OAD
Osservatorio
Attacchi Digitali
in Italia

Rapporto OAD 2026

Marco R. A. Bozzetti

In collaborazione con

AICA | FIDA INFORM | | POLIZIA POSTALE T@

Partner

QINTESI

Prefazioni di:

Massimo Di Virgilio, Presidente FIDAInform
Ivano Gabrielli, Direttore Servizio Polizia Postale e per la Sicurezza Cibernetica
Antonio Piva, Presidente AICA

Ringraziamenti

Si ringraziano tutte le persone che hanno compilato il questionario online ed i Patrocinatori che hanno aiutato a promuovere la compilazione del questionario e contribuiranno alla diffusione del presente Rapporto OAD 2026.

Uno speciale ringraziamento agli estensori delle tre prefazioni al Rapporto:

- al dott. Massimo Di Virgilio, Presidente FIDAInform
- al dott. Ivano Gabrielli, Direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica
- al dott. Antonio Piva, Presidente AICA.

Un grazie particolare al Partner Qintesi e alle persone che hanno collaborato in vario modo alla realizzazione del questionario on line e del rapporto finale:

- la dott.ssa Carmen Genovese di AICA
- per il Servizio Polizia Postale e per la Sicurezza Cibernetica, che ha fornito dati e testi del Capitolo 8: il Direttore dott. Ivano Gabrielli, l'Ispettore dott. Gaetano Martucci, l'Agente Valeria Pettirossi, l'Assistente Luigi Ummaro.

Utilizzo di strumenti di intelligenza artificiale generativa

Nella predisposizione del Rapporto OAD 2026 è stato utilizzato, quale strumento di supporto, ChatGPT di OpenAI, principalmente per la revisione e il miglioramento dei testi, la verifica della chiarezza espositiva e l'approfondimento di alcuni argomenti. L'elaborazione e l'interpretazione dei dati dell'indagine, le valutazioni e le conclusioni riportate nel Rapporto rimangono sotto la piena responsabilità dell'autore.

Disclaimer - Dichiarazione di non responsabilità

I grafici e i testi del presente Rapporto OAD 2026 sono stati elaborati e redatti con la massima accuratezza possibile, sulla base delle risposte raccolte mediante un questionario online totalmente anonimo e pertanto non verificabili singolarmente.

I risultati dell'indagine forniscono indicazioni sui fenomeni rilevati e sulle relative tendenze, ma non costituiscono stime statisticamente rappresentative dell'intera popolazione delle aziende e degli enti operanti in Italia.

Le informazioni, le analisi e le indicazioni contenute nel Rapporto hanno finalità esclusivamente informative e divulgative e non costituiscono un servizio di consulenza professionale.

L'autore, Marco R. A. Bozzetti, i Partner e i Patrocinatori di OAD 2026 declinano, nei limiti consentiti dalla legge, ogni responsabilità per eventuali perdite o danni derivanti dall'utilizzo delle informazioni, delle analisi e delle indicazioni contenute nel presente Rapporto.

© OAD 2026

Tutti i diritti riservati, salvo quelli espressamente concessi dalla licenza Creative Commons Attribuzione – Non commerciale – Non opere derivate 4.0 Internazionale (CC BY-NC-ND 4.0).

Rapporto OAD 2026 pubblicato il 25 novembre 2026.

Tutti i marchi depositati e i marchi di fabbrica citati nel presente documento sono dei rispettivi titolari.

Studio MRAB Via Savona 26 20144 Milano - tel. 02 72191512 mrab@mrab.it

Rapporto OAD 2026

Osservatorio Attacchi Digitali in Italia

Marco R. A. Bozzetti

Prefazioni di

Massimo Di Virgilio, Presidente FIDAInform

Ivano Gabrielli, Direttore Servizio Polizia Postale e per la Sicurezza Cibernetica

Antonio Piva, Presidente AICA

INDICE Rapporto OAD 2026

Sommario

INDICE Rapporto OAD 2026 4
GUIDA ALLA LETTURA DEL RAPPORTO 7
PREFAZIONI 8
PREFAZIONE del dott. Massimo Di Virgilio 9
PREFAZIONE del dott. Ivano Gabrielli 10
PREFAZIONE del dott. Antonio Piva 11
1 Sintesi Direzionale 12
1bis Executive Summary 15
2. L'indagine OAD 18
2.1 OAD 2026: dall'indagine annuale a un ecosistema collaborativo 19
2.1.1 La Comunità OAD 20
2.1.2 OAD Insight 21
2.1.3 Il Gruppo OAD su LinkedIn 21
2.1.4 Enti collaboratori, partner e patrocinatori 21
2.2 Il Questionario OAD 2026 21
2.2.1 Struttura del questionario OAD 2026 22
2.2.2 Anonimato del Questionario OAD 2026 22
3. Il quadro generale dei rischi e degli attacchi digitali intenzionali 24
3.1 Il quadro a livello internazionale 25
3.1.1 I principali attacchi digitali a livello mondiale nel 2025 e nel 1° quadrimestre 2026 28
3.2 Il quadro a livello Unione Europea (ENISA) 33
3.3 Il quadro a livello italiano 41
3.3.1 Il confronto dei dati CSIRT Italia-ACN con quelli del CNAIPIC del Servizio Polizia Postale e per la Sicurezza Cibernetica 43
4. Gli attacchi digitali in Italia dall'indagine OAD 2026 45
4.1 La tendenza negli anni degli attacchi digitali in Italia dalle indagini OAD 47
4.2 Tipologie e tecniche di attacco emerse da OAD 2026 48
5. Tipologie di attacchi digitali e tecniche di attacco più temute nel prossimo futuro 54
6. Il campione delle organizzazioni rispondenti e dei loro Sistemi Informativi emerso dall'indagine OAD 2026 58
6.1 L'Azienda/Ente rispondente 58
6.2 Tipologie, ruoli e principali caratteristiche dei Sistemi Informativi delle organizzazioni rispondenti 60
6.2.1 Ruolo della persona rispondente 67
7. Le misure di sicurezza in essere nei Sistemi Informativi dei rispondenti 69
7.1 Le misure organizzative per la sicurezza digitale in essere nelle aziende/enti rispondenti 70
7.2 Le misure tecniche 79

7.2.1 Inventario e controllo risorse ICT 80
7.2.2 Accessi e protezione account 82
7.2.3 Patch, anti-malware, anti-virus, EDR, protezione endpoint 83
7.2.4 Rete, firewall, accessi remoti 85
7.2.5 Backup e continuità operativa 87
7.2.6 Monitoraggio della sicurezza digitale e gestione Log 90
7.2.7 Gestione vulnerabilità e incidenti 91
8. I dati dal Servizio Polizia Postale e per la Sicurezza Cibernetica 94
PREMESSA 100
CENTRO NAZIONALE ANTICRIMINE INFORMATICO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE (C.N.A.I.P.I.C.) – COMPUTER CRIME 105
CENTRO NAZIONALE PER IL CONTRASTO DELLA PEDOPORNOGRAFIA ON-LINE (C.N.C.P.O.) 105
IL COMMISSARIATO DI P.S. ONLINE 105
PREVENZIONE CYBERTERRORISMO 106
LE FRODI INFORMATICHE 106
LE TRUFFE ONLINE 106
REATI CONTRO LA PERSONA 106
DATI STATISTICI PUBBLICABILI - PRIMO SEMESTRE 2026 (1° gen - 30 giu 2026) *(Dati Dossier Viminale 2026)* 107
ALLEGATI 108
ALLEGATO A - Aspetti metodologici dell'indagine OAD 2026 109
A.1 La tassonomia degli attacchi digitali per OAD 2026 111
A.2 La macro-valutazione qualitativa del livello di sicurezza digitale del sistema informatico oggetto delle risposte al questionario 115
ALLEGATO B - Mini Glossario essenziale 117
ALLEGATO C - Principali fonti e riferimenti 124
C.1 Dall'OCI all'OAI e a OAD: un po' di storia della sicurezza digitale in Italia 125
C.2 Le principali fonti sugli attacchi, i rischi ICT e le vulnerabilità ICT 126
ALLEGATO D - Il profilo dell'autore Marco R. A. Bozzetti 127
ALLEGATO E - Collaborazioni istituzionali 130
E.1 AICA 131
E.2 FIDAInform 132
E.3 Servizio Polizia Postale e per la Sicurezza Cibernetica 133
ALLEGATO F - Profilo Partner 134
Gruppo Qintesi 135
ALLEGATO G - Profili Patrocinatori 138
ALLEGATO H - Studio MRAB 142

GUIDA ALLA LETTURA DEL RAPPORTO

A partire dall'edizione 2026, il Rapporto OAD introduce una nuova modalità di rappresentazione grafica di alcuni contenuti, finalizzata a facilitare la lettura, la consultazione e l'individuazione delle informazioni di particolare rilevanza.

Considerata l'ampiezza e l'articolazione delle tematiche trattate, nonché la varietà dei destinatari del Rapporto, si è ritenuto opportuno introdurre specifici riquadri, contraddistinti da icone e colori differenti, per richiamare l'attenzione del lettore su determinati contenuti.

🔍 **Approfondimenti**, con sfondo verde chiaro

Informazioni integrative, chiarimenti concettuali, tecnici o normativi ed elementi di contesto utili a una migliore comprensione delle tematiche trattate.

⚠ **Criticità**, con sfondo rosso chiaro

Aspetti particolarmente rilevanti o critici, problematiche emergenti, potenziali rischi e considerazioni che meritano una specifica attenzione da parte del lettore.

📈 **Dati e statistiche di particolare rilevanza**, con sfondo azzurro chiaro

Evidenze quantitative, risultati significativi dell'indagine OAD, confronti statistici e tendenze ritenuti di particolare interesse ai fini della comprensione dell'evoluzione degli attacchi digitali e delle misure di sicurezza adottate.

Questa impostazione editoriale intende favorire differenti livelli di lettura del Rapporto, consentendo sia un'analisi sistematica e approfondita dei contenuti sia una consultazione più rapida e mirata delle principali evidenze emerse.

PREFAZIONI

PREFAZIONE del dott. Massimo Di Virgilio



Il Rapporto OAD 2026 è arrivato alla diciannovesima edizione di una 'storia' che inizia ed è continuata grazie alla passione, alla competenza e all'impegno che l'ing. Marco Bozzetti ha profuso nel tempo nelle sue diverse vesti professionali. Ne è destinatario il composito mondo delle organizzazioni pubbliche e private del Paese. Il suo apporto, da profondo conoscitore sia dell'informatica che della cybersecurity, è molto ricco, non solo di dati, ma anche di elementi di riflessione, utili per monitorare e comprendere gli effetti che le tecnologie digitali producono nei gangli vitali della nostra società. Fa il suo lavoro con grande determinazione, sapendo che ci si trova in «…una burrasca, semplicemente una burrasca», 1) come scriveva il prof. Asor Rosa, per ricordare J.Conrad e per sottolineare le implicazioni che un "Tifone" porta con sé, rimarcando che chi conduce una nave "non rifiuta il suggerimento di un cambio di rotta, ma prepara il proprio equipaggio all'uragano". 2) Un tifone che il rapporto OAD 2026 suggerisce di tenere nel debito conto, provando ad aprire un dialogo, in primis, con le Istituzioni impegnate in prima linea nel fronteggiare i tanti uragani in atto, a protezione del Paese; e naturalmente con l'arcipelago delle aziende, nelle loro variegate articolazioni, giustamente schierate a difesa della libertà d'impresa, con le tante associazioni attive a sostegno delle categorie rappresentate, e con le persone molto interessate ma troppo parcellizzate per tutelare efficacemente i sacri diritti democratici di cittadinanza. Di fronte a ondate di attacchi capaci di sprigionare energie smisurate, la domanda da porsi è: possiamo rimanere in questa configurazione, o è il caso di dar vita finalmente a una concertazione tra le tante disparate forze per coordinare azioni "collaborative", unica strategia capace, a nostro avviso, di contrastare offensive sempre più numerose, invadenti, invasive e pericolose? I fatti stanno inoppugnabilmente dimostrando che molti 'equipaggi' sono in difficoltà: dal dodici novembre scorso, e nelle ore e nei giorni successivi, "prima Microsoft con Outlook e gli altri servizi out per 24 ore, poi il blocco dei voli, poi ancora una rete riservata della NSA, l'agenzia di intelligence americana, e il down di diversi servizi di Apple". 3) A queste si aggiungono miriadi di incursioni a danno delle principali strutture critiche anche con la spregiudicata messa in campo di stuoli di soggetti assoldati nell'ambito di una "gig economy" del sabotaggio. La domanda è: abbiamo a che fare con un "bugmageddon, una sorta di Apocalisse dei bug", 4) capace di provocare un collasso della quotidianità? Il Rapporto OAD giunge puntuale, sintonizzandosi proprio su queste frequenze, ben sapendo che avendo a che fare con sistemi complessi, bisogna prestare grande attenzione all'insegnamento di una nota studiosa, 5) allorché ci esorta a non guardare solo gli effetti a valle ma a vedere e studiare i flussi a monte. Un ammonimento che impone a tutte le forze di questo Paese di regolarsi di conseguenza, facendosi portatori sani di iniziative complementari informative e formative, soprattutto a supporto delle 'persone', che dovrebbero costituire il vero baricentro. Non a caso, il Papa, il 9 novembre scorso a Buenos Aires, andando alla radice, ha parlato della necessità di "un'economia a misura d'uomo". Il Rapporto OAD esce allo scoperto, proponendo la costruzione di 'Comunità', capaci di collegare esperienze, competenze e culture per massimizzare le capacità di autotutela, non escluse quelle di contrapposizione, attivando processi formativi a largo spettro fondamentali e imprescindibili per assicurare "una maggiore tutela dell'uomo". Come Fidainform, visto che "…il ritmo incalzante imposto dal capitalismo, mirato a rendere sempre più veloce ed efficiente il ciclo produzione-consumo, determinava valori e ritmi che influenzavano ogni aspetto della vita collettiva e individuale…", come scriveva già Calvino, 6) ci candidiamo a fare la nostra parte, contribuendo "pro bono" nella educazione delle persone nell'uso del digitale. Nella convinzione che il miglior antidoto per indirizzare correttamente a monte i 'flussi', cui accennava la nota studiosa prof.ssa Greison, sia un utilizzo più consapevole e competente della sofisticata e manipolatoria moltitudine di strumenti in circolazione. Noi, su questo piano, siamo pronti a fare la nostra parte, come testimonia la creazione nel 2024 di "Comunità Collaborative", coscienti che occorrerà armarsi di tenacia e pazienza per cominciare a vincere la strutturale congenita inerzia di una realtà complessa.

