico…
Infostealer	***Malware*** finalizzato a sottrarre informazioni, quali ad esempio credenziali, dal dispositivo infetto.
Instant phishing	Tecnica di attacco nella quale nell'istante in cui l'utente inserisce le credenziali, o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi in real time, queste informazioni per effettuare azioni dispositive.
Interception and Modification	Nell'ambito VOIP intercettazione di comunicazioni lecite tra utenti ed alterazione delle stesse con lo scopo di arrecare disservizi come l'abbassamento della qualità delle conversazioni e/o l'interruzione completa e continua del servizio.
Intrusion software	***Spyware*** (definizione della Commissione Europea nell'ambito della regolamentazione dell'esportazione di prodotti ***dual use***). Un "intrusion software", ad esempio, può essere utilizzato da una società di security per testare la sicurezza di un sistema informatico e al contempo essere usato da uno Stato non democratico per controllare e intercettare le conversazioni dei propri cittadini.
IoA (Indicatori di attacco)	Informazioni funzionali all'individuazione di un potenziale attacco anche prima che ci sia contatto diretto tra attaccante e attaccato.

© Clusit 2026

IoC (Indicatori di compromissione)	Qualsiasi informazione che possa essere utilizzata per cercare o identificare sistemi potenzialmente compromessi (indirizzo IP/nome dominio, URL, file hash, indirizzo email, X-Mailer…) *(Common Framework for Artifact Analysis Activities – ENISA)*
IP Fragmentation	Tipo di attacco ***DDOS*** (Destribuited Denial of Service) che sfrutta il principio di frammentazione del protocollo IP.
IPMI (Intelligent Platform Management Interface)	Specifica di una interfaccia di basso livello utilizzata da diversi costruttori che consente ad un amministratore di sistema di gestire server a livello hardware. Attraverso la BMC *(Baseboard Management Controller)* consente, tra le altre cose, l'accesso al BIOS, ai dischi ed ai dispositivi hardware in generale e, di fatto, il controllo del server. IPMI contiene una serie di vulnerabilità ampiamente descritte e conosciute e, in definitiva, non dovrebbe essere aperto all'esterno.
IPS (Intrusion prevention system)	Dispositivo in grado non solo di identificare possibili attacchi, ma anche di prevenirli.
ISA/IEC 62443	Uno standard ISO che definisce requisiti di sicurezza per i sistemi di automazione e controllo industriale.
ITDR (Identity Threat Detection and **Response)**	Insieme di strategie, processi, tecnologie utilizzati per rilevare, analizzare e rispondere alle minacce che prendono di mira le identità digitali.
Jamming	Interferenza intenzionale o volontaria di un segnale elettromagnetico al fine di disturbare, bloccare o impedire la ricezione corretta del segnale da parte dei dispositivi destinatari.
LOTL (Living Off The Land)	Tipo di attacco basato su strumenti nativi preinstallati nel sistema operativo.
LOTS (Living Off Trusted Sites)	Tecnica di attacco che permette agli attori di sfruttare strumenti presenti nei sistemi attaccati per eseguire attività malevole senza essere scoperti.

MAAS (Malware as a Service)	Modello di erogazione del codice malevole dove un team di esperti "produce" malware, sviluppa exploits e si occupa della loro ricerca e sviluppo, mentre una catena di distributori si occupa di procacciare i clienti.
Malvertising	Tecniche che utilizzano l'ambito della pubblicità on line come veicolo di diffusione di ***malware***.
Man in the browser	Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di una banca, al fine di poterle riutilizzare.
Meaconing	Interferenza con i segnali di navigazione, come quelli provenienti dai sistemi GPS, al fine di alterare le informazioni di posizione e indirizzare in modo errato i dispositivi di navigazione o di localizzazione.
Memcached	Software spesso usato sui server web per effettuare caching di dati e per diminuire il traffico sul database o sul backend. Il server memcached è pensato per non essere esposto direttamente su Internet, per questo nella sua configurazione di default non richiede autenticazione e risponde sia via TCP che via UDP.
MFA (Multi-Factor Authentication)	Autenticazione a più fattori, nella quale si combinano più elementi di autenticazione per rendere più complessa la compromissione del sistema.
MFA Fatigue	Tecnica di attacco in cui l'utente riceve numerose richieste di autenticazione multi-fattore fino a quando, per stanchezza, ne approva una.
MFU (Malicious File Upload)	Attacco ad un web server basato sul caricamento remoto di ***malware*** o più semplicemente di file di grandi dimensioni.
Mining	Creazione di nuova criptovaluta attraverso la potenza di calcolo degli elaboratori di una ***blockchain***.

© Clusit 2026

MitC (Man in the Cloud) Definizione coniata dall'azienda Imperva	Tipo di attacco nel quale la potenziale vittima è indotta a installare del software malevolo attraverso meccanismi classici come l'invio di una mail contenente un link a un sito malevolo. Successivamente il malware viene scaricato, installato, e ricerca una cartella per la memorizzazione di dati nel cloud sul sistema dell'utente. Successivamente, il malware sostituisce il token di sincronizzazione dell'utente con quello dell'attaccante.
Mules	Soggetti che consentono di "convertire" attività illegali in denaro (cash out) ad esempio attraverso attività di riciclaggio.
NHI (Non-Human Identity)	Identità digitali non riferite a una persona (account di servizio, bot, chiavi API, workload, agenti AI).
NTP (Network Time Protocol)	***Protocollo*** che consente la sincronizzazione degli orologi dei dispositivi connessi ad una rete.
OF2CEN (On line Fraud Cyber Centre and Expert Network)	Piattaforma in cui far confluire tutte le segnalazioni provenienti da banche e Forze di polizia su transazioni sospette che avvengono in Rete, in modo da poter analizzare e condividere in tempo reale ogni informazione e bloccare così le operazioni illegali. "Eu-of2cen" (European Union Online Fraud Cyber Centre Expert Network) è il progetto ideato dalla Polizia di Stato, gestito dalla Polizia postale e delle comunicazioni, e finanziato dall'Unione europea per il contrasto al cybercrime finanziario. (https://www.poliziadistato.it)
OPSEC (Operation Security)	Processo mediante il quale, durante un'operazione di intelligence, si previene l'esposizione involontaria di informazioni sensibili/riservate/classificate riguardanti le proprie attività, intenzioni o capacità.
Oracoli	Fonti esterne (API di un sito, output di un oggetto IoT…) alla ***blockchain*** per alimentare uno smart contract e scatenarne o influenzarne l'esecuzione.
OSINT (Open Source INTelligence)	Attività di intelligence tramite la consultazione di fonti aperte di pubblico accesso.

OT (Operation Technology)	Componenti hardware e software dedicati al monitoraggio ed alla gestione di asset fisici in ambito industriale, trasporti…
Payload	Letteralmente carico utile. Nell'ambito della sicurezza informatica è la parte di un ***malware*** che arreca danni.
Password hard-coded	Password inserite direttamente nel codice del software.
Pharming	Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.
PHI (Protected Health Information)	Informazioni personali relative alla salute fisica o mentale di una persona fisica, comprese le relative valutazioni, cure… ed i relativi pagamenti, indipendentemente dalla forma o dal media utilizzato per la loro rappresentazione.
Phishing	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.
Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Ping flood	Attacco basato sul continuo ping dell'indirizzo della macchina vittima. Se migliaia e migliaia di computer, che fanno parte di una ***botnet***, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.
Ping of Death	Attacco basato sull'inoltro di un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.
PIR (Priority Intelligence Requirements)	Requisiti informativi che orientano le priorità nella pianificazione delle attività di intelligence.