Massimo Di Virgilio

Presidente FIDAInform

PREFAZIONE del dott. Ivano Gabrielli



C'è un dato che, più di altri, racconta il tempo che stiamo vivendo: la distinzione tra spazio fisico e spazio digitale ha ormai valore puramente descrittivo. Le minacce che attraversano la rete non restano confinate alla rete. Colpiscono i dati, le infrastrutture, i servizi. Ma colpiscono anche la fiducia dei cittadini, la continuità delle imprese, la credibilità delle istituzioni. È questa la ragione per cui il Rapporto OAD 2026, giunto alla sua nuova edizione, rappresenta molto più di un esercizio statistico: è uno strumento di lettura della realtà. OAD, con questa indagine annuale, offre da anni un contributo prezioso. Lo fa con rigore metodologico e con una capacità di sintesi che aiuta chi ha responsabilità operative a orientarsi in uno scenario in cui la minaccia cambia più rapidamente di quanto cambino gli strumenti per affrontarla. A OAD va il mio ringraziamento, insieme al riconoscimento per un lavoro che tiene insieme il mondo della ricerca, il settore privato e le istituzioni.

I dati raccolti dal Servizio Polizia Postale e per la Sicurezza Cibernetica nel corso del 2025 restituiscono la misura della sfida. Nel corso dell'anno sono stati investigati 52.590 eventi criminosi. Un numero che, da solo, dice poco. Dietro ogni pratica ci sono persone, imprese, enti locali. Ci sono truffe nel trading online, frodi su piattaforme di e-commerce, campagne sempre più credibili perché sostenute da strumenti di intelligenza artificiale generativa. E ci sono reati che incidono in modo profondo sulla sfera personale delle vittime: la sextortion, la diffusione non consensuale di contenuti intimi, il cyberbullismo. Fenomeni che non si combattono soltanto con l'azione investigativa, ma con una capacità di ascolto e di sostegno che deve accompagnare ogni intervento.

Sul fronte della protezione delle infrastrutture critiche, il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche ha gestito oltre 9.000 eventi informatici di rilevante entità, ha diramato più di 50.000 alert di sicurezza e ha avviato 47 complesse collaborazioni internazionali. Sono numeri che testimoniano un lavoro costante, spesso invisibile, che si svolge nelle sale operative e nei canali di cooperazione con i partner europei e internazionali. È un lavoro che non produce notizie, ma produce sicurezza. Questa capacità di intervento poggia su una struttura diffusa e radicata nel territorio: i 18 Centri Operativi Sicurezza Cibernetica e le 82 Sezioni Operative garantiscono prontezza operativa e supporto qualificato alle realtà locali. È una rete che presidia il territorio giorno per giorno, e che rappresenta una delle peculiarità del nostro modello. Non un modello centralizzato, ma un sistema che tiene insieme specializzazione e prossimità.

Accanto all'attività investigativa, il Commissariato di P.S. Online svolge un ruolo complementare e altrettanto fondamentale. Offre informazione costantemente aggiornata, raccoglie segnalazioni, riduce la distanza tra cittadini e istituzioni. Attraverso questo canale passa una parte significativa delle campagne di prevenzione e sensibilizzazione, strutturate per diffondere una cultura della sicurezza digitale che non può essere delegata alla sola tecnologia.

In un contesto caratterizzato da dinamiche geopolitiche sempre più interconnesse e da un'evoluzione tecnologica rapidissima, l'isolamento non è un'opzione. Nessuna istituzione, nessuna impresa, nessun centro di ricerca può affrontare da solo una minaccia che non conosce confini. Il Rapporto OAD 2026 è, in questa prospettiva, uno strumento di confronto essenziale. Non si limita a fotografare lo stato dell'arte: contribuisce a costruire quella sinergia strategica tra istituzioni, mondo della ricerca e settore privato che rappresenta la nostra difesa sistemica. La sicurezza informatica non è un costo. È un investimento. E la conoscenza è la sua materia prima.

Ivano Gabrielli

Direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica

PREFAZIONE del dott. Antonio Piva



La sicurezza digitale è oggi una condizione essenziale per l'esercizio consapevole della cittadinanza, la competitività delle imprese e l'affidabilità delle istituzioni. In una realtà nella quale la dimensione fisica e quella digitale sono ormai inseparabili, proteggere informazioni, infrastrutture e processi significa tutelare la libertà delle persone, la continuità delle attività economiche e la capacità della società di progettare il proprio futuro.

Il Rapporto OAD 2026, giunto al diciannovesimo anno consecutivo di indagine, rappresenta un prezioso patrimonio di conoscenza per il nostro Paese. La continuità dell'osservazione consente di comprendere l'evoluzione delle minacce e di valutare l'adeguatezza delle nostre risposte. Nel 2025 il CSIRT Italia ha gestito 2.729 eventi cibernetici, in crescita del 38% rispetto all'anno precedente, di cui 615 classificati come incidenti. A livello globale, il *Global Cybersecurity Outlook 2026* del *World Economic Forum* evidenzia come le vulnerabilità legate all'intelligenza artificiale rappresentino il rischio informatico in più rapida crescita per l'87% degli intervistati, mentre ENISA richiama l'attenzione sulla crescente interdipendenza dei sistemi digitali e sui rischi che ne derivano per la sicurezza delle organizzazioni e delle filiere produttive. Di fronte a questo scenario, l'innovazione tecnologica, da sola, non è sufficiente. Alla crescente sofisticazione delle minacce deve corrispondere un investimento altrettanto significativo nella maturità digitale delle persone. Digitalizzazione e maturità digitale, infatti, non coincidono: disporre di tecnologie avanzate non significa necessariamente possedere le competenze per utilizzarle e governarle in sicurezza.

È in questa prospettiva che si colloca la missione di AICA, che dal 1961 promuove la cultura informatica e lo sviluppo, il riconoscimento e la valorizzazione delle competenze digitali. Un impegno che riguarda tanto la diffusione di comportamenti consapevoli e responsabili presso tutti i cittadini quanto la qualificazione delle professionalità chiamate a governare la complessità dei sistemi informativi. La crescente domanda di specialisti ICT impone di poter contare su competenze verificabili, riconosciute e costantemente aggiornate rispetto all'evoluzione tecnologica, normativa e alle esigenze del mercato del lavoro. Attraverso il sistema e-CFplus, basato sull'European e-Competence Framework (UNI EN 16234-1:2020), e le attività di certificazione professionale condotte in conformità alla norma ISO/IEC 17024, con schemi accreditati da Accredia, AICA contribuisce concretamente a rispondere a questa esigenza. La certificazione delle competenze assume così un valore che supera il riconoscimento individuale: è uno strumento di trasparenza per il mercato, di garanzia per le organizzazioni e di fiducia per la collettività.

La consolidata collaborazione con l'Osservatorio OAD è espressione concreta di questo impegno. Anche per l'edizione 2026 AICA ha contribuito alla raccolta dei dati attraverso la propria rete, mettendo a disposizione corsi gratuiti con autovalutazione, dedicati alla cybersecurity e all'intelligenza artificiale, e un'agevolazione sul servizio di autovalutazione delle competenze professionali ICT. L'obiettivo è favorire il passaggio dalla conoscenza dei rischi alla capacità concreta di affrontarli. Accogliamo pertanto con particolare favore l'evoluzione dell'Osservatorio in Comunità OAD, uno spazio indipendente e permanente di confronto, condivisione delle esperienze e crescita reciproca. In un ecosistema interconnesso, nel quale la vulnerabilità di un'organizzazione può rapidamente diventare quella di molte altre, anche la sicurezza deve essere intesa come una responsabilità condivisa.

Nel ringraziare l'ingegner Marco R. A. Bozzetti e quanti contribuiscono alla realizzazione del Rapporto, desidero ribadire la convinzione che anima l'impegno di AICA: la sicurezza digitale non è un traguardo acquisito una volta per tutte, ma un patrimonio collettivo da costruire e rinnovare ogni giorno.

Perché il futuro di una società autenticamente digitale non si misura soltanto dalla potenza delle tecnologie di cui dispone, ma dalla qualità delle competenze, dall'autonomia di giudizio e dal senso di responsabilità delle persone chiamate a governarle.

Antonio Piva

Presidente AICA

1 Sintesi Direzionale

Il Rapporto OAD 2026, Osservatorio Attacchi Digitali in Italia, è al diciannovesimo anno consecutivo di indagini online ed analizza gli attacchi digitali intenzionali rilevati dalle aziende e dagli enti rispondenti nell'intero 2025 e nel primo quadrimestre 2026, le principali caratteristiche dei loro Sistemi Informativi (SI) e delle misure tecniche e organizzative adottate per proteggerli.

L'edizione 2026 si colloca in uno scenario internazionale caratterizzato dall'intensificarsi delle tensioni geopolitiche, dalla crescente dipendenza da infrastrutture e servizi digitali, dall'estensione delle catene di fornitura ICT e dalla rapida diffusione dell'Intelligenza Artificiale (IA), utilizzata sia per potenziare gli attacchi sia per migliorare le capacità di difesa.

All'indagine hanno risposto, compilando il questionario online, centinaia di aziende ed enti operanti in Italia, appartenenti a differenti settori e classi dimensionali, con una significativa presenza di piccole e medie organizzazioni (63,67% dei rispondenti). Questa costituisce una caratteristica distintiva di OAD, che intende coinvolgere anche le piccole e piccolissime realtà, spesso meno considerate nelle principali indagini nazionali e internazionali sulla sicurezza digitale.

Come nelle precedenti edizioni, l'indagine è totalmente anonima e basata sulla partecipazione volontaria. Il bacino dei rispondenti non costituisce pertanto un campione statisticamente rappresentativo dell'universo delle organizzazioni italiane, ma consente di individuare fenomeni ricorrenti, criticità e tendenze significative nell'evoluzione degli attacchi digitali e delle misure di sicurezza adottate.

La persistente insicurezza digitale sistemica

Il primo risultato rilevante di OAD 2026 è la conferma dell'elevata diffusione degli attacchi digitali intenzionali. Nel 2025 circa due terzi delle organizzazioni rispondenti dichiarano di aver rilevato attacchi ai propri Sistemi Informativi, 66,30%, percentuale che sale all'84,02% nel primo quadrimestre 2026. Pur riferendosi a periodi di diversa durata, questi risultati evidenziano l'elevata esposizione agli attacchi delle organizzazioni partecipanti.

L'analisi storica delle indagini OAI/OAD evidenzia come, a partire dal 2020, la percentuale delle organizzazioni che rilevano attacchi sia stabilmente superiore a quella delle organizzazioni che dichiarano di non averne rilevati.

Questi risultati confermano, secondo l'interpretazione dell'autore, una situazione di insicurezza digitale sistemica, nella quale gli attacchi costituiscono una minaccia permanente per le organizzazioni e le misure di sicurezza adottate non sempre riescono a prevenirli o contrastarli efficacemente.

Le principali tendenze emerse da OAD risultano, in linea generale, congruenti con quelle evidenziate da ENISA e ACN, che confermano la crescente complessità degli attacchi e i loro possibili impatti anche sui servizi essenziali e sulle infrastrutture critiche, pur nella diversità delle rispettive metodologie di rilevazione.

L'evoluzione degli attacchi e delle tecniche utilizzate

L'indagine OAD 2026 evidenzia una significativa varietà delle tipologie di attacco rilevate, tra cui l'utilizzo non autorizzato di risorse ICT, le modifiche malevoli ai sistemi e alle applicazioni, il furto di informazioni e gli attacchi a servizi ICT terziarizzati o in cloud.

Un elemento particolarmente importante riguarda “l'utilizzo combinato di più tecniche di attacco”, che risulta la modalità maggiormente rilevata negli attacchi più gravi: 59,09% nel 2025 e 57,14% nel primo quadrimestre 2026.

La crescente sofisticazione degli attacchi rende inoltre più difficile individuare tempestivamente le compromissioni e ricostruire le tecniche effettivamente utilizzate, come suggerisce l'aumento delle risposte che dichiarano di non averle potute identificare.

L'Intelligenza Artificiale, sempre più utilizzata per automatizzare e potenziare gli attacchi, rappresenta lo strumento di attacco maggiormente temuto dai rispondenti per il prossimo futuro (73,74%).

Le minacce geopolitiche e le catene di fornitura digitali

Accanto alle tradizionali motivazioni economiche della criminalità informatica, assumono crescente rilevanza l'hacktivism, lo spionaggio e il sabotaggio digitale, anche in relazione alle tensioni geopolitiche e ai conflitti internazionali.

ENISA evidenzia il peso delle motivazioni ideologiche (57,3% degli incidenti analizzati), frequentemente associate ad attacchi DDoS, Distributed Denial of Service. Anche i rispondenti OAD manifestano crescenti preoccupazioni per le minacce di natura geopolitica, pur continuando a temere soprattutto frodi, ricatti e sabotaggi.

La crescente dipendenza da fornitori ICT e servizi cloud (91,36% dei rispondenti OAD utilizza risorse terziarizzate) aumenta l'esposizione agli attacchi che possono propagarsi lungo le catene di forniture digitali, come confermano anche ENISA e ACN.

Le misure di sicurezza: diffusione e criticità

Tra i rispondenti alle sezioni opzionali sulle misure di sicurezza (47% dei partecipanti), emerge una significativa diffusione di strumenti fondamentali, quali l'autenticazione multifattoriale (82,67%), gli aggiornamenti software periodici (89,19%) e le copie di backup. Anche le principali misure organizzative risultano relativamente diffuse.

Permangono tuttavia criticità nella sistematicità delle attività di formazione, monitoraggio e gestione delle vulnerabilità e degli incidenti. Soltanto il 27,78% dei rispondenti dichiara di effettuare una formazione periodica e obbligatoria sulla sicurezza digitale.

Particolarmente significativa è la differenza tra la disponibilità di strumenti e procedure di sicurezza e la loro effettiva verifica attraverso attività periodiche di controllo, simulazione e prova.

La resilienza e la continuità operativa: una delle maggiori criticità

Uno dei risultati più significativi di OAD 2026 riguarda la capacità delle organizzazioni rispondenti di reagire agli incidenti e ripristinare il funzionamento dei propri Sistemi Informativi.

Sebbene la realizzazione di copie di backup sia ampiamente diffusa (83,56% dei rispondenti alla sezione), soltanto il 37% dichiara di aver effettuato, negli ultimi dodici mesi, prove effettive di ripristino dei sistemi utilizzando tali copie.

Anche la disponibilità di piani di Disaster Recovery e di risorse ICT alternative risulta limitata: soltanto il 32,88% dichiara di disporre di un piano di DR con risorse alternative previste e una percentuale ancora inferiore ne garantisce la copertura completa dei sistemi essenziali. Questo evidenzia una criticità fondamentale: disporre di backup non significa necessariamente essere in grado di ripristinare tempestivamente i sistemi e garantire la continuità delle attività dell'organizzazione.

La crescente complessità dei Sistemi Informativi, il loro ruolo essenziale per il funzionamento delle organizzazioni e la dipendenza da fornitori esterni rendono sempre più importante la capacità di affrontare incidenti anche gravi, limitandone gli impatti e assicurando il ripristino dei servizi.

La resilienza digitale richiede quindi non soltanto misure di prevenzione e protezione, ma anche capacità di rilevazione degli incidenti, ripristino e continuità operativa, supportate da procedure periodicamente verificate. Il loro sviluppo, anche nelle organizzazioni di minori dimensioni, richiede il coinvolgimento diretto dei vertici aziendali nelle decisioni relative a rischi, responsabilità e investimenti.

Il quadro nazionale e il contributo della Polizia Postale

Le informazioni dell'ACN e del Servizio Polizia Postale e per la Sicurezza Cibernetica completano il quadro in Italia delineato da OAD, evidenziando la rilevanza degli attacchi alle infrastrutture critiche e ai servizi essenziali, delle frodi informatiche, delle truffe online e dei reati contro la persona.

Le principali tendenze indicate da ACN e dalla Polizia Postale risultano sostanzialmente congruenti con quelle dell'indagine OAD, pur considerando i differenti ambiti e criteri di rilevazione, che non consentono confronti quantitativi diretti.

L'evoluzione di OAD

Con l'edizione 2026, OAD evolve da indagine annuale a ecosistema collaborativo di informazione, sensibilizzazione e confronto sulla sicurezza digitale.

All'indagine e al Rapporto annuale si affiancano la Comunità OAD, la rubrica periodica OAD Insight e il Gruppo OAD su LinkedIn, per mantenere viva durante tutto l'anno l'attenzione sui rischi digitali e sulle principali misure di prevenzione e contrasto.

L'obiettivo rimane quello perseguito fin dalla nascita dell'Osservatorio: contribuire alla diffusione della cultura della sicurezza digitale in Italia, coinvolgendo specialisti, vertici delle organizzazioni e utenti dei Sistemi Informativi.

1bis Executive Summary

The OAD 2026 Report (Osservatorio Attacchi Digitali in Italia – Observatory of Digital Attacks in Italy) marks the nineteenth consecutive year of online surveys and analyses intentional cyberattacks detected by participating companies and organisations throughout 2025 and the first four months of 2026, the main characteristics of their Information Systems (IS), and of the technical and organisational security measures implemented to protect them.

The 2026 edition is set against an international backdrop characterised by escalating geopolitical tensions, growing dependence on digital infrastructures and services, increasingly interconnected ICT supply chains, and the rapid spread of Artificial Intelligence (AI), which is being used both to enhance cyberattacks and to strengthen defensive capabilities.

The survey collected responses from hundreds of companies and organisations operating in Italy, across different sectors and size categories, with significant participation from small and medium-sized organisations (63.67% of respondents). This is a distinctive feature of OAD, which aims to involve even small and micro-organisations, often underrepresented in major national and international cybersecurity surveys.

As in previous editions, the survey is fully anonymous and based on voluntary participation. The respondents therefore do not constitute a statistically representative sample of all Italian organisations. Nevertheless, the findings provide valuable insights into recurring phenomena, critical issues and significant trends in the evolution of cyberattacks and the security measures adopted.

Persistent Systemic Cyber Insecurity

The first major finding of OAD 2026 is the confirmation of the widespread occurrence of intentional cyberattacks. In 2025, approximately two-thirds of participating organisations reported detecting attacks against their Information Systems (66.30%), a figure that rose to 84.02% in the first four months of 2026. Although these figures refer to periods of different lengths, they highlight the substantial exposure of participating organisations to cyberattacks.

Historical analysis of the OAI/OAD surveys shows that, since 2020, the proportion of organisations detecting cyberattacks has consistently exceeded that of organisations reporting no detected attacks.

According to the author's interpretation, these findings confirm a situation of systemic cyber insecurity, in which cyberattacks represent a persistent threat to organisations and the security measures in place are not always sufficient to prevent or effectively counter them.

Overall, the main trends emerging from OAD are broadly consistent with those highlighted by ENISA and the Italian National Cybersecurity Agency (ACN). Despite differences in their respective data collection methodologies, these sources also confirm the growing complexity of cyberattacks and their potential impact on essential services and critical infrastructures.

The Evolution of Cyberattacks and Attack Techniques

The OAD 2026 survey highlights a wide variety of detected cyberattacks, including unauthorised use of ICT resources, malicious modifications to systems and applications, information theft, and attacks against outsourced or cloud-based ICT services.

One particularly important finding concerns the combined use of multiple attack techniques, which was the most frequently reported approach in the most serious attacks: 59.09% in 2025 and 57.14% in the first four months of 2026.

The increasing sophistication of cyberattacks also makes it more difficult to promptly detect compromises and reconstruct the techniques employed, as suggested by the growing proportion of respondents who were unable to identify them.

Artificial Intelligence, increasingly used to automate and enhance cyberattacks, is the attack-enabling technology most feared by respondents for the near future (73.74%).

Geopolitical Threats and Digital Supply Chains

Alongside the traditional financial motivations of cybercrime, hacktivism, cyberespionage and digital sabotage are becoming increasingly significant, also in connection with geopolitical tensions and international conflicts.

ENISA highlights the importance of ideologically motivated attacks (57.3% of the incidents analysed), frequently associated with Distributed Denial of Service (DDoS) attacks. OAD respondents also express growing concerns about geopolitical cyber threats, while continuing to regard fraud, extortion and sabotage as their main concerns.

Growing dependence on ICT suppliers and cloud services (91.36% of respondents use outsourced ICT resources) increases exposure to attacks that may spread across digital supply chains, as also confirmed by ENISA and ACN.

Security Measures: Adoption and Critical Issues

Among respondents who completed the optional sections on security measures (47% of participants), the survey reveals widespread adoption of fundamental security controls, including multi-factor authentication (82.67%), regular software updates (89.19%) and data backups. Key organisational security measures are also relatively widespread.

However, significant shortcomings remain in the systematic implementation of training, security monitoring, vulnerability management and incident management activities. Only 27.78% of respondents report providing regular and mandatory cybersecurity training.

A particularly significant issue is the gap between the availability of security tools and procedures and their actual effectiveness, as verified through periodic checks, simulations and testing.

Digital Resilience and Business Continuity: A Major Area of Concern

One of the most significant findings of OAD 2026 concerns organisations' ability to respond to incidents and restore the operation of their Information Systems.

Although data backups are widely adopted (83.56% of respondents to the relevant section), only 37% report having carried out actual system recovery tests using those backups during the previous twelve months.

The availability of Disaster Recovery (DR) plans and alternative ICT resources is also limited: only 32.88% report having a DR plan that includes alternative ICT resources, and an even smaller proportion ensure full coverage of essential systems.

This highlights a fundamental weakness: having backups does not necessarily mean being able to restore systems promptly and ensure business continuity.

The increasing complexity of Information Systems, their essential role in organisational operations and dependence on external suppliers make the ability to manage even serious incidents, limit their impact and restore services increasingly important.

Digital resilience therefore requires not only preventive and protective measures, but also incident detection, recovery and business continuity capabilities, supported by regularly tested procedures.

Developing these capabilities, including in smaller organisations, requires the direct involvement of senior management in decisions concerning risks, responsibilities and investments.

The Italian Cybersecurity Landscape and the Contribution of the Postal and Cybersecurity Police

Information provided by ACN and the Italian Postal and Cybersecurity Police Service (Servizio Polizia Postale e per la Sicurezza Cibernetica) complements the picture, in Italy, outlined by OAD, highlighting the significance of attacks against critical infrastructures and essential services, computer fraud, online scams and crimes against individuals.

The main trends are broadly consistent with those identified by the OAD survey, although differences in scope and data collection criteria do not allow direct quantitative comparisons.

The Evolution of OAD

With its 2026 edition, OAD is evolving from an annual survey into a collaborative ecosystem for cybersecurity information, awareness and knowledge sharing.

The annual survey and Report are now complemented by the OAD Community, the periodic OAD Insight series and the OAD LinkedIn Group, helping to maintain year-round attention on cyber risks and the main measures available to prevent and counter cyberattacks.

The objective remains the same as when the Observatory was established: to contribute to the development of a stronger cybersecurity culture in Italy, engaging not only specialists but also organisational leaders, decision-makers and Information System users.

2. L'indagine OAD

OAD, **Osservatorio Attacchi Digitali in Italia**, è un'indagine indipendente condotta online sugli attacchi digitali intenzionali subiti dai Sistemi Informativi di aziende ed enti operanti in Italia e sulle principali misure tecniche e organizzative adottate per prevenirli e contrastarli.

L'indagine è aperta liberamente, in forma anonima, ad aziende ed enti di ogni settore merceologico e dimensione, incluse le Pubbliche Amministrazioni centrali e locali. Possono quindi partecipare sia grandi organizzazioni sia piccole e piccolissime realtà, che costituiscono una componente particolarmente significativa del tessuto economico e organizzativo italiano.

L'approccio adottato da OAD consiste nel coinvolgere ogni anno il maggior numero possibile di rispondenti attraverso un questionario online, diffuso tramite i canali dell'Osservatorio e degli enti che collaborano, patrocinano e sostengono l'iniziativa.

Non viene definito preventivamente un campione statistico fisso e rappresentativo dell'universo delle aziende e degli enti italiani. Il campione emerge quindi progressivamente dalle risposte raccolte e comprende organizzazioni differenti per dimensione, settore di appartenenza e caratteristiche del proprio Sistema Informativo.

Per tale motivo i risultati dell'indagine non hanno una valenza statistica rigorosamente rappresentativa dell'intero universo italiano. La numerosità delle risposte raccolte e la loro distribuzione tra organizzazioni di differenti dimensioni e settori consentono tuttavia di ricavare indicazioni significative sull'evoluzione del fenomeno degli attacchi digitali e sulle misure di sicurezza adottate.

Una caratteristica distintiva di OAD è l'attenzione anche alle piccole e piccolissime organizzazioni, che rappresentano la grande maggioranza delle realtà italiane ma che non sempre trovano adeguata rappresentazione nelle principali indagini nazionali e internazionali sulla sicurezza digitale.

L'obiettivo primario dell'Osservatorio è analizzare, anno dopo anno:

- la diffusione e le principali caratteristiche degli attacchi digitali intenzionali rilevati dalle aziende e dagli enti rispondenti;
- le misure tecniche e organizzative adottate per la sicurezza dei loro Sistemi Informativi;
- l'evoluzione nel tempo dei fenomeni osservati;
- i principali elementi di criticità e le tendenze emergenti.