© Clusit 2026

Plausible Deniability	Capacità di un soggetto, in genere in posizione gerarchica elevata, di negare di essere a conoscenza di azioni dannose commesse da soggetti di livello più basso, in assenza di prove che possano dimostrare il contrario.
Poisoning	Nell'ambito delle applicazioni di IA attacco che consiste nel contaminare i dati di addestramento per impedire al sistema di funzionare correttamente.
Port Sweeping	Scansione di vari sistemi alla ricerca di una specifica porta in ascolto.
Pretexting	Tecnica di ingegneria sociale nella quale l'attaccante usa una storia inventata, ad esempio una carta di credito bloccata, per carpire la fiducia della vittima e manipolarla fino a farle condividere informazioni sensibili, scaricare malware, inviare denaro a criminali o arrecare danni alla propria organizzazione.
Prompt Injection	Input apparentemente legittimi che possono contenere istruzioni malevole in grado di alterare il comportamento del sistema, aggirare le direttive originali o indurre la divulgazione.
PSYOPs (Psychological Operations)	"Operazioni psicologiche" consistenti nel far giungere a comunità, organizzazioni e soggetti stranieri informazioni selezionate al fine di orientarne a proprio vantaggio opinioni e comportamenti. *(Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi* - www.sicurezzanazionale.gov.it*)*
Pulse Wave (o Hit & Run)	*Hit & Run (o Pulse wave)*
QKD (Quatum Key Distribution)	Tecnologia che utilizza i principi della meccanica quantistica per creare canali di comunicazione sicuri; permettendo di condividere chiavi crittografiche con totale sicurezza, poiché qualsiasi tentativo di intercettazione verrebbe immediatamente rilevato.
QTSP (Qualified Trust Service Provider)	Un ***prestatore di servizi fiduciari*** che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato.

Quishing/QRishing	Tecnica di attacco che utilizza QR code malevoli per indurre le vittime a visitare siti web fraudolenti o scaricare malware.
RDP (Remote Desktop Protocol)	Protocollo per la comunicazione remota fra computer (in particolare per le comunicazioni tra Terminal Server e il client Terminal Server).
Regolamento Macchine (UE 2023/1230)	Regolamento che sostituisce la procedente direttiva, introducendo anche requisiti di sicurezza informatica per le macchine.
Resilienza	"La capacità di un'organizzazione di assorbire gli shock e di adattarsi ad un contesto in continua evoluzione". *Definizione da* ISO 22316:2017
Resource ransom	Tecnica di attacco che nel mondo cloud consiste nel tentare di bloccare l'accesso a risorse nel cloud compromettendo l'account cloud pubblico della vittima e tentando di cifrare o limitare in altro modo l'accesso al maggior numero possibile di risorse cloud.
Responsible AI	L'insieme di pratiche che garantiscono il comportamento etico e controllabile del sistema di AI. Include la capacità di operare in modo equo, evitando bias algoritmici, e di fornire spiegazioni comprensibili delle decisioni (explainability). Il controllo umano e l'accountability sono elementi centrali.
Retrieving data	Fase di ricerca e raccolta dei dati relativi all'obiettivo individuato durante un'attività OSINT. In questa fase gli analisti sfruttano i motori di ricerca, scandagliano i siti web alla ricerca di documenti di interesse avendo cura di conservare ogni traccia raccolta come ad esempio testi, URL, video, immagini, documenti, etc.
Rootkit	***Malware*** che consente sia il controllo occulto di un dispositivo, sia di nascondere la presenza propria e di altri malware.
SASE (Secure Access Service Edge)	Approccio alla sicurezza attraverso il modello Zero-Trust, dove ogni accesso è rigorosamente controllato per garantire che solo utenti e dispositivi autorizzati possano accedere alle risorse aziendali.

© Clusit 2026

SAST (Static Application Security Testing)	Analisi statica del codice finalizzata alla individuazione di vulnerabilità.
SBOM (Software Bill of Materials)	Inventario "nested" di tutti i prodotti software e relativi componenti e fornitori presenti all'interno dell'azienda.
Scrubbing center	Letteralmente centro di pulizia. In uno Scrubbing center il traffico di rete viene analizzato e "ripulito" delle componenti dannose.
Self-sovereign Identity	Modello di identità digitale dove la gestione dei dati non è affidata a provider esterni o Identity Provider, ma lascia agli utenti il pieno controllo sui propri dati.
Service Abuse	Tecniche di attacco in ambito VOIP in cui si utilizza l'infrastruttura della rete VOIP della vittima per generare traffico verso numerazioni particolari a tariffazione speciale.
Shadow AI	Uso non governato di strumenti e modelli di intelligenza artificiale da parte degli utenti, che può esporre dati sensibili e introdurre vulnerabilità senza controlli adeguati.
Side-channel attacks	Tecnica di attacco nella quale l'attaccante tenta di posizionare una macchina virtuale sullo stesso server fisico della potenziale vittima.
SIEM (Security information & event management)	Sistema per la raccolta e normalizzazione dei log e per la correlazione degli eventi finalizzato al monitoraggio della sicurezza.
SIGINT (SIGnals INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza originate da segnali e/o emissioni elettromagnetiche provenienti dall'estero. Le principali branche della SIGINT sono la COMINT e la ELINT. *(Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)*
Sinkhole	Tecnica per reindirizzare il traffico di rete verso uno specifico server al fine, ad esempio, di analizzarlo.

SMB (Server Message Block)	Protocollo per la condivisione di file e stampanti nelle reti locali. Se esposto su internet può essere utilizzato per accedere a documenti e file condivisi.
Smoking Guns	Termine che indica una prova (quasi) certa dell'aver commesso un crimine.
SOAR (Security Orchestration Automation and Response)	Approccio che consente di orchestrare le tecnologie di sicurezza al fine di avere una gestione il più possibile automatizzata della raccolta, analisi e risposta agli eventi di sicurezza.
SOC (Security Operations Center)	Centro la gestione delle funzionalità di sicurezza e per il monitoraggio degli eventi che potrebbero essere una fonte di minaccia.
Social Threats	Versione VOIP del furto d'identità finalizzata a impersonare un utente e perpetrare azioni malevole con lo scopo di arrecare danni; ad esempio, furto di informazioni aziendali riservate.
SOCMINT (Social Media Intelligence)	Ramo dell'Open Source Intelligence specificatamente dedicato alla raccolta di informazione attraverso i social network.
SOP (Standard Operating Procedure)	Procedure operative standard che indicano i passi da seguire durante la conduzione di indagini ***OSINT***, consentendo di rendere efficiente l'esecuzione di operazioni ripetitive e di ottenere uniformità nelle prestazioni, nella qualità degli output ed evitando il mancato rispetto di standard e normative di settore, eventualmente imposte dalla propria organizzazione.
Spear phishing	***Phishing*** mirato verso specifici soggetti.
Spoofing	Modifica di una informazione, ad esempio l'indirizzo mittente di un pacchetto IP.
Spyware	***Malware*** che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante.
SQL injection	Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.
SL-A (Security Level - Achieved)	Livello di sicurezza effettivamente raggiunto.