Accanto alla rilevazione dei fenomeni, OAD persegue inoltre una finalità di **informazione, sensibilizzazione e formazione continua** sui temi della sicurezza digitale. La compilazione del questionario, la lettura del Rapporto annuale e le ulteriori iniziative sviluppate da OAD intendono contribuire alla crescita della consapevolezza sui rischi digitali, non solo tra gli specialisti ICT e cybersecurity, ma anche tra le figure di vertice delle organizzazioni, che tipicamente decidono sugli ambiti ICT, tra gli utenti finali di sistemi ICT, che devono essere consci su come utilizzare questi sistemi ed Internet in maniera sicura.

Chi decide al vertice dell'organizzazione sull'ICT ha un ruolo determinante nell'individuazione delle priorità, nella definizione degli investimenti e nell'assegnazione delle risorse necessarie per migliorare il livello di sicurezza digitale.

Il Rapporto OAD offre un riferimento indipendente ed autorevole per comprendere l'evoluzione degli attacchi digitali e delle relative contromisure in Italia, con particolare attenzione anche alle organizzazioni di minori dimensioni.

Il quadro nazionale viene inoltre contestualizzato rispetto alle principali tendenze internazionali ed europee, facendo riferimento, tra le altre fonti, ai rapporti del **World Economic Forum**, dell'Agenzia dell'Unione Europea per la Cybersicurezza, **ENISA,** e dell'Agenzia per la Cybersicurezza Nazionale, **ACN**.

Il sito **www.oadweb.it** costituisce il punto di riferimento delle iniziative dell'Osservatorio e l'archivio della documentazione prodotta nel corso degli anni, a partire dai Rapporti annuali OAD.

La fig. 2-1 riporta le copertine dei Rapporti pubblicati negli anni.



Fig. 2-1

L'Osservatorio ha una lunga continuità storica. Fino al 2015 l'indagine era denominata **OAI, Osservatorio Attacchi Informatici in Italia**. Dal 2016 la denominazione è stata modificata in **OAD, Osservatorio Attacchi Digitali in Italia**, per sottolineare l'evoluzione del fenomeno e la crescente integrazione tra informatica e telecomunicazioni nell'ambito dei moderni Sistemi Informativi.

2.1 OAD 2026: dall'indagine annuale a un ecosistema collaborativo

OAD 2026 rappresenta il diciannovesimo anno consecutivo di indagini online ed è focalizzata sugli attacchi digitali rilevati nell'intero anno 2025 e nel primo quadrimestre 2026.

Con questa edizione l'Osservatorio compie un'ulteriore evoluzione: OAD non è più soltanto un'indagine annuale, ma diviene un ecosistema collaborativo sulla sicurezza digitale in Italia.

L'indagine e il Rapporto annuale rimangono il nucleo centrale dell'iniziativa, ma sono affiancati da ulteriori strumenti di informazione, confronto e condivisione che operano durante l'intero anno.

L'obiettivo di questa evoluzione è duplice:

- aumentare la partecipazione all'indagine, ampliando progressivamente il bacino delle aziende e degli enti coinvolti;
- rendere OAD uno strumento continuativo di informazione e sensibilizzazione sui principali fenomeni riguardanti gli attacchi e la sicurezza digitale.

Tale impostazione risponde in particolare alle caratteristiche del sistema italiano, costituito prevalentemente da PMI, microimprese e organizzazioni di piccola dimensione, comprese numerose Pubbliche Amministrazioni centrali e locali.

Come sintetizzato nella fig. 2.1-1, l'ecosistema OAD comprende oggi diverse componenti tra loro complementari:

- l'**indagine annuale OAD**;
- il **Rapporto annuale** che ne presenta e analizza i risultati;
- la **Comunità OAD**;
- la rubrica periodica **OAD Insight**;
- il **Gruppo OAD su LinkedIn**.



Fig. 2.1-1

2.1.1 La Comunità OAD

La **Comunità OAD** riunisce professionisti, imprese, enti, associazioni e persone interessate a comprendere meglio i temi della sicurezza digitale e degli attacchi informatici.

La Comunità non è rivolta esclusivamente agli specialisti ICT e cybersecurity, ma anche a chi utilizza, gestisce o deve assumere decisioni riguardanti sistemi e strumenti digitali.

La partecipazione non ha finalità commerciali: attraverso la Comunità OAD non vengono inviate pubblicità né proposte di prodotti, sistemi o servizi.

La Comunità si propone invece come iniziativa indipendente e trasversale rispetto alle singole associazioni e organizzazioni, con l'obiettivo di contribuire alla diffusione di una maggiore cultura della sicurezza digitale.

L'iscrizione consente di ricevere aggiornamenti selezionati sulle attività dell'Osservatorio, sui temi critici della sicurezza digitale e sui principali elementi che emergono progressivamente dall'indagine.

2.1.2 OAD Insight

A partire dal 2026 è stata inoltre sviluppata la rubrica **OAD Insight**, attraverso la quale vengono periodicamente approfonditi, in forma sintetica e divulgativa, specifici temi di particolare interesse o attualità in merito alla sicurezza digitale. Gli Insight hanno lo scopo di mantenere vivo durante tutto l'anno il confronto sui rischi digitali, evidenziando casi concreti, tendenze emergenti, tecniche di attacco e possibili misure di prevenzione e contrasto.

Essi rappresentano quindi un ulteriore strumento per tradurre fenomeni spesso complessi in informazioni più facilmente fruibili anche da parte di un pubblico non strettamente specialistico.

2.1.3 Il Gruppo OAD su LinkedIn

Il **Gruppo OAD su LinkedIn** costituisce lo spazio aperto di confronto e discussione collegato all'Osservatorio.

La Comunità OAD rappresenta quindi principalmente il canale informativo diretto, mentre il Gruppo LinkedIn costituisce uno spazio complementare di confronto, condivisione e discussione sui principali temi riguardanti gli attacchi e la sicurezza digitale.

2.1.4 Enti collaboratori, partner e patrocinatori

La realizzazione e la diffusione dell'indagine OAD sono supportate dalla collaborazione con associazioni, enti e organizzazioni che contribuiscono, con ruoli differenti, alla promozione del questionario, alla diffusione dei risultati e allo sviluppo delle iniziative dell'Osservatorio.

Il loro contributo è particolarmente importante per ampliare il bacino potenziale dei rispondenti e raggiungere organizzazioni appartenenti a settori, territori e dimensioni differenti.

Le collaborazioni istituzionali, i Partner e i Patrocinatori dell'edizione OAD 2026 sono descritti negli specifici Allegati del presente Rapporto.

2.2 Il Questionario OAD 2026

Il **Questionario OAD 2026**, disponibile online e in lingua italiana, è completamente anonimo ed è costituito prevalentemente da domande con risposte predefinite da selezionare.

Rispetto alle precedenti edizioni, il questionario è stato significativamente ridotto e semplificato, con l'obiettivo di abbreviare i tempi di compilazione e ampliare il più possibile il numero delle organizzazioni partecipanti.

Le principali innovazioni introdotte riguardano:

- una forte riduzione del numero complessivo di domande rispetto alle precedenti edizioni;
- la suddivisione del questionario in sezioni tematiche, alcune delle quali opzionali;

- una nuova impostazione grafica responsive, per consentirne una migliore compilazione anche tramite dispositivi mobili;
- l'introduzione di controlli logici sulle risposte, finalizzati a ridurre possibili errori e incongruenze nella compilazione;
- la possibilità, per chi completa anche le sezioni dedicate alle misure di sicurezza, di ottenere al termine della compilazione una **macro-valutazione personalizzata del livello di sicurezza digitale del proprio Sistema Informativo**, accompagnata da un riepilogo delle principali criticità emerse.

Quest'ultima funzionalità trasforma il questionario anche in uno strumento di prima autovalutazione e sensibilizzazione, offrendo a chi risponde un immediato ritorno informativo rispetto alle misure di sicurezza adottate.

2.2.1 Struttura del questionario OAD 2026

Il Questionario OAD 2026 è articolato nelle seguenti principali aree:

- **S1 – Brevi informazioni sull'Azienda/Ente** rispondente, sempre anonime;
- **S2 – Attacchi digitali rilevati nel 2025** e **nel primo quadrimestre 2026**, con riferimento al Sistema Informativo dell'organizzazione;
- **S3 – Attacchi maggiormente temuti nel prossimo futuro**;
- **S4 – Macro-caratteristiche del Sistema Informativo**;
- **S5 – Principali misure tecniche di sicurezza digitale**, tra le quali:
  - inventario delle risorse ICT e architettura di base degli strumenti di sicurezza;
  - protezione degli accessi e degli account;
  - patching, antimalware, antivirus, EDR e protezione degli endpoint;
  - reti, firewall e accessi remoti;
  - backup e continuità operativa;
  - monitoraggio della sicurezza e gestione dei log;
  - gestione delle vulnerabilità e degli incidenti.
- **S6 – Principali misure organizzative per la sicurezza digitale**
- **S7 – Ruolo della/del rispondente**.

Al termine della compilazione, per chi ha completato anche le sezioni relative alle misure tecniche e organizzative, il sistema effettua automaticamente i calcoli necessari per produrre la macro-valutazione complessiva del livello di sicurezza digitale del Sistema Informativo oggetto delle risposte.

La struttura del questionario costituisce anche uno dei riferimenti per l'organizzazione dei successivi capitoli del presente Rapporto, nei quali vengono analizzate separatamente la diffusione degli attacchi, gli attacchi maggiormente temuti, le caratteristiche delle organizzazioni e dei loro Sistemi Informativi e le misure di sicurezza adottate.

2.2.2 Anonimato del Questionario OAD 2026

L'anonimato costituisce fin dalle prime edizioni uno dei principi fondamentali dell'indagine OAD.

Le domande e le relative risposte sono formulate in modo tale da non consentire l'identificazione dell'Azienda/Ente o della persona che compila il questionario.

Non vengono richiesti dati identificativi della/del rispondente né dell'organizzazione di appartenenza; non viene registrato l'indirizzo IP e sulla banca dati delle risposte non viene memorizzata la data di compilazione.

I dati raccolti vengono utilizzati esclusivamente in forma aggregata per la produzione delle analisi, delle tabelle e dei grafici contenuti nel presente Rapporto, senza alcun riferimento alle singole risposte.

L'impostazione del questionario è pertanto finalizzata a consentire alle organizzazioni e ai loro rappresentanti di fornire informazioni sulla propria esperienza in materia di attacchi e sicurezza digitale senza esporre elementi riservati o confidenziali.

La tutela dell'anonimato rappresenta un elemento essenziale anche per favorire risposte il più possibile libere e aderenti alla situazione effettivamente riscontrata nelle organizzazioni partecipanti.

3. Il quadro generale dei rischi e degli attacchi digitali intenzionali

L'indagine OAD si concentra sul contesto italiano, ma l'analisi dei rischi e degli attacchi digitali richiede un inquadramento internazionale, considerate la natura transnazionale delle minacce informatiche e la crescente interdipendenza delle infrastrutture e dei servizi digitali.

Il periodo di riferimento dell'indagine OAD 2026, comprendente l'intero anno 2025 e il primo quadrimestre 2026, è stato caratterizzato da tre fattori principali:

- **L'intensificarsi delle tensioni geopolitiche e dei conflitti internazionali**, che ha favorito la diffusione di operazioni cyber con finalità politiche, militari, economiche e di spionaggio.
- **La crescente dipendenza da grandi operatori tecnologici e infrastrutture digitali globali**, con conseguenti rischi di concentrazione, vulnerabilità delle catene di fornitura e possibili impatti sistemici degli attacchi digitali.
- **La rapida diffusione delle tecnologie emergenti, in particolare dell'Intelligenza Artificiale**, che introduce nuove opportunità di innovazione ma anche ulteriori vulnerabilità, superfici di attacco e strumenti utilizzabili dagli attaccanti.

A questi fattori si aggiungono le tradizionali motivazioni economiche della criminalità informatica, tra cui frodi finanziarie, furti di informazioni e identità digitali, estorsioni mediante ransomware e attacchi finalizzati all'interruzione dei servizi.

Il quadro che emerge conferma come la **sicurezza digitale sia ormai strettamente connessa non soltanto alla protezione tecnologica dei sistemi informativi, ma anche alla resilienza delle organizzazioni, delle infrastrutture critiche e dei sistemi economici nazionali**.

Gli **attori** più critici degli attacchi digitali includono strutture a livello di Stato ed organizzazioni criminali ben organizzate, dotate di elevate capacità tecniche ed economiche, che a livello internazionale svolgono attacchi quasi sempre con obiettivi economici. Talune operano anche per le strutture statali, di fatto contribuendo alle guerre ibridi e digitali (cyber warfare)[1].

Come approfondito nel Capitolo 4, per l'autore, l'Italia è dal 2020 nell'**era della insicurezza digitale sistemica** (**systemic cyber insecurity**), ed anche il 2025 ed il 2026 (primo quadrimestre) confermano questo stato di grave rischio, nel quale le contromisure adottate non sono più sufficienti ed efficaci, e non riescono a contrastare tutti gli attacchi digitali portati. Un ulteriore aspetto critico di questo stato di "perenne insicurezza cibernetica" è dato dalla **crescente gravità degli attacchi**, soprattutto in termini di impatti sul business e sul funzionamento di intere parti del sistema paese.

[1] La cyber warfare, o guerra informatica, o guerra digitale, è definita dalla Enciclopedia Treccani come "*Uso di computer e di reti, come Internet, per attaccare o difendersi nel cyberspazio*". Wikipedia la definisce in modo simile: "*Insieme delle attività di preparazione e conduzione di operazioni di contrasto nello spazio cibernetico*".

3.1 *Il quadro a livello internazionale*

⚠ A livello mondiale Il Global Risk Report[2] del World Economic Forum, WEF, nella sua ultima versione del 2026, sintetizza la gravità dei rischi complessivi, inclusi quelli ICT, per l'intero mondo con una semplice frase: "**nel 2026 il mondo è su un precipizio**".

Innumerevoli i rischi, sempre più gravi ed impattanti, e tra loro in parte correlati, mostrati nella fig. 3.1-1, che includono il confronto-scontro geoeconomico, l'arretramento del multilateralismo, il crescente protezionismo, la ridotta trasparenza e il minor rispetto dello Stato di diritto, la crescente polarizzazione sociale e politica, l'intensificarsi dei rischi economici, i gravi rischi ambientali che stanno perdendo priorità, l'aumento dei rischi tecnologici.

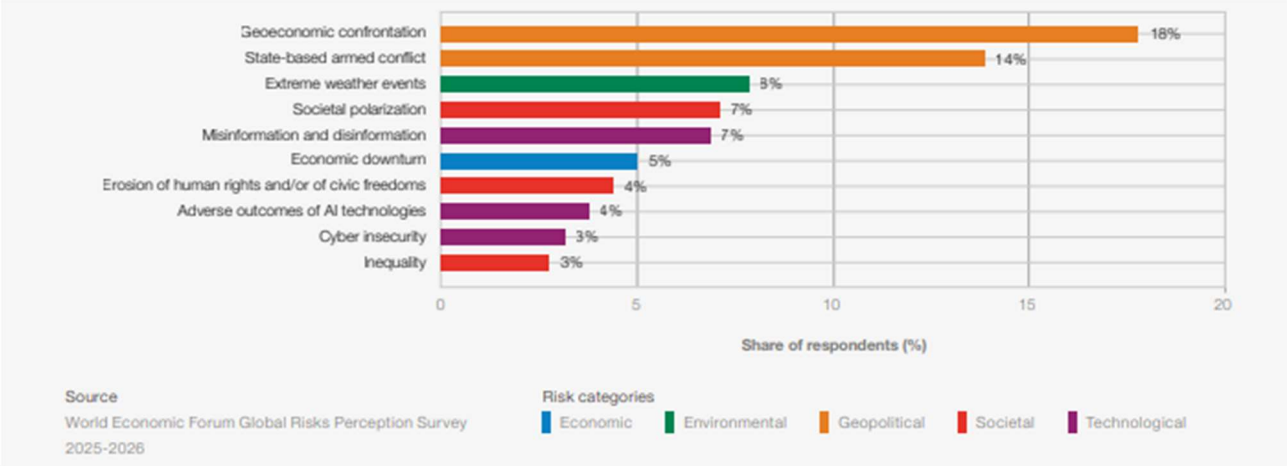


Fig. 3.1-1

⚠ Con particolare riferimento al mondo ICT e della sicurezza digitale, la fig. 3.1-2 mostra che la **malainformazione/disinformazione** è, nel breve termine (2 anni) al secondo posto, e nel lungo termine al quarto. Il rischio **cyber insecurity** a breve termine è al sesto posto, a lungo termine è all'ottavo.

A lungo termine, al quinto posto, il rischio "Adverse outcomes of AI technologies", ossia i possibili esiti e le **conseguenze negative nell'uso dell'intelligenza artificiale** (che nel seguito indicheremo sia con l'acronimo italiano, IA, che con quello inglese, AI, Artificial Intelligence): questo rischio era al sesto posto nella precedente edizione.

[2] Questo rapporto (https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf) è la ventunesima edizione dell'indagine condotta a livello mondiale su circa 1300 leader globali ed esperti del mondo accademico, imprenditoriale, governativo, delle organizzazioni internazionali e della società civile.

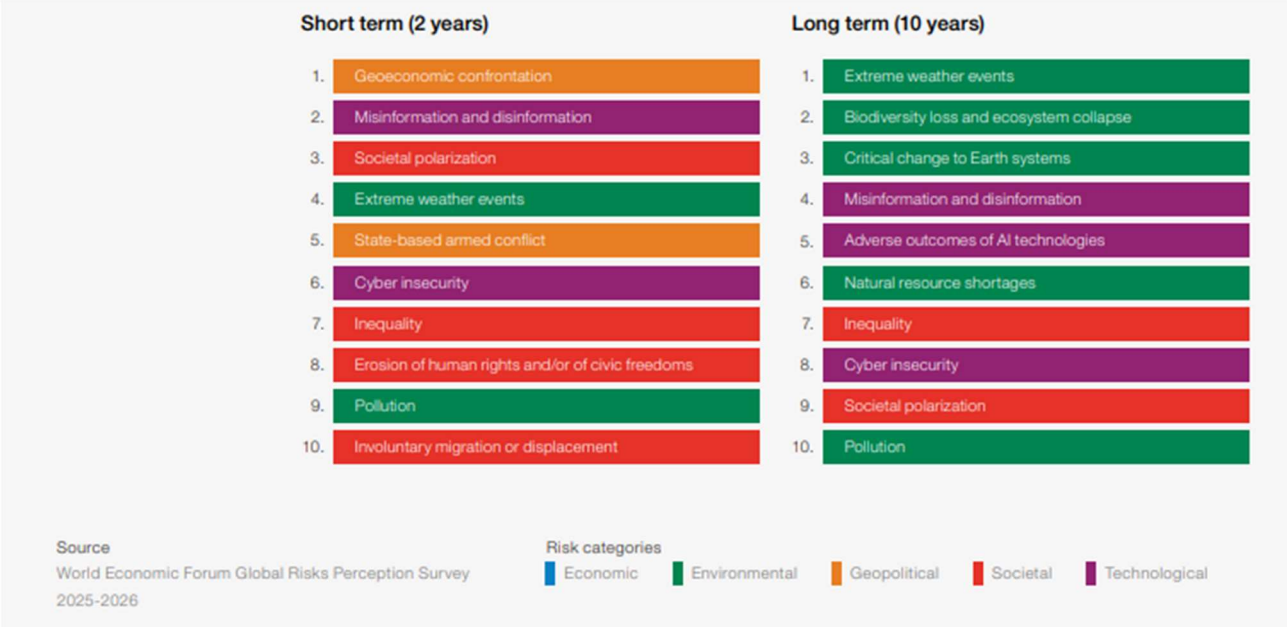


Fig. 3.1-2

Al secondo posto, nel breve termine, si colloca il rischio "**misinformation and disinformation**", che era al primo posto nelle due precedenti edizioni del 2025 e del 2024.

I due termini, che sono spesso considerati sinonimi, hanno significati ben diversi:

- **misinformation**: informazioni false o non corrette, ma generate per errore e non intenzionali. Le prime tre lettere "**mis**" chiariscono il concetto: le informazioni false sono causate da errori ("**mis**take") e da inconsapevolezza che la notizia è falsa. Tipici esempi includono comunicazioni involontariamente inesatte, insulti, scherzi.
- **disinformation**: informazioni deliberatamente e volutamente false o scorrette, non solo hoaxes, e spear phishing, ma soprattutto un certo tipo di propaganda e di pubblicità sui siti web, sui social, via e-mail, su riviste e quotidiani. L'autore della "disinformazione" è perfettamente consapevole della sua falsità o scorrettezza.

Misinformation e disinformation nel lungo termine sono al quarto posto in ordine di criticità, mentre erano al quinto nelle due precedenti edizioni del rapporto WEF. Esse sono un sempre più grave pericolo, soprattutto nell'ambito delle guerre ibride[3], delle tensioni geopolitiche, delle votazioni. Questo rischio spesso evidenzia anche la polarizzazione sociale[4] come uno dei rischi più gravi, al terzo posto nel breve (era al quarto nel 2025) e al nono nel lungo termine (era all'ottavo nel 2025), si veda fig. 3.1-1.

Contenuti di scarsa qualità e mancanza di fiducia nelle fonti di informazione continuano a rappresentare una minaccia per la società.

[3] Guerra ibrida: una guerra che fa uso e mescola elementi della guerra "tradizionale", svolta da militari con armi, con elementi di guerra "non tradizionale", che includono in maniera significativa elementi di economia (restrizione economiche, blocco di merci, etc.), di psicologia, di disinformazione, di guerra digitale (cyber warfare).

[4] La polarizzazione sociale, in inglese "societal polarization", è definita da WEF nel rapporto come "Divisioni ideologiche e culturali presenti o percepite all'interno e tra le comunità, che portano a un declino della stabilità sociale, a blocchi nei processi decisionali, a disordini economici e a una maggiore polarizzazione politica." In termini generali, all'interno di un gruppo sociale, la polarizzazione di gruppo consiste nella tendenza degli individui membri ad assumere sistematicamente e in modo graduale delle posizioni (atteggiamenti) che sono più estreme rispetto alla media delle posizioni iniziali dei restanti membri.

La fig. 3.1-3 mostra la mappa delle interconnessioni tra i vari rischi considerati, e le dimensioni dei singoli nodi rappresentano la gravità del rischio: **misinformation and disinformation** hanno dimensioni tra le più impattanti.

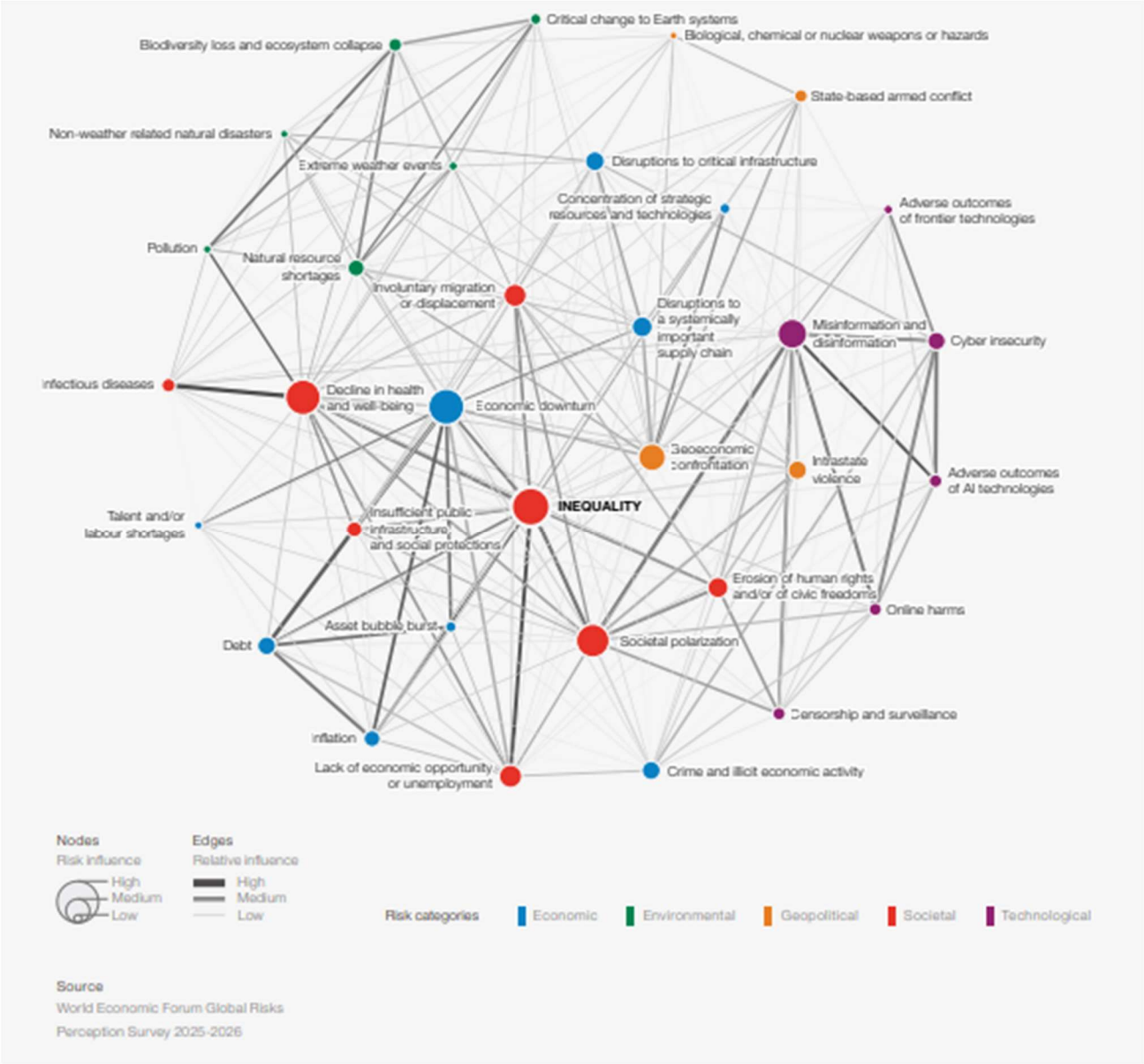


Fig. 3.1-3

Dal Rapporto WEF sulla sicurezza digitale[5] è interessante il confronto, sintetizzato in fig. 3.1-4, tra le opinioni dei CEO e dei CISO intervistati da WEF nel 2026 e nel 2025.