© Clusit 2026

SL-T (Security Level-Target)	Livello di sicurezza richiesto.
SSDLC (Secure Software Development Life Cycle)	Programma che indirizza la sicurezza sin dalle prime fasi di progettazione di un'applicazione software e non si conclude con la fase di delivery, ma segue tutto il ciclo di vita dell'applicazione.
SSDP (Simple Service Discovery Protocol)	***Protocollo*** che consente di scoprire e rendere disponibili automaticamente i dispositivi di una rete.
SSH (Secure Shell)	***Protocollo*** cifrato che consente l'interazione remota con apparati di rete o di server permettendone, ad esempio, l'amministrazione.
SSPM (Security Posture Management)	Soluzioni di sicurezza per ambienti SaaS che garantiscono un monitoraggio costante delle impostazioni di sicurezza, delle autorizzazioni degli utenti, delle connessioni esterne…, permettendo alle organizzazioni di individuare e intervenire rapidamente su possibili rischi.
Steganografia	Tecnica che consiste nel nascondere una informazione all'interno di un media (immagine, video, file audio…). Un attacco basato su tale tecnica può nascondere, ad esempio, un malware all'interno di file multimediali.
STIX (Structured Threat Information eXpression)	Linguaggio strutturato che consente la descrizione e condivisione automatizzata di cyber threat intelligence (CTI) fra organizzazioni, utilizzando il protocollo ***TAXII***.
Tampering	An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.
TARA (Threat Analysis Risk Assessment)	Metodologia utile per dettagliare tutti i possibili threat a cui un prodotto può essere soggetto e assegnare un rischio basandosi su parametri, sempre descritti nello standard ISO/SAE 21434, che coprono l'ambito della safety, della privacy dell'utente, dell'impatto economico e dell'impatto sull'operatività del prodotto e del veicolo.

TAXII (Trusted Automated eXchange of Indicator Information)	Protocollo che consente lo scambio (in HTTPS) di CTI (cyber threat intelligence) descritti mediante ***STIX***.
TCP Synflood	Tipo di attacco nel quale tramite pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente) si impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, essendo l'IP destinatario inesistente, lascerà la connessione "semi-aperta". Con un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.
TDM (Time-division multiplexing)	Tecnica che consente la condivisione, da parte di più dispositivi, di un canale di comunicazione per un tempo limitato predefinito.
Tecniche di amplificazione degli attacchi	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Ad esempio nel caso del protocollo ***NTP*** si può amplificare la potenza dell'attacco anche di 600 volte.
Tecniche di riflessione degli attacchi (DRDoS – Distributed Reflection Denial of Service)	La tecnica più diffusa sfrutta host esposti sulla Big Internet come riflettori del traffico a loro indirizzato sfruttando le ***vulnerabilità*** intrinseche ad alcuni protocolli quali ***NTP*** o ***DNS***.
TLP (Traffic Light Protocol)	Protocollo per facilitare la condivisione delle informazioni "sensibili" che definisce il grado di possibile diffusione (red, amber, green, white) stabilito dalla controparte inviante.
TLS (Transport Layer Security)	Protocollo per la comunicazione sicura su reti TCP/IP successivo al SSL (Secure Sockets Layer).
Tradecraft	Combinazione di metodi, capacità e risorse che un attaccante sfrutta nel compimento delle proprie azioni.

© Clusit 2026

TSP (Trust Service provider)	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come ***prestatore di servizi fiduciari qualificato*** o come prestatore di servizi fiduciari non qualificato.
TTE (Time-to-Exploit)	Tempo che intercorre dalla divulgazione pubblica di una vulnerabilità al primo sfruttamento osservato.
UBA (User Behavior Analytics)	Tecnologia atta ad apprendere il "normale" comportamento degli utenti di un sistema informativo mediante l'analisi di rilevanti quantità di dati (log…), e di segnalare successivamente il verificarsi di attività anomale messe in atto dagli stessi.
UDP Flood	Il ***protocollo*** UDP non prevede l'instaurazione di una connessione vera e propria e possiede tempi di trasmissione/risposta estremamente ridotti. Tali condizioni offrono maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.
UEBA (User and Entity Behavior Analytics)	Evoluzione della UBA che estende l'analisi comportamentale anche alle entità non umane (dispositivi, applicazioni, account di servizio) per rilevare deviazioni dalla baseline.
UpnP (Universal Plug and Play)	***Protocollo*** di rete che consente la connessione e condivisione automatica di dispositivi ad una rete.
VNC (Virtual Network Computing)	Strumento di condivisione del desktop da remoto.
Vetting	Il processo di identificazione dei partecipanti ad una ***blockchain***.
VHUMINT (Virtual Human Intelligence)	Estensione al mondo virtuale del concetto di Human Intelligence, cioè di una metodologia investigativa imperniata sulla raccolta di informazioni per mezzo di contatti interpersonali. Attraverso la VHUMINT vi è dunque l'interazione proattiva con gli attori della minaccia al fine di raccogliere informazioni di contesto necessarie a mitigare efficacemente la minaccia.
Vishing	Variante "vocale" del ***phishing***.

Volume Boot Record	Il VBR è una piccola porzione di disco allocata all'inizio di ciascuna partizione che contiene codice per caricare in memoria e avviare il sistema operativo contenuto nella partizione.
Watering Hole	Attacco mirato nel quale viene compromesso un sito web al quale accede normalmente l'utente target dell'attacco.
Weaponization	Modifica di file e documenti per trasformali in vere e proprie armi per colpire i sistemi e gli utenti e per favorire l'installazione di codice malevolo.
Web Injects	Tecnica che consente di mostrare nel browser dell'utente informazioni diverse rispetto a quelle originariamente presenti sul sito consultato.
WEF Quantum Readiness Toolkit	Kit che fornisce cinque principi per aiutare le organizzazioni a prepararsi per l'economia quantistica sicura, valutando la loro prontezza quantistica e identificando le azioni prioritarie.
Whaling	Letteralmente "caccia alla balena"; è un'ulteriore specializzazione dello ***spearphishing*** che consiste nel contattare una persona interna all'azienda spacciandosi per un dirigente della stessa. Di solito si tratta di truffe finanziarie e il bersaglio è l'amministrazione con l'obiettivo di indurre la vittima a eseguire, con l'inganno, un pagamento a beneficio del truffatore.
Wiper	Tipologia di virus che hanno come unico scopo quello di distruggere il sistema target (IT e OT).
XDR (Extended Detection and Response)	Dispositivi che integrano tutte le componenti della soluzione di sicurezza in un'unica piattaforma di individuazione (detection) e risposta agli incidenti (Incident Response) portando l'intelligenza di protezione fino al terminale del dipendente, sia esso un computer o uno smartphone.
XSS (Cross Site Scripting)	Vulnerabilità che sfrutta il limitato controllo nell'input di un form su un sito web mediante l'uso di qualsiasi linguaggio di scripting.
Zero-day attach	Attacco compiuto sfruttando ***vulnerabilità*** non ancora note/risolte.

© Clusit 2026

Zero Trust	Paradigma i cui principi fondamentali sono: si assuma che l'ambiente sia ostile, non si distingua tra utenti interni ed esterni, non si assuma "trust" (da cui il nome), si eroghino applicazioni solo a device e utenti riconosciuti e autenticati, si effettuino analisi dei log e dei comportamenti utente. In pratica occorre trattare tutti gli utenti nello stesso modo, utenti della stessa azienda o esterni, che siano nel perimetro della rete aziendale o meno, che i dati a cui vogliono accedere siano dentro l'azienda o da qualche parte nel cloud.