[5] https://www.weforum.org/publications/global-cybersecurity-outlook-2026

Rank	Chief executive officer (CEO)		Chief information security officer (CISO)	
	2025	**2026**	2025	**2026**
1	Ransomware attack	**Cyber-enabled fraud and phishing**	Ransomware attack	**Ransomware attack**
2	Cyber-enabled fraud and phishing	**AI vulnerabilities**	Supply chain disruption	**Supply chain disruption**
3	Supply chain disruption	**Exploitation of software vulnerabilities**	Cyber-enabled fraud and phishing	**Exploitation of software vulnerabilities**

Fig. 3.1-4

Due gli approfondimenti dell'analisi dei rischi WEF sulle tecnologie ICT: il quantum computing e l'intelligenza artificiale.

Per quanto riguarda il quantum computing, due principali rischi:

- i futuri attacchi basati sul calcolo quantistico contro le attuali tecniche di crittografia classiche, che potrebbero compromettere tutte le infrastrutture, e in particolare quelle critiche. Sul tema si veda anche OAD Insight #5 – Crittografia post-quantistica (https://www.oadweb.it/it/comunita-oad/oad-insight/oad-insight-5-crittografia-post-quantistica.html);
- lo scenario geopolitico potrebbe evolvere verso forme estreme di concentrazione del potere economico e imprenditoriale che da un lato potrebbero esacerbare il divario digitale all'interno delle società e tra i diversi Paesi, dall'altro la supremazia in ambito quantistico che garantirebbe enormi vantaggi strategici e tattici nei conflitti; per tale supremazia il rapporto considera soprattutto USA e Cina, che realizzerebbero, e stanno già realizzando, due ecosistemi ciascuno coi propri standard, filiere di produzione e protocolli e con poco o nulla interoperabilità tra loro.

Per **l'Intelligenza Artificiale (IA)**, WEF evidenzia che, nel corso del tempo, la diffusione di sistemi di IA generativa e agentica[6] ha il potenziale di trasformare le economie e, sebbene le opportunità e i benefici siano enormi, vi sono anche rischi che potrebbero manifestarsi rapidamente a causa delle dinamiche di mercato, delle pressioni geopolitiche e della lenta definizione di quadri di governance. Sia le opportunità che i rischi associati all'IA saranno distribuiti in modo disomogeneo. L'IA sta fortemente contribuendo al miglioramento ed al potenziamento da un lato delle tecniche e modalità di attacco digitale, dall'altro delle analisi dei rischi digitali e delle misure di sicurezza digitale. La crescente varietà di applicazioni militari dell'IA comporterà rischi proporzionali, portando, nell'ipotesi peggiore, a un'escalation rapida e forse involontaria dei conflitti non solo digitali (cyber warfare), ma anche sul campo e ibride.

3.1.1 I principali attacchi digitali a livello mondiale nel 2025 e nel 1° quadrimestre 2026

Come "principali" attacchi digitali si intendono quelli che combinano, come gravità ed impatto, danno economico, interruzione operativa, numero di persone/organizzazioni coinvolte, rilevanza sistemica e geopolitica.

La tabella di fig. 3.1.1-1 mostra i principali attacchi (max. 3/mese) occorsi mese per mese nel corso del 2025. La scelta degli attacchi è stata fatta dall'autore, con l'ausilio di specifiche indagini in Internet.

[6] Un sistema di "**IA generativa**" crea contenuti solo su richiesta (in pratica inserendo le proprie domande nel "promt"). Un sistema di "**IA agentica**" non si limita a rispondere a singoli comandi, ma è in grado di agire in modo autonomo per raggiungere obiettivi specifici, pianificando e completando attività complesse passo dopo passo.

L'attacco è attribuito al mese in cui l'incidente è stato rilevato o è divenuto noto all'organizzazione colpita, indipendentemente dalla data, eventualmente precedente, del primo accesso o dell'inizio della compromissione. Se l'attacco produce un evento manifesto prima della formale scoperta, ad esempio ransomware attivato, sistemi bloccati, furto materialmente eseguito, viene considerata la data di quell'evento.

Mese 2025	Organizzazione / attacco	Tipologia	Principali effetti
Gennaio	Catasto della Slovacchia	Cyberattacco a infrastruttura pubblica	Un attacco su larga scala ha reso indisponibili i sistemi catastali nazionali, causando la chiusura temporanea di uffici e l'interruzione di servizi connessi alle transazioni immobiliari.
	NoName057(16) contro istituzioni italiane	DDoS / hacktivism	Il gruppo filorusso ha colpito siti di ministeri, Consob, Carabinieri, Marina, Aeronautica e aziende di trasporto pubblico, causando temporanee indisponibilità dei servizi online.
Febbraio	Bybit	Furto di criptovalute / supply chain	Sottratti asset digitali per circa 1,5 miliardi di dollari. L'FBI ha attribuito l'operazione alla Corea del Nord (TraderTraitor).
	Lee Enterprises	Ransomware / data breach	Gli attaccanti hanno cifrato applicazioni critiche ed esfiltrato file, compromettendo distribuzione dei giornali, fatturazione, incassi e pagamenti ai fornitori.
Marzo	Ukrzaliznytsia – Ferrovie ucraine	Cyberattacco a infrastruttura critica	Un attacco mirato e su larga scala ha interrotto i servizi digitali e la vendita online dei biglietti. Il traffico ferroviario è proseguito, ma il ripristino dei sistemi IT ha richiesto diverse settimane.
	Malaysia Airports Holdings	Cyberattacco / estorsione	I sistemi digitali dell'operatore aeroportuale sono stati colpiti da un attacco accompagnato da una richiesta di riscatto di 10 milioni di dollari, rifiutata dal governo malese.
Aprile	Marks & Spencer	Cyberattacco / disruption operativa	L'incidente ha causato problemi ai pagamenti contactless e ha successivamente imposto la sospensione degli ordini online, con conseguenze rilevanti sull'operatività e sulla logistica.
	SK Telecom	Malware / data breach	Un'intrusione ha compromesso informazioni legate alle SIM dei clienti. L'operatore ha avviato la sostituzione gratuita delle SIM per circa 23 milioni di utenti.
Maggio	Kettering Health	Ransomware	L'attacco del gruppo Interlock ha prodotto un'estesa indisponibilità dei sistemi IT, cancellazione o riprogrammazione di procedure mediche e disservizi ai sistemi di

			comunicazione e alle applicazioni per i pazienti.
Giugno	Nobitex	Cyberattacco geopolitico / crypto	Il principale exchange iraniano di criptovalute ha subito una perdita superiore a 90 milioni di dollari. L'attacco è stato rivendicato dal gruppo filoisraeliano Predatory Sparrow e gran parte dei fondi sarebbe stata deliberatamente resa irrecuperabile.
	WestJet	Intrusione / data breach	Un soggetto criminale sofisticato ha ottenuto accesso non autorizzato ai sistemi della compagnia aerea e sottratto dati.
Luglio	Microsoft SharePoint – ToolShell	Zero-day / exploitation su larga scala	Vulnerabilità critiche di SharePoint Server sono state sfruttate contro numerose organizzazioni pubbliche e private, comprese infrastrutture governative sensibili.
	UNC3886 contro infrastrutture critiche di Singapore	APT / cyberespionage	Singapore ha rilevato una campagna sofisticata e prolungata contro proprie infrastrutture critiche. Le indagini successive hanno accertato che erano stati presi di mira tutti e quattro i principali operatori di telecomunicazioni nazionali.
Agosto	Salesloft Drift / Salesforce	Supply-chain attack / furto di credenziali	La compromissione delle credenziali OAuth dell'integrazione Drift ha consentito l'esfiltrazione di dati da istanze Salesforce di numerose organizzazioni. FINRA ha indicato oltre 700 organizzazioni coinvolte.
	F5	APT / compromissione della supply chain software	Un attore statale non individuato ha mantenuto accesso persistente ai sistemi F5 e sottratto porzioni del codice sorgente BIG-IP e informazioni relative a vulnerabilità non ancora pubbliche.
Settembre	Jaguar Land Rover	Cyberattacco / disruption industriale	L'attacco ha costretto JLR a spegnere i sistemi globali e ha fermato la produzione automobilistica per settimane, con conseguenze rilevanti anche sulla supply chain. La produzione ha iniziato a ripartire gradualmente solo in ottobre.
	Collins Aerospace	Ransomware / supply-chain attack	La compromissione dei sistemi condivisi di check-in e-boarding ha interessato diversi aeroporti europei, fra cui Heathrow, Bruxelles e Berlino, causando ritardi, cancellazioni e ricorso a procedure manuali.
	Asahi Group	Ransomware / disruption industriale	L'attacco del 29 settembre ha sospeso ordini, spedizioni e

			customer service in Giappone e interessato i sistemi produttivi. Le indagini hanno successivamente confermato ransomware ed esfiltrazione di dati.
Ottobre	ASKUL	Ransomware / disruption logistica	Un ransomware del 19 ottobre ha causato una grave interruzione dei sistemi e dei servizi logistici dell'operatore giapponese. Il ripristino completo delle capacità di spedizione si è protratto per diversi mesi.
	Oracle E-Business Suite / Cl0p	Zero-day / estorsione	Una campagna di attacchi ha sfruttato vulnerabilità critiche di Oracle E-Business Suite contro organizzazioni clienti. Oracle ha pubblicato patch di emergenza per vulnerabilità sfruttabili da remoto anche senza autenticazione.
Novembre	Shai-Hulud 2.0	Software supply-chain attack	Un malware autoreplicante ha compromesso l'ecosistema npm: in pochi giorni risultavano coinvolti oltre 700 pacchetti, con rischio di furto di credenziali, token e altri segreti e propagazione automatica ad ulteriori pacchetti.
	Congressional Budget Office (CBO)	APT / cyberespionage	Un attore sofisticato ha ottenuto accesso a circa 29.500 e-mail appartenenti a 22 caselle di posta del CBO statunitense, in una compromissione protrattasi tra luglio e novembre.
Dicembre	La Poste	DDoS	Attacchi DDoS su larga scala hanno provocato disservizi ai servizi online del gruppo francese durante il periodo natalizio. La stessa La Poste ha qualificato l'intensità dell'attacco come senza precedenti, senza evidenze di compromissione dei dati personali.
	Trust Wallet	Software supply-chain / crypto theft	Una compromissione della versione 2.68 dell'estensione browser ha esposto i wallet degli utenti tra il 24 e il 26 dicembre. Trust Wallet ha stimato in circa 7 milioni di dollari gli asset sottratti e ha annunciato il rimborso degli utenti coinvolti.

Fig. 3.1.1-1

La tabella in fig. 3.1.1-2 mostra i principali attacchi (max. 3/mese) occorsi mese per mese nel corso del 1° quadrimestre 2026.Come per la precedente tabella, la scelta degli attacchi è stata fatta dall'autore, con l'ausilio di specifiche indagini in Internet.

Mese 2026	Organizzazione / attacco	Tipologia	Principali effetti
Gennaio	AZ Monica	Cyberattacco / disruption sanitaria	Il 13 gennaio un grave attacco informatico ha costretto l'ospedale belga a disattivare i sistemi dei campus di Anversa e Deurne. Sono stati cancellati circa 70 interventi chirurgici, alcuni pazienti critici sono stati trasferiti e i servizi di emergenza hanno operato a capacità ridotta.
Febbraio	University of Mississippi Medical Center (UMMC)	Ransomware / disruption sanitaria	L'attacco del 19 febbraio ha reso indisponibili numerosi sistemi IT, compresa la piattaforma Epic per le cartelle cliniche elettroniche, determinando la chiusura di tutte le 35 cliniche del network, le cancellazioni di visite e di interventi programmati e il ricorso a procedure manuali.
	Ivanti EPMM – Commissione europea e autorità olandesi	Zero-day / cyberespionage	Vulnerabilità zero-day critiche di Ivanti Endpoint Manager Mobile sono state sfruttate contro diverse organizzazioni, tra cui la Commissione europea, l'Autorità olandese per la protezione dei dati e il Consiglio della magistratura dei Paesi Bassi. La Commissione ha dichiarato di aver contenuto l'intrusione entro nove ore.
Marzo	Stryker	Cyberattacco distruttivo / geopolitica	L'attacco dell'11 marzo ha provocato una disruption globale dell'ambiente Microsoft interno del produttore di dispositivi medicali, con conseguenze sull'elaborazione degli ordini, sulla produzione e sulle spedizioni. L'operazione è stata rivendicata dal gruppo Handala, collegato all'Iran.
	Parlamento albanese	Cyberattacco distruttivo / APT	Il 10 marzo il Parlamento albanese ha segnalato un attacco volto a cancellare dati e compromettere diversi sistemi interni e di posta elettronica. La responsabilità è stata rivendicata da Homeland Justice, gruppo collegato all'Iran.
Aprile	KelpDAO / LayerZero	Supply-chain / crypto theft / attore statale	Il 18 aprile il bridge rsETH di KelpDAO è stato compromesso, con la sottrazione di circa 116.500 rsETH, pari a circa 292 milioni di dollari**.** L'attacco, attribuito a TraderTraitor/UNC4899 della Corea del Nord, aveva avuto origine il 6 marzo attraverso il social engineering di uno sviluppatore.
	ChipSoft	Ransomware / supply-chain sanitaria	Il 7 aprile ChipSoft ha rilevato anomalie nei propri sistemi, successivamente ricondotte a un ransomware. Sono stati temporaneamente disconnessi alcuni servizi utilizzati dalle strutture sanitarie e l'indagine forense ha confermato la sottrazione di dati personali, compresi dati sanitari, relativi a pazienti di alcuni clienti.

Fig. 3.1.2-2

La selezione dei principali attacchi digitali verificatisi nel 2025 e nel primo quadrimestre 2026 evidenzia come gli effetti più rilevanti non siano limitati alla compromissione delle informazioni, ma comprendano interruzioni prolungate dei servizi, blocchi produttivi e conseguenze su organizzazioni terze, talvolta non direttamente coinvolte nell'attacco iniziale. Particolarmente significativa è la ricorrenza di attacchi alle catene di fornitura digitali e alle infrastrutture condivise, che possono amplificare gli effetti di un singolo incidente su molteplici organizzazioni. Tra gli attacchi più rilevanti selezionati per il primo quadrimestre 2026 emergono anche operazioni attribuite a gruppi riconducibili a Stati, in particolare all'Iran e alla Corea del Nord. Tali episodi evidenziano il crescente intreccio tra criminalità informatica, obiettivi economici e finalità geopolitiche.

3.2 Il quadro a livello Unione Europea (ENISA)

I rischi per la sicurezza digitale a livello mondiale riportati nel precedente paragrafo, si riflettono anche sui paesi dell'Unione Europea (UE), e quindi di fatto all'intera area europea, come ben dettagliato nei più recenti rapporti ENISA, l'Agenzia europea per la cybersicurezza (https://www.enisa.europa.eu/), in particolare

ENISA ora ha anche il compito di effettuare analisi sui rischi e sugli attacchi digitali, sulle misure di sicurezza in essere nelle aziende/enti che devono seguire le varie normative emanate dall'UE, le principali elencate nella fig. 3.2-1.

L'evoluzione del quadro normativo europeo per la sicurezza digitale

Negli ultimi anni l'Unione Europea ha progressivamente ampliato e rafforzato il quadro normativo che disciplina la sicurezza digitale, la protezione dei dati, la resilienza operativa e l'utilizzo delle nuove tecnologie, con particolare attenzione all'intelligenza artificiale.

Provvedimenti quali NIS2, DORA, Cyber Resilience Act e AI Act, insieme alle normative sulla protezione dei dati e alle ulteriori iniziative legislative europee, delineano un approccio sempre più integrato alla sicurezza digitale, che non riguarda soltanto le infrastrutture e i sistemi informatici, ma coinvolge i processi aziendali, le catene di fornitura, la gestione dei rischi e le responsabilità degli organi di governo delle organizzazioni pubbliche e private.

Questa evoluzione normativa comporta, per le organizzazioni interessate, la necessità di adottare misure tecniche e organizzative adeguate, rafforzare le capacità di prevenzione, rilevazione e risposta agli incidenti, verificare la sicurezza dei fornitori e assicurare la continuità delle attività e dei servizi.

La crescente articolazione del quadro regolatorio richiede inoltre un approccio coordinato alla conformità normativa, evitando che gli adempimenti relativi alle diverse disposizioni siano affrontati separatamente e senza una visione complessiva dei rischi digitali.

La tabella seguente, fig. 3.2-1**,** presenta una sintesi dei principali provvedimenti e delle iniziative normative dell'Unione Europea rilevanti per la sicurezza digitale delle organizzazioni, evidenziando la progressiva estensione degli ambiti regolamentati.

Normativa	Riferimento UE	Obiettivi norma	Link alla normativa
GDPR, General Data Protection Regulation	2016/679	Regolamento sulla privacy, con nuove regole per la protezione dei dati personali, che sostitusice la precedente Direttiva 95/46/EC	http://data.europa.eu/eli/reg/2016/679/oj
Cyber Security Act	2019/881	Regolamento per la riorganizzazione ENISA e per realizzare l'European cybersecurity certification framework tipo Common Criteria europeo	https://eur-lex.europa.eu/eli/reg/2019/881/oj
Regolamento **beni a duplice uso** (dual-use)	2021/821	Regolamento per la creazione di un nuove regime dell'UE per il controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di beni a duplice uso (rifusione)	http://data.europa.eu/eli/reg/2021/821/oj
Data Governance Act (DGA)	2022/868	Definisce un quadro per il riutilizzo e la condivisione dei dati, disciplinando intermediari dei dati, altruismo dei dati e meccanismi di fiducia.	https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R0868
DORA, Digital Operational Resilience Act	2022/2554	Regolamento per incrementare le misure di sicurezza a favore della resilienza e della sicurezza informatica del settore finanziario	https://eur-lex.europa.eu/eli/reg/2022/2554/oj
NIS 2, Network and Information Security	2022/2555	Direttiva sulle misure di sicurezza per i fornitori di servizi essenziali per i ogni Stato Membro (infrastrutture critiche)	https://eur-lex.europa.eu/eli/dir/2022/2555/oj
CER, Critical Entities Resilience Directive	2022/2557	Direttiva relativa alla resilienza dei soggetti critici	https://eur-lex.europa.eu/eli/dir/2022/2557/oj
DSA, Digital Services Act	2022/2065	Regolamento con nuove regole per contrastare la diffusione di contenuti illegali e disinformazione sulle piattaforme ed I motori di ricerca	https://eur-lex.europa.eu/eli/reg/2022/2065/oj
Data Act	2023/2854	Disciplina accesso e utilizzo equo dei dati, portabilità e passaggio tra servizi di elaborazione dati/cloud, nonché garanzie relative ad accessi illeciti a dati non personali.	https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32023R2854
eIDAS 2.0, electronic IDentification, Authentication and trust Services	2024/1183	Revisione del precedente Regolamento eIDAS (2014/910), per creare un'identità digitale europea sicura e interoperabile per tutti i cittadini e le imprese. Il nuovo regfolamento introduce l'European Digital Identity Wallet (EUDI Wallet), un portafoglio digitale sicuro per tutti i dati e documenti d'identità.	https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401183
AI Act, Artificial Intelligence Act	2024/1689	Stabilisce un quadro normativo per l'intelligenza artificiale nell'UE, classificando i sistemi di IA in base al loro rischio e imponendo requisiti in base al livello di rischio; prima normativa a livello mondiale che crea un quadro giuridico armonizzato, con l'obiettivo di garantire un'IA affidabile, sicura e rispettosa dei diritti fondamentali.	https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ:L_202401689&qid=1757777904772
Regolamento di esecuzione NIS2	Reg. esec. (UE) 2024/2690	Specifica i requisiti tecnici e metodologici di gestione del rischio cyber e i criteri di incidente significativo per determinate categorie di fornitori digitali e servizi fiduciari.	https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32024R2690
CRA, Cyber Resilience Act	2024/2847	Regolamento che stabilisce requisiti obbligatori di cybersecurity per tutti i prodotti con elementi digitali (hardware e software) immessi sul mercato europeo.	https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024R2847
Cybersecurity Act – servizi di sicurezza gestiti	2025/37	Modifica il Cybersecurity Act (2019/881), estendendo i possibili schemi UE di certificazione della cybersicurezza ai servizi di sicurezza gestiti (monitoraggio, risposta agli incidenti ecc.).	https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32025R0037
Cyber Solidarity Act	2025/38	Rafforza la capacità UE di rilevare, prepararsi e rispondere a minacce e incidenti cyber, attraverso allerta comune, interventi di emergenza e cooperazione tra Stati membri.	https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32025R0038
European Health Data Space (EHDS)	2025/327	Istituisce lo spazio europeo dei dati sanitari per accesso, controllo, scambio e riutilizzo sicuro dei dati sanitari elettronici, con requisiti di interoperabilità.	https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32025R0327
Digital Omnibus on AI (approvato)	Reg. (UE) 2026/1744	Modifica l'AI Act e altri regolamenti UE per semplificare l'attuazione della normativa sull'IA, adeguandone obblighi e tempistiche di conformità.	https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32026R1744
Digital Omnibus – dati, privacy e cybersecurity (PROPOSTA)	COM(2025) 837 final	PROPOSTA NON APPROVATA: razionalizza disposizioni su GDPR, ePrivacy, Data Act, NIS2 e CER; propone semplificazioni e coordinamento delle notifiche e degli adempimenti.	https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52025PC0837
NOTA	Proposte in iter	Nel gennaio 2026 la Commissione europea ha proposto la revisione del Cybersecurity Act e interventi su NIS2. Le proposte non costituiscono norme approvate.	

Fig. 3.2-1

Tra le tante informazioni fornite da ENISA con vari rapporti, l'autore ha scelto quelle del rapporto "ENISA Threat Landscape (ETL) 2026"[7], che fanno riferimento all'intero anno 2025. Questi dati derivano da quanto raccolto dalle diverse Agenzie per la sicurezza digitale nell'UE, come l'ACN per l'Italia, e quindi fanno riferimento prevalentemente a sistemi informativi "critici" e soggetti prevalentemente alla Direttiva NIS2.

In estrema sintesi, tra i risultati di questo ultimo rapporto ENISA emerge che nel 2025, in ambito UE:

- Il ransomware rimane la tipologia di incidente con il maggiore impatto nel breve termine.
- La Pubblica Amministrazione continua a essere il settore più colpito.
- Le campagne DDoS legate all'hacktivism rimangono strettamente connesse alle tensioni geopolitiche.

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

- La dipendenza da fornitori, servizi e componenti digitali amplia la superficie di attacco.
- I modelli di IA emergenti sono destinati a essere utilizzati sempre più spesso a supporto di attività malevole.

I gruppi di criminalità informatica, gli hacktivisti e gli attori legati ad apparati statali hanno fatto sempre più ricorso a tecniche scalabili, modelli di strumenti condivisi e ambienti digitali affidabili per condurre attività malevole. Nel 2025 ENISA ha inoltre osservato una crescente integrazione dell'intelligenza artificiale nelle attività informatiche illecite, incluse quelle messe in atto da criminali informatici, gruppi di intrusione legati ad apparati statali e attori dediti alla manipolazione dell'informazione (IMS, Information Manipulation Sets).

gli attacchi DDoS rimangono la tipologia di incidente principale (51,3%), seguiti dagli accessi non autorizzati (39,5%);

Gli aspetti geopolitici, come il protrarsi della guerra di aggressione della Russia contro l'Ucraina o l'escalation del conflitto in Medio Oriente, hanno continuato a influenzare attacchi digitali e disinformazione in ambito UE. Le operazioni guidate da motivazioni ideologiche hanno rappresentato una quota significativa delle attività osservate (57,3%), in particolare attraverso campagne DDoS condotte da "hacktivist" contro servizi esposti al pubblico, enti essenziali e organizzazioni legate a sviluppi politici o al sostegno a paesi come l'Ucraina o Israele. Gruppi di intrusione riconducibili ad attori statali hanno continuato a svolgere attività di spionaggio informatico (5,9%): quelli legati alla Russia hanno preso di mira principalmente enti governativi centrali e diplomatici, mentre quelli riconducibili alla Cina hanno mostrato un costante interesse per il settore dei trasporti, incluso quello marittimo.

La fig. 3.2-2 visualizza la ripartizione % dei vettori di attacco[8]: il 60,4% è dovuto a vulnerabilità, gli altri vettori hanno percentuali assai più basse.

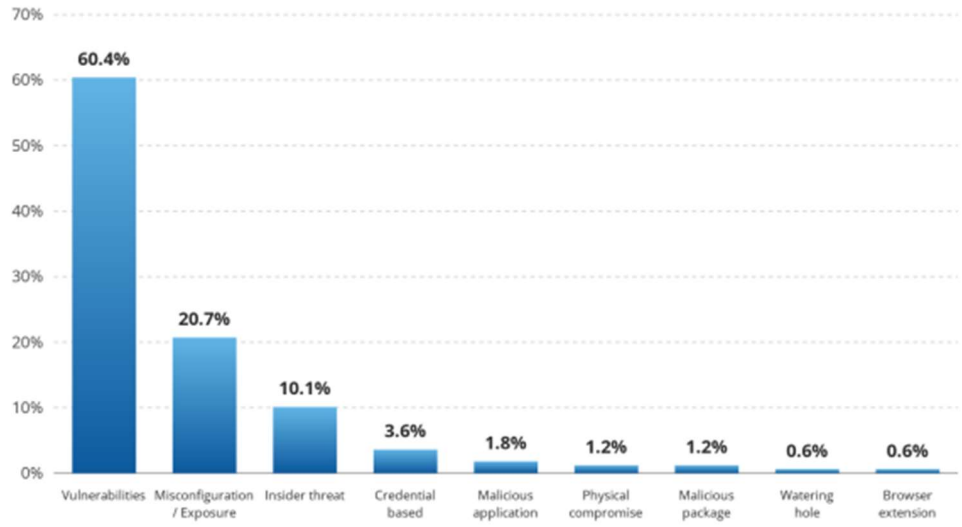


Fig. 3.2-2 (Fonte: ENISA)

[8] Il termine "vettore d'attacco" (attack vector) indica il percorso, il metodo o lo strumento utilizzato per attuare un attacco digitale. Tipici esempi: phishing e ingegneria sociale, malware e ransomware, sfruttamento di vulnerabilità, furto di credenziali, compromissione della supply chain, ecc.