Gli autori del Rapporto Clusit 2026 - Edizione di ottobre



Mauro Andreolini, è ricercatore universitario presso l›Università di Modena e Reggio Emilia. Svolge ricerca negli ambiti della Sicurezza Informatica (con particolare riferimento all›automazione delle operazioni offensive e difensive) e dei Sistemi Operativi, con oltre 50 pubblicazioni internazionali. È docente titolare degli insegnamenti «Sistemi Operativi» (LT) e «Sviluppo di Software Sicuro» (LM). È responsabile di Ateneo per l›iniziativa CyberChallenge.it.



Antonio Apruzzese, Prefetto, con laurea in Giurisprudenza, è stato Direttore della Polizia Postale e delle Comunicazioni dal 2009 al 2015. Impegnato nel contrasto dei crimini informatici, ha sperimentato innovativi modelli di investigazione portando a definizione un complesso progetto europeo denominato OF2CEN (On-line Fraud Cyber Centre and Expert Network) per la tutela transnazionale di servizi bancari on line impostata su una innovativa partnership pubblico/privato tra primari gruppi bancari e Forze di Polizia specializzate europee. Ha inoltre ricoperto ruoli di rilievo istituzionale nel settore, tra cui quello di rappresentante del Ministero dell'Interno nel Tavolo Tecnico di supporto del CISR (Comitato Interministeriale per la Sicurezza della Repubblica) per la definizione della nuova architettura nazionale in tema di cyber sicurezza. Attualmente svolge attività di consulenza per primarie realtà pubbliche e private tra cui l'Automobile Club d'Italia per la gestione e la sicurezza di interconnessioni tra banche dati istituzionali. È altresì Docente di Criminalità Informatica presso l'Università di Modena e Reggio Emilia, e relatore in numerosi convegni sulle problematiche della sicurezza informatica e dei processi di digitalizzazione, con attività di pubblicazione scientifica. È membro del Collegio dei Probiviri e del Comitato Scientifico del Clusit.



Luca Bechelli, Information & Cyber Security Advisor, è Partner in P4I - Digital360, dove ha contribuito a fondare e gestisce l'area di IT & Cybersecurity Governance. Svolge dal 2000 consulenza per progetti nazionali ed internazionali su tematiche di Security Governance, Risk Management, Data Protection, Privilege Management, Cryptography, Incident Handling, Crisis Management, OT Security, IT Compliance e Application Security. Ha operato, tra gli altri, nei settori delle telecomunicazioni, bancario, assicurativo, difesa, aerospaziale, retail e grande distribuzione, manifacturing, trasporti, navale, sanità, pubblica amministrazione centrale e locale, andando di volta in volta a calare gli standard e le best practice della cybersecurity nell'ambito delle regolamentazioni e delle esigenze operative degli specifici mercati, prima come libero professionista e in collaborazione con grandi firme della consulenza, fino al 2017 con l'attuale impegno in P4I. Svolge attività di ricerca e sviluppo tramite collaborazioni con enti di ricerca e associazioni, nell'ambito delle quali ha svolto docenze per master post-laurea. Ha partecipato alla realizzazione di numerosi studi e pubblicazioni di riferimento per il settore, ed ha contribuito alla stesura di standard, normative e linee guida tecniche in materia di sicurezza delle informazioni. Dal 2007 è membro del Consiglio Direttivo e del Comitato Scientifico del Clusit. Dal 2017 è Senior Advisor presso l'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano, supportando il coordinamento e la redazione di linee guida e pubblicazioni nell'ambito di gruppi di lavoro. Dal 2023 coordina il team per l'elaborazione e la stesura dei dati del Rapporto Clusit.



Giancarlo Butti, ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Referente Regolamento DORA e Inclusion del Comitato Scientifico del CLUSIT.
Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Oltre 200 corsi e seminari tenuti presso ISACA/ AIEA, ORACLE/CLUSIT, ITER, Informa Banca, CONVENIA, CETIF, IKN, Università di Milano, CEFRIEL, Ca Foscari, Università degli Studi Suor Orsola Benincasa, ABI…; già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei. Ha all'attivo oltre 900 articoli e collaborazioni con oltre 40 testate. Ha pubblicato 32 fra libri e white paper alcuni dei quali utilizzati come

testi universitari; ha partecipato alla redazione di 31 opere collettive nell'ambito di ABI LAB, Oracle/CLUSIT Community for Security, Rapporto CLUSIT. Socio e già proboviro di ISACA/AIEA è socio del CLUSIT, di ACFE, di DFA e del BCI e partecipa a numerosi gruppi di lavoro. Ha inoltre acquisito le certificazioni/qualificazioni (LA BS 7799), (LA ISO IEC 27001:2005/2013/2022), (LA ISO 20000-1), (LA ISO 22301), (LA ISO IEC 42001), CRISC, CDPSE, ISM, DPO, DPO UNI 11697:2017, DPO UNI CEI EN 17740:2024, CBCI, AMBCI.



Andrea Cabras, è Cyber Security Manager in Webuild, dove si occupa di governance della sicurezza, compliance normativa e continuità operativa nei grandi progetti infrastrutturali internazionali, con responsabilità su bidding, start-up di commessa e innovazione. Ha oltre dodici anni di esperienza maturata nei settori telco, bancario, energy e oil & gas. È fondatore di Ichnos Security, boutique di consulenza specializzata in cybersecurity, sicurezza fisica e compliance. Lead Auditor ISO/IEC 27001 e ISO/IEC 42001, è membro del Comitato Scientifico Clusit e dell'Advisory Board dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano. Firma contributi su testate giornalistiche nazionali dedicate ai temi cyber e svolge attività di formazione e sensibilizzazione per aziende, università e comitati nazionali.



Georgia Cesarone, è Responsabile Innovazione e Formazione del Centro di Competenza START 4.0. È Consigliere Segretario dell'Ordine degli ingegneri di Genova, Presidente del Club per Tecnologie dell'Informazione CTI Liguria e Vicepresidente FIDA Inform (Federazione Nazionale delle Associazioni Professionali di Information Management). Membro del CdA e Vicepresidente di IIC (Istituto Internazionale delle Comunicazioni). Ingegnere elettronico con un master di secondo livello in Trasferimento tecnologico, imprenditorialità e innovazione nei settori dell'alta tecnologia. È innovation manager riconosciuto dal Ministero dello Sviluppo Economico e Project Manager certificato. Fondatrice di due start-up innovative, con un forte background nell'elettronica hardware e nella gestione di progetti di R&I, negli ultimi anni si è concentrata sull'introduzione delle tecnologie e lo sviluppo delle competenze che abilitano la trasformazione digitale nelle aziende.

© Clusit 2026



Mauro Cicognini, parte del team che ha fondato Rexilience nel 2021, si occupa di ICT dal 1989 e di cybersecurity dal 1996. Ha lavorato in aziende dei servizi e dell'alta tecnologia (software, systems integration, telecomunicazioni, automazione industriale), progettando e gestendo software, servizi e reti ICT in realtà che spaziano dalla multinazionale alla PMI. Le sue aree di responsabilità hanno toccato Europa, Africa, Sud America e Medio Oriente; parla inglese, italiano, spagnolo e francese. Interviene sui media nazionali e di settore, ed ha tenuto sessioni su IoT, sul GDPR, sulla Business Continuity, sulla sicurezza fisica, e così via. La sua attività convegnistica è rivolta sia agli specialisti di settore sia, a livello divulgativo, alle scuole ed alle iniziative civiche. Dal 2019 è docente presso il Cefriel – Politecnico di Milano nell'ambito del Corso di Alta Formazione per DPO. Ha fatto parte del Comitato Direttivo e poi del Comitato Scientifico di Clusit ininterrottamente dal 2006. Si è laureato nel 1995 al Politecnico di Milano in ingegneria elettronica (indirizzo bioingegneria), ed ha conseguito nel 2009 un "Executive Certificate in Management and Leadership" presso il Massachussetts Institute of Technology.



Giorgia Dragoni, Ricercatrice Senior dell'Osservatorio Cybersecurity & Data Protection e Direttrice dell'Osservatorio Digital Identity del Politecnico di Milano, si è laureata nel 2014 in Ingegneria Gestionale al Politecnico di Milano, indirizzo Manufacturing & Management, e nello stesso anno ha iniziato a lavorare negli Osservatori Digital Innovation occupandosi di trasformazione digitale e cybersecurity. Attualmente è ricercatrice sui temi della Cybersecurity & Data Protection e dei Big Data Analytics e dal 2020 è Direttrice dell'Osservatorio Digital Identity. Nel 2022 ha conseguito l'Executive Master in Management presso la Polimi Graduate School of Management. È membro del Comitato Scientifico del Clusit e delle Women for Security.



Cinzia Ercolano, fondatrice e amministratore delegato di Astrea, agenzia nata e cresciuta nel mondo della tecnologia e, in particolare, della Sicurezza Informatica, si occupa del format del Clusit "Security Summit", uno degli eventi di Sicurezza Informatica di riferimento in Italia da oltre 15 anni. Dal 2015 si occupa attivamente della comunicazione del CLUSIT, coordinando le attività di ufficio stampa, social media e relazioni con le aziende. Nel 2020 ha ideato e creato, insieme ad un gruppo di specialiste della cybersecurity, Women For Security, community tutta al femminile, che si pone l'obiettivo di mettere a fattor comune le competenze delle donne in ambito information security. Partecipa a diversi eventi di divulgazione del digitale in generale e della cybersecurity in particolare verso le nuove generazioni, inoltre contribuisce con la community a sostenere le campagne di diffusione delle discipline STEM e delle professioni cyber verso il mondo femminile in particolare e adolescenziale in generale.



Maria Ferrucci, è analista di ricerca presso il CERTFin, il centro di collaborazione del settore finanziario italiano per la prevenzione e la gestione delle minacce informatiche, dove coordina il team che ha curato la redazione del Report Sicurezza e frodi informatiche in banca – Edizione 2026. Nell'ambito della sua attività, partecipa attivamente ad approfondimenti, tavoli e gruppi di lavoro a livello nazionale ed europeo dedicati all'evoluzione delle frodi e truffe digitali e delle principali minacce cyber che interessano il settore finanziario e i sistemi di pagamento. Segue inoltre l'evoluzione del quadro normativo di settore, con particolare attenzione alla prevenzione delle frodi e alla cybersecurity.

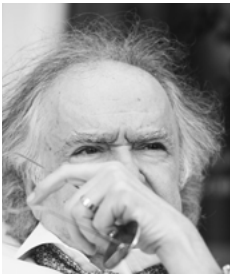


Ivano Gabrielli, laureato in Giurisprudenza e Scienze Politiche con il massimo dei voti, master in Scienze della Sicurezza e master in Homeland Security, è nella Polizia Postale dal 2006. Ha diretto prima il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) e successivamente la III Divisione del Servizio Polizia Postale (CNAIPIC e Cyber-terrorismo). Nel gennaio 2022 è stato nominato Direttore del Servizio Polizia Postale e delle Comunicazioni. Dal luglio 2024, nominato Dirigente Superiore della Polizia di Stato, ha assunto l'incarico di Direttore del Servizio Polizia Postale e per la

sicurezza cibernetica, incardinato nella neoistituita Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, che ha ereditato anche le storiche competenze del Servizio Polizia Postale e delle Comunicazioni.



Paola Girdinio, è professore ordinario di elettrotecnica presso l'Università degli Studi di Genova, è stata preside della facoltà di ingegneria e membro del consiglio di amministrazione di Ateneo. È stata consigliere di amministrazione di Enel, di Ansaldo STS, , del Distretto ligure delle tecnologie marine, di Banca Carige, della società D'Appolonia, di Fondazione Carige, di Banca Popolare di Bari, ricopre attualmente analogo incarico in Ansaldo Energia, Ansaldo Nucleare, in Wsense, in Fondazione Costa Crociere e in Fondazione Amga. È presidente del Centro di Competenza sulla sicurezza e ottimizzazione delle infrastrutture strategiche 4.0 e presidente dell'Osservatorio Nazionale per la Cyber Security, Resilienza e Business Continuity dei Sistemi Elettrici. L'attività di ricerca di Paola Girdinio riguarda i settori della superconduttività applicata, dei materiali dielettrici a basse temperature, del calcolo di campi elettrici e magnetici con metodi numerici e della progettazione assistita da calcolatore di dispositivi elettrici e magnetici, compatibilità elettromagnetica industriale, cybersecurity per le infrastrutture.



Paolo Giudice, è segretario generale del CLUSIT. Negli anni 80 e 90 ha svolto attività di consulenza come esperto di gestione aziendale e rischi finanziari. L'evoluzione del settore IT, che ha messo in evidenza le carenze esistenti in materia di Security, lo ha spinto ad interessarsi alla sicurezza informatica e, nel luglio 2000, con un gruppo di amici, ha fondato il CLUSIT. Dal 2001 al 2008 ha coordinato il Comitato di Programma di Infosecurity Italia e dal 2009 coordina il Comitato Scientifico del Security Summit. Dal 2011 coordina il Comitato di Redazione del Rapporto Clusit. Paolo è Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.



Corrado Giustozzi, membro del Comitato Scientifico di Clusit, è fondatore e senior partner di Rexilience. Già esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale/CERT-AGID (2015-2020) con la responsabilità dello sviluppo del CERT della Pubblica Amministrazione, già membro (mandati 2010-12, 2012-15, 2015-17 e 2017-20) dell'Advisory Board dell'Agenzia dell'Unione Europea per la Cybersecurity (ENISA). In oltre trent'anni di attività come consulente di sicurezza delle informazioni ha condotto importanti progetti di audit ed assessment, e progettato infrastrutture di sicurezza e trust, presso grandi aziende e pubbliche amministrazioni. Ha collaborato per oltre venti anni con il Reparto Indagini Tecniche del ROS Carabinieri nello svolgimento di attività investigative e di contrasto del cybercrime e del cyberterrorismo. Ha partecipato a progetti internazionali di contrasto alla cybercriminalità e al cyberterrorismo con l'Ufficio delle Nazioni Unite per il Controllo della Droga e la Prevenzione del Crimine (UNODC) e l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL). È docente in numerosi Master Universitari. Giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), svolge da sempre un'intensa attività di divulgazione culturale sui problemi tecnici, sociali e legali della sicurezza delle informazioni. Ha al suo attivo oltre mille articoli e quattro libri. L'Università di Roma Tor Vergata gli ha conferito la laurea magistrale honoris causa in Ingegneria di Internet e delle Tecnologie per l'Informazione e la Comunicazione.



Alberto Greco, è Sales Engineering di CrowdStrike per l'Italia. L'inizio in CrowdStrike avviene nel gennaio 2022 con lo scopo di seguire il team dedicato al mercato enterprise e mid-market; il suo ruolo è agire da punto di congiunzione tra le esigenze di business dei clienti e le soluzioni tecnologiche di CrowdStrike: dall'endpoint al cloud, dal mondo identity alla threat intelligence, dall'XDR all'IT Operations. In passato è stato SE Enterprise per l'intero portfolio Palo Alto Networks, SE in Forcepoint con focus sulla network security, technical trainer Fortinet in Exclusive Networks e, prima ancora, network security specialist in Thales Alenia Space. Convinto sostenitore della frase "Se non lo sai spiegare in modo semplice, non l'hai capito abbastanza bene", Alberto è convinto che una diffusione della cultura CyberSec ad ogni livello sia fondamentale per una piena consapevolezza delle problematiche e, ancor più, delle opportunità che ne derivano.

© Clusit 2026



Veronica Leonardi, ha una solida esperienza nella costruzione e valorizzazione di brand nel digitale. È CMO, Board Member e Investor Relations Manager di Cyberoo: tre ruoli che uniscono visione strategica, responsabilità di governance e dialogo con il mercato e gli investitori. Voce e volto di Cyberoo, lavora per portare la cybersecurity fuori dalla "nicchia" rendendola più chiara, più concreta e più vicina alle persone, guidando posizionamento, comunicazione e crescita internazionale dell'azienda.



Mauro Leoncini, è professore ordinario di Informatica presso il Dipartimento di Scienze Fisiche, Informatiche e Matematiche dell'Università di Modena e Reggio Emilia, dove è titolare dell'insegnamento di "Compilatori" per la laurea triennale e di "Algoritmi di crittografia" per la laurea magistrale. I suoi interessi di ricerca vertono nel più ampio settore degli algoritmi per diversi modelli di calcolo e della complessità computazionale. Su questi temi ha pubblicato una quarantina di lavori su rivista internazionale.



Federica Maria Rita Livelli, Consulente in Risk Management & Business Continuity, svolge un'attività di diffusione e sviluppo della cultura della resilienza presso varie istituzioni e università italiane e straniere.
È membro di: CLUSIT – Direttivo; BCI - Cyber Resilience Group; FERMA Digital Committee; Start 4.0 -Italian Working Group for Cyber Resilience & Al of Energetic Grids. Svolge attività di docente di moduli di resilienza presso l'Università di Genova – Master Infrastrutture Critiche, l'Università di Udine -Master di Intelligence & ICT e l'Università di Verona – RiskMaster. Relatrice e moderatrice in diversi seminari, conferenze nazionali ed internazionali, autrice di numerosi articoli e white paper su diverse riviste italiane e straniere. Co-autrice di: Rapporto Clusit - Cyber Security (ed. dal 2020 ad oggi); Libri tematici CLUSIT rif. Intelligenza Artificiale (2020) e Rischio Cyber (2021), Supply Chain Risk (2023); "Lo Stato in Crisi" ed. Angeli (2022); "The ACP book of best practices 3rd edition - Important topics within resilience" (2025); "The ACP book of best practices 4thedition -The Joy of Metrics: Harness the Power of Measurement & Visualization to Enhance Your Organizational Resilience Program"; Revista de Ciencia de la "Revista de Ciencia de la Legislación", pubblicata da IJEditores, Argentina.



Luca Nilo Livrieri, è il Direttore della struttura di Sales Engineering di CrowdStrike per il Sud Europa. L'ingresso in CrowdStrike avviene nel maggio 2021, con la responsabilità di seguire lo sviluppo e la crescita della struttura di prevendita nel Sud Europa e Israele. Partecipa ormai da parecchi anni come relatore a diversi eventi nazionali e internazionali su privacy, AI, sicurezza, cloud e digital transformation fra cui Clusit Security Summit, di cu è anche autore del rapporto, ISMS forum, IDC, Cybersecurity Italy, Tisec e Cybertech. Prima di Crowdstrike, Livrieri è stato manager per l'Italia, la Spagna e il Portogallo della struttura prevendita di Forcepoint. Ha maturato esperienze come membro dell'"Office of the CSO" e Senior SE per il mercato enterprise, e la formazione e affiancamento del canale di rivendita in Websense e Surfcontrol. Prima di svolgere il ruolo di SE ha lavorato come consulente Gfi-Ois per la programmazione web presso alcune importanti aziende italiane. Precedentemente ha conseguito la Laurea magistrale in Comunicazione nella Società dell'Informazione, con tesi specialistica presso il dipartimento di informatica dell'Università Degli Studi Di Torino.



Giovanni Manigrasso, è Innovation Specialist presso Dintec, il Consorzio per l'innovazione tecnologica in house di Unioncamere, delle Camere di Commercio e dell'ENEA. In Dintec supporta l'unità Innovazione e Digitale nel pianificare e coordinare iniziative e progetti sulla Transizione 5.0, in particolare sui temi dell'intelligenza artificiale, della cybersecurity e della maturità digitale delle MPMI, e sui temi dell'innovazione, come la valorizzazione della proprietà intellettuale.



Mirco Marchetti, è Professore Associato presso il Dipartimento di Ingegneria "Enzo Ferrari" dell'Università di Modena e Reggio Emilia, dove insegna "Sicurezza Informatica" e "Automotive Cyber Security". Ha conseguito il Dottorato di Ricerca in Information and Communication Technologies nel 2009 presso la stessa università. I suoi interessi di ricerca includono la Sicurezza informatica per i sistemi cyber-fisici e le interazioni tra Sicurezza informatica e intelligenza artificiale.

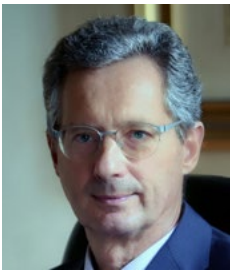
© Clusit 2026



Fabio Martinelli, è Direttore dell'Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) del Consiglio Nazionale delle Ricerche (CNR). I suoi principali interessi di ricerca riguardano la sicurezza e la privacy nei sistemi distribuiti e mobili, nonché i fondamenti di sicurezza, privacy e fiducia (trust). Ha coordinato la rete di eccellenza europea NESSoS (Network of Excellence in Future Internet Security) e la rete di formazione europea sulla sicurezza informatica NeCS (Training Network on Cyber Security) e coordina il progetto europeo SYNAPSE. È stato tra i cinque fondatori dell'European Cyber Security Organization (ECSO) e attualmente ricopre la carica di vicepresidente del Board di ECSO in rappresentanza della accademia e ricerca.



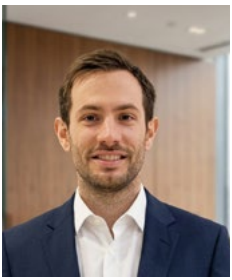
Alessio Misuri, innovation manager presso Dintec e Responsabile dell'unità innovazione e digitale di Dintec scrl, società in house di Unioncamere, è fortemente impegnato nello sviluppo di modelli di valutazione digitale e sistemi di supporto all'orientamento al business anche attraverso tecnologie di intelligenza artificiale. È responsabile per Dintec del team che coordina la rete PID (Punti impresa digitale): la rete delle Camere di commercio per guidare le PMI verso la trasformazione digitale e le tecnologie 4.0.
Dal 2022 inoltre è Professore a contratto di Gestione dell'innovazione tecnologica presso l'università Cattolica.



Giuseppe Molinari, (Modena 1962) ha conseguito la laurea in Ingegneria Meccanica a Bologna nel 1987 e dopo aver lavorato per 5 anni in Ferrari Auto Spa, oggi ricopre la carica di Amministratore Delegato nell'azienda Caffè Molinari spa di cui è socio. Ha assunto nel tempo alcuni incarichi di natura istituzionale: tra il 2009 e il 2018 è stato Consigliere in Confindustria Modena e Confindustria Emilia Romagna, Presidente di Confindustria Servizi Modena. Dal 2018 è Presidente della Camera di Commercio di Modena, dal 2021 Consigliere della Fondazione Casa Natale Enzo Ferrari e dal 2022 è Presidente del Centro Sudi Guglielmo Tagliacarne di Unioncamere.



Alessio L.R. Pennasilico, Information & Cyber Security Advisor, Security Evangelist, noto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto dei temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie. Per questa ragione partecipa da anni come relatore ai più rilevanti eventi di security italiani ed internazionali ed è stato intervistato dalle più prestigiose testate giornalistiche, radio e televisioni nazionali ed internazionali. All'interno di P4I, per importanti Clienti operanti nei più diversi settori di attività, sviluppa progetti mirati alla riduzione dell'impatto del rischio informatico/cyber sul business aziendale, tenendo conto di compliance a norme e standard, della gestione del cambiamento nell'introduzione di nuovi processi ed eventuali tecnologie correlate. Credendo che il cyber risk sia un problema organizzativo e non un mero problema tecnologico, Alessio da anni aiuta il top management, lo staff tecnico e l'organizzazione nel suo complesso a sviluppare la corretta sensibilità in merito al problema, tramite sessioni di awareness, formazione e coaching. Alessio è inoltre membro del Comitato Scientifico di Clusit, membro del Comitato Direttivo di AIP -Associazione Informatici Professionisti, membro del Comitato di Schema UNI 11506 di Kiwa Cermet e Vice Presidente del Comitato di Salvaguardia per l'Imparzialità di LRQA, l'ente di certificazione dei Lloyd's.



Matteo Ranzato, è Principal Engineer presso Oplon Networks, azienda italiana specializzata in cybersecurity e soluzioni per la sicurezza degli accessi. Laureato in Informatica presso l'Università degli Studi di Padova, dal 2019 lavora in Oplon, dove ha maturato una significativa esperienza nello sviluppo e nell'evoluzione di soluzioni per la protezione degli accessi a sistemi, applicazioni e infrastrutture IT. Nel corso della sua esperienza professionale ha approfondito tematiche legate alla cybersecurity, all'access control, alla gestione delle identità e degli accessi e ai moderni modelli di secure access, contribuendo alla progettazione e all'evoluzione tecnologica delle soluzioni Oplon. Nel ruolo di Principal Engineer combina competenze di software engineering e security architecture, con particolare attenzione all'applicazione pratica dei principi di sicurezza in contesti infrastrutturali complessi. Partecipa inoltre ad attività di divulgazione e confronto tecnico sui temi della cybersecurity e della sicurezza degli accessi, contribuendo alla condivisione di esperienze e competenze maturate sul campo.

© Clusit 2026



Antonio Romeo, è dirigente dell'Area Innovazione e Digitale di Unioncamere, dove guida le attività legate alla trasformazione digitale, all'innovazione tecnologica e alla gestione del Registro delle Imprese. Con oltre vent'anni di esperienza nel Sistema Camerale, è attuale direttore in Dintec, coordinando progetti nazionali e internazionali su digitalizzazione, qualità, sostenibilità e normativa tecnica. È coordinatore nazionale della rete PID – Punti Impresa Digitale, che ha contribuito a creare nel 2017, e partecipa a gruppi di lavoro strategici con enti di ricerca come CNR ed ENEA, oltre a organismi nazionali e internazionali quali UNI e ACCREDIA. Esperto nei temi dell'innovazione e della digital transformation, è relatore in numerosi eventi e docente universitario in Economia e Gestione d'Impresa.



Pier Luigi Rotondo, dopo una lunga carriera come Account Technical Leader per IBM Italia S.p.A., adesso ricopre il ruolo di Cyber Advisor nella divisione Cyber & Security Solutions di Leonardo S.p.A. Ha contribuito a molti progetti nazionali e internazionali su soluzioni di Threat Management, Threat Intelligence, Offensive Security, Attack Surface Management, Identity and Access Governance, e Single Sign-on. Con una laurea in Scienze dell'Informazione presso Sapienza Università di Roma, Pier Luigi è coinvolto in attività accademiche su temi di sicurezza delle informazioni in Corsi di Laurea e Master presso l'Università di Roma e di Perugia. Scrive articoli divulgativi, e contribuisce permanentemente dal 2015 al Rapporto Clusit sulla Sicurezza ICT in Italia su temi di cybercrime nel settore finanziario, presentando le tendenze del mercato della cyber security. È stato membro del Comitato Scientifico del CLUSIT dal 2021, ora è membro del Comitato Direttivo.



Leonardo Sartore, diplomato in "Industrial Cyber Security" presso l'ITS Academy Meccatronico Veneto, ricopre il ruolo di Information & Cyber Security Advisor in Partners4Innovation. Affianca quotidianamente diverse realtà nazionali su tematiche di Compliance, Security Governance e Data Protection. Le sue principali aree di competenza comprendono la tutela del patrimonio informativo aziendale e la protezione dei dati personali. Collabora con gli Osservatori del Politecnico di Milano come relatore di webinar su tematiche di Information & Cyber Security.



Sofia Scozzari, appassionata di tecnologia da sempre, ha maturato oltre 15 anni di esperienza nella Cyber Security. Ha lavorato come System Administrator, ICT Consultant, Project Manager, Pre-sale, Cyber Security Consultant e Cyber Security Manager per principali società Italiane e multinazionali. Già CEO e COO di iDIALOGHI, società di consulenza e formazione in ambito Cyber Security, è stata anche co-founder di Security Brokers, cooperativa di Global Cyber Defense & Security Services. Da 4 anni risiede negli Emirati Arabi Uniti dove ha fondato e dirige Hackmanac, con cui elabora dati sulle minacce Cyber a supporto di attività di Threat Intelligence e Risk Management.
È nel Comitato Direttivo di Women For Security, la Community delle Cyber Ladies italiane con cui partecipa ad iniziative a supporto della Cyber Security Awareness, dai corsi di formazione per scuole ed aziende ad eventi di settore. Membro del Comitato Scientifico CLUSIT, fin dalla prima edizione nel 2011 contribuisce come co-autore al Rapporto Clusit, curando l'analisi di migliaia di attacchi informatici ogni anno e diversi approfondimenti verticali. È inoltre autrice di diversi articoli e guide in tema di Cyber Security, e co-autrice dei paper «La Sicurezza dei Social Media» (2014, Oracle Community for Security), e «Blockchain & Distributed Ledger: aspetti di governance, security e compliance» (2019, CLUSIT).



Paolo Spagnoletti, Professore Ordinario di Organizzazione Aziendale presso il Dipartimento di Business e Management della Luiss dove è direttore del corso di laurea in Economia e Management e di master e programmi executive sui temi dell'innovazione e governance del digitale. È presidente di Cyber 4.0 e direttore del laboratorio congiunto Cyber Safe AI Innovation (XAI Lab) Luiss - Cyber 4.0. È autore di oltre 100 lavori sui temi dell'innovazione digitale e della cybersecurity. Ha ricoperto incarichi didattici e di ricerca in Francia, Norvegia, Svizzera, UK e USA.

© Clusit 2026



Claudio Telmon, è membro del Comitato Direttivo del Clusit e Senior Partner - Information & Cyber Security at P4I - Partners4Innovation. Attivo nel campo della sicurezza da più di venti anni, ha gestito il laboratorio di sicurezza del Dipartimento di Informatica dell›Università di Pisa, ed in seguito ha continuato a collaborare con il Dipartimento per attività di didattica e di ricerca, in particolare nel campo della gestione del rischio. Si è occupato come professionista dei diversi aspetti tecnologici e organizzativi della sicurezza, lavorando per aziende del settore finanziario, delle telecomunicazioni e per pubbliche amministrazioni.



Giorgia Tombesi, Project Officer presso Cyber 4.0, si occupa della pianificazione e gestione di progetti di formazione e advisory in ambito cybersecurity, coordinando attività, partner e stakeholder. Ha maturato competenze in cybersecurity, risk management, compliance e project management, con particolare riferimento a standard e framework quali ISO/IEC 27001, NIST e alla normativa europea NIS2. Ha conseguito la certificazione ISO/IEC 27001:2022 Lead Auditor e possiede una formazione specialistica in Cyber Security e Governance, Risk & Compliance (GRC), integrata da conoscenze in ambito data e tecnologie digitali.



Anna Vaccarelli, è Presidente del Clusit. È stata Dirigente Tecnologo al Consiglio Nazionale delle Ricerche (CNR) nell' Istituto di Informatica e Telematica di Pisa. Per quasi 15 anni, a partire dal 1998, si è occupata di ricerca nel settore delle cybersecurity e dal 2010 di divulgazione del digitale in generale e della cybersecurity in particolare. Dal 2004 al 2012 è stata docente del corso di sicurezza informatica al Master congiunto Università di Pisa-Cnr in Tecnologie Internet. Nel 2011 ha ideato e poi coordinato fino al 2024, il progetto di formazione Ludoteca del Registro.it, un'azione di diffusione della cultura di internet nelle scuole, focalizzata soprattutto sulla cybersecurity, incontrando oltre 20.000 studenti. Nel dicembre 2021 ha ricevuto dall'Associazione Informatici Professionisti il premio come miglior informatico dell'anno. Negli anni ha coordinato numerosi progetti di ricerca nazionali e internazionali e scritto oltre 100 pubblicazioni scientifiche e tecniche. Dal 2020 è nel comitato direttivo delle Women For Security e dal 2022 nel comitato direttivo di Clusit.



Artsiom Yautsiukhin è ricercatore presso il Gruppo di Trust, Security and Privacy dell'Istituto di Informatica e Telematica (IIT) del Consiglio Nazionale delle Ricerche (CNR), Italia. Ha conseguito il titolo di Dottore di Ricerca (PhD) in Information and Communication Technology presso l'Università di Trento nel 2009. È coautore di oltre 50 pubblicazioni scientifiche apparse su riviste internazionali, workshop e conferenze, e ha partecipato a numerosi progetti europei, tra cui DUCA, SPARTA, CyberSure e MEDINA. Ha inoltre contribuito a diverse attività europee di definizione di roadmap strategiche nell'ambito di progetti europei (ad esempio Camino, Aegis e SPARTA) e di organizzazioni per la cybersicurezza quali ERCIM ed ECSO. I suoi interessi di ricerca includono i metodi di valutazione della cybersicurezza, le metriche di sicurezza e del rischio, l'assicurazione contro i rischi informatici (cyber insurance) e la certificazione della sicurezza.



Andrea Zapparoli Manzoni, si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. È stato membro dell'Osservatorio per la Sicurezza Nazionale (OSN) nel 2011-12 e del Consiglio Direttivo di Assintel dal 2012 al 2016, coordinandone il GdL Cyber Security. È membro del Comitato Scientifico del Clusit, e Board Advisor del Center for Strategic Cyberspace + Security Science (CSCSS) di Londra. Per oltre 10 anni è stato Presidente de iDialoghi, società milanese dedicata alla formazione ed alla consulenza in ambito ICT Security. Nel gennaio 2015 ha assunto il ruolo di Head of Cyber Security Services della divisione Information Risk Management di KPMG Advisory. Dal giugno 2017 è Managing Director di un centro di ricerca internazionale in materia di Cyber Defense. È spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Fin dalla prima edizione (2011) del "Rapporto Clusit sulla Sicurezza ICT in Italia", si è occupato della sezione relativa all'analisi dei principali attacchi a livello internazionale, ed alle tendenze per il futuro.

© Clusit 2026

Il Clusit, **nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano**, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre **700 organizzazioni**, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare all'elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Le attività e i progetti in corso

- Formazione specialistica: i Webinar Clusit, assieme agli Osservatori del Politecnico di Milano.
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria", arrivato alla 21a edizione.
- Le Conference specialistiche: Security Summit (a Milano, Roma, Napoli, Cagliari e Verona).
- Gli Atelier on line della Security Summit Academy.
- I Security Summit verticali, nei settori: Energia & Utilities; Healthcare; Manufacturing e Finance.
- Gruppi di Lavoro: condotti dalla Clusit Community for Security.
- Rapporti Clusit: rapporti con aggiornamento semestrale sul Cybercrime e ICT Security in Italia, con approfondimenti settoriali.
- Il progetto "SicuraMente Clusit" con attività di formazione nelle scuole italiane.
- Il progetto "SicuraMente Senior" per la sensibilizzazione e la diffusione di competenze in cybersecurity verso le persone Senior.

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e per la Sicurezza Cibernetica, Arma dei Carabinieri e Guardia di Finanza, Agenzia per la Cybersicurezza Nazionale (ACN), Autorità Garante per la tutela dei dati personali, Cyber 4.0 - il Centro di Competenza nazionale ad

alta specializzazione per la cybersecurity, Start 4.0, Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea, ENISA (European Union Agency for Cybersecurity), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

SECURITY SUMMIT

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni. Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'ICT Security.

La partecipazione è libera e gratuita, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione ed organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'ICT.
Certificata dalla folta schiera di **relatori** (**più di 800** sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre **20.000 partecipanti,** e sono stati rilasciati circa **15.000 attestati** validi per l'attribuzione di oltre **48.000 crediti formativi** (CPE).
Nel 2025 i Security Summit sono stati oggetto di oltre **800 articoli e servizi su web, cartaceo, Radio e TV**.

Gli eventi del 2026

Dopo le edizioni in presenza a **Milano** in marzo, a **Napoli** in maggio, a **Roma** in giugno, ancora a Milano con la prima edizione del **Security Summit OT** in settembre, il Security Summit si sposta il 28 ottobre a **Verona** e il 18 novembre con il verticale **Energy & Utilities 2026**, presso la sede di SNAM a Milano.

L'edizione 2027

Inizierà con la tappa di **Milano** dal 16 al 18 marzo, cui seguiranno quelle di **Cagliari** in maggio, di **Roma** in giugno e ancora a Milano in giugno con il **Security Summit OT**. Nella seconda parte dell'anno è prevista una tappa a **Napoli** in settembre e a **Verona** il 27 ottobre, oltre ad alcuni verticali.

Sono inoltre in programma alcune edizioni InHouse del Security Summit, in cui il format viene proposto e declinato su una specifica realtà aziendale.

Informazioni

- Agenda e contenuti: info@clusit.it, +39 349 7768 882
- Altre informazioni: info@astrea.pro
- Informazioni per la stampa: press@securitysummit.it
- Sito web: www.securitysummit.it/

In collaborazione con

CROWDSTRIKE

oplon

SECURITY SUMMIT

www.securitysummit.it