La fig. 3.2-3 mostra le tipologie di attacco percentualmente più diffuse in UE, iniziate coi vettori di cui alla precedente figura. A livello UE la stragrande maggioranza è data da DoS/DDoS con un 51,3%, seguito da accessi non autorizzati per il 39,5%

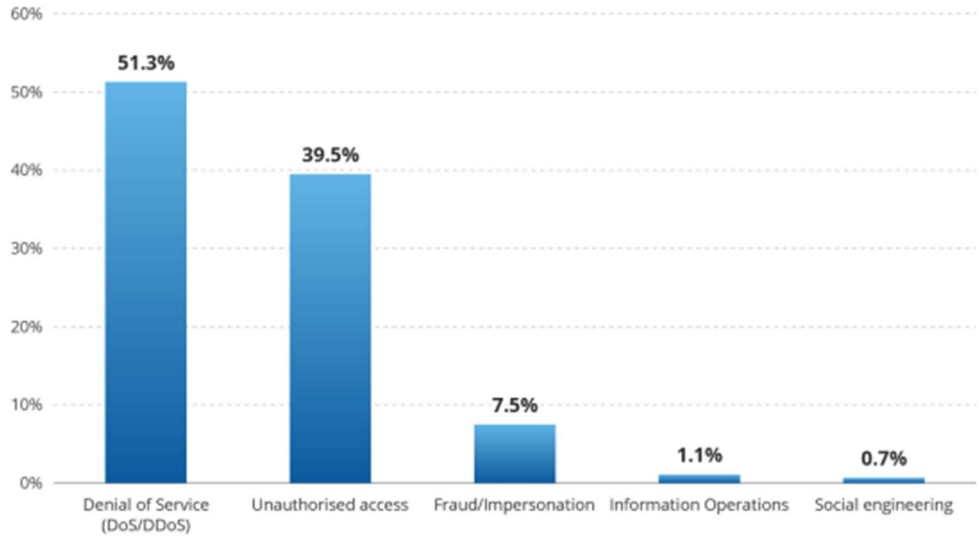


Fig. 3.2-3 (Fonte: ENISA)

In merito alle tipologie di attacco, ENISA per il 2025 sottolinea che:

- tra le tecniche di ingegneria sociale, il phishing si conferma il vettore di intrusione più diffuso (77,8%), seguito dallo spam malevolo, che rappresenta il 13%;
- si è riscontrato un crescente ricorso alla tecnica "ClickFix"[9], che induce la vittima a "risolvere" un problema portando di fatto all'esecuzione di codice malevolo;
- cresce la diffusione di kit per il phishing e di piattaforme "Phishing-as-a-Service" (PhaaS);
- lo sfruttamento di vulnerabilità di tipo N-day e 0-day rimane un vettore di intrusione prevalente. Tra gli incidenti di accesso non autorizzato per i quali l'ENISA è riuscita a identificare un vettore di intrusione (5,2%), nel 60,4% dei casi è stato riscontrato lo sfruttamento di una vulnerabilità, mentre le configurazioni errate e l'esposizione accidentale continuano a rappresentare un motivo di preoccupazione (20,7%)

La fig.3.2-4 evidenzia come la distribuzione delle categorie di minaccia si concentri in poche aree: le minacce per dispositivi mobili rappresentano la quota maggiore, pari al 42,4%, confermando come tali dispositivi continuino a costituire una superficie di attacco privilegiata. Seguono le minacce web con il 27,3%, a sottolineare il costante sfruttamento di servizi e applicazioni online. Le minacce legate alle tecnologie operative (OT) si attestano al 18,2%, riflettendo la crescente esposizione dei sistemi industriali e infrastrutturali critici, sempre più interconnessi e oggetto di attacchi mirati. I rischi legati alla catena di approvvigionamento (supply chain) costituiscono il 10,6%, dimostrando come gli attaccanti sfruttino attivamente vettori indiretti attraverso fornitori terzi e dipendenze esterne.

[9] Tecnica ingegneria sociale in cui l'attaccante inganna la vittima facendole installare autonomamente un malware, mascherando l'operazione come la risoluzione di un problema tecnico o una verifica di sicurezza

⚠ La fig. 3.2-4 fornisce il dato più interessante, secondo l'autore: il 57,3% delle motivazioni dell'attacco sono di tipo "**ideologico**", prevalentemente associate all'hacktivism e realizzate mediante attacchi DDoS, contro il 29,3% di attacchi motivati da illeciti guadagni finanziari. Nell'ambito delle motivazioni ideologiche possono essere inclusi anche alcuni casi di cyber terrorismo e di cyber warfare, ma occorre evidenziare che questi ultimi sono fenomeni diversi per finalità, caratteristiche e soprattutto gravità: il più delle volte questi ultimi attacchi sono caratterizzati da maggiore sofisticazione tecnica, e con impatti ben più gravi e distruttivi.

Le operazioni a scopo di lucro sono state condotte prevalentemente da attori della criminalità informatica, sebbene alcuni casi siano stati ricondotti a gruppi di hacktivisti e a minacce legate ad attori statali. Infine, le campagne di cyberspionaggio hanno rappresentato il 5,9% del totale.

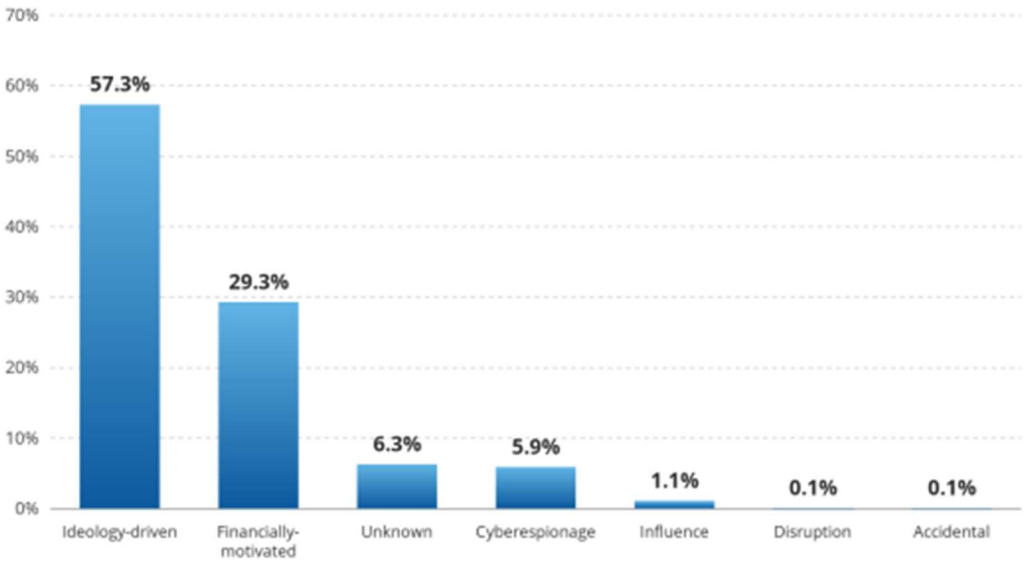


Fig. 3.2-4 (Fonte: ENISA)

La fig. 3.2-5 evidenzia, in percentuale, i principali settori europei sotto attacco digitale nel 2025. Le Pubbliche Amministrazioni, sia centrali che locali, sono largamente in testa con un 31,8%, mentre l'ambito finanziario sono ultime nel grafico con un 5,6%. Questo è un ulteriore indicatore che conferma come gran parte degli attacchi nel 2026 abbiano avuto motivazioni

Importante ricordare che questi dati prodotti da ENISA sono basati su quanto riscontrato dalle agenzie nazionali per la sicurezza digitali dei paesi dell'UE, organizzazioni che controllano prevalentemente la cyber sicurezza delle infrastrutture critiche e dei servizi essenziali per ogni singolo paese.

Per meglio inquadrare la prevalenza delle motivazioni ideologiche negli incidenti digitali analizzati da ENISA, è utile considerare il contesto geopolitico in cui si colloca l'Unione Europea (UE) e, più in generale, il peso demografico delle democrazie nel mondo:

- L'UE rappresenta circa il 5,4% della popolazione mondiale secondo le stime 2026 di Eurostat (452 milioni di abitanti nell'UE rispetto a circa 8,33 miliardi nel mondo);
- le principali democrazie industrializzate e i Paesi democratici affini (UE, Stati Uniti, Canada, Australia, Giappone, Regno Unito, Nuova Zelanda, Svizzera, Norvegia, Corea del Sud e Taiwan) rappresentano complessivamente circa il **14% della popolazione mondial;
- I paesi classificati come democrazie liberali o elettorali[10] rappresentano complessivamente quasi il **26%** della popolazione mondiale, comprendendo anche democrazie dell'America Latina, dell'Africa, e dell'Asia e Oceania, oltre a Israele;
- Secondo il Democracy Report 2026 di V-Dem, solo circa **il 7%** della popolazione mondiale vive in Paesi classificati come democrazie liberali, secondo i criteri più rigorosi dell'istituto. Dal 2025 gli Stati Uniti sono classificati come democrazia elettorale, così come Israele dal 2023.

Le democrazie liberali rappresentano quindi una minoranza della popolazione mondiale, pur esercitando un'influenza economica, finanziaria, scientifica e tecnologica ben superiore al loro peso demografico. In un contesto internazionale caratterizzato da crescenti tensioni geopolitiche, contrapposizioni politiche e competizione tecnologica, tale ruolo contribuisce a esporre l'UE e le altre democrazie a iniziative ostili, comprese quelle condotte nello spazio digitale. Il dato ENISA sulle motivazioni ideologiche degli attacchi va letto anche in questo contesto: una parte rilevante degli incidenti rilevati è riconducibile ad attività di hacktivism, spesso realizzate attraverso attacchi DDoS e collegate a conflitti, tensioni internazionali e posizioni politiche assunte dai Paesi bersaglio.

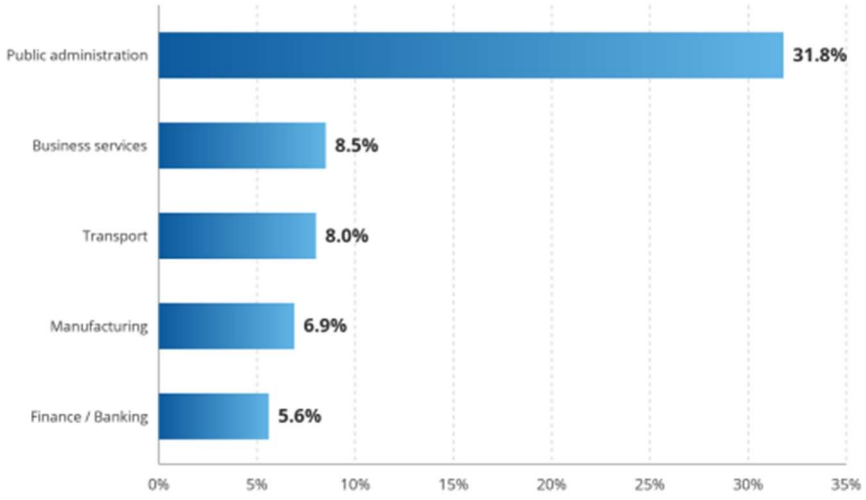


Fig. 3.2-5 (Fonte: ENISA)

[10] Il V-Dem Institute, dell'Università di Göteborg, https://www.v-dem.net/, produce annualmente un **Democracy Report**, e distingue, tra le altre categorie:

- **Democrazia elettorale**: sistema in cui i cittadini possono scegliere e sostituire i governanti attraverso elezioni libere, corrette e competitive, con le libertà politiche necessarie.
- **Democrazia liberale**: sistema che, oltre a garantire elezioni democratiche, tutela i diritti individuali, lo Stato di diritto, l'indipendenza della magistratura e l'effettiva limitazione del potere esecutivo.

A livello UE le principali tendenze sugli attacchi includono:

- L'attività di intrusione rimane significativa, con il ransomware al centro.
- Gruppi di minaccia legati ad attori statali hanno intensificato le loro campagne di cyberspionaggio a lungo termine contro i settori delle telecomunicazioni, delle reti logistiche e manifatturiero nell'UE, dimostrando tecniche operative avanzate quali la compromissione della catena di approvvigionamento, l'impiego di framework malware furtivi e l'abuso di driver firmati.
- L'attività di hacktivism continua a dominare, rappresentando quasi l'80% degli incidenti registrati e essendo trainata principalmente da operazioni di Distributed Denial of Service (DDoS) di basso livello. Sebbene nel complesso comportino un impatto molto ridotto, tali campagne dimostrano come strumenti a basso costo vengano impiegati su larga scala per operazioni guidate da motivazioni ideologiche.
- Il phishing come principale vettore iniziale di attacchi, in particolare per il furto di credenziali, … session hijacking, payload deployment o l'esecuzione di comandi. Significativo il contributo di piattaforme di Phishing-as-a-Service (PhaaS), tra le quali Dracula, Lucid, FlowerStorm.
- Le reti della pubblica amministrazione rimangono l'obiettivo principale (31,8%), in particolare per gli hacktivisti e i gruppi di intrusione legati ad attori statali, mentre il settore dei trasporti – segnatamente quello marittimo e la logistica – è emerso come un ambito di grande interesse. Le attività del trasporto aereo e della movimentazione merci hanno subito interruzioni causate da ransomware, mentre le infrastrutture e i servizi digitali continuano a rappresentare obiettivi strategici sia per attività di cyberspionaggio sia per gli autori di attacchi ransomware.
- L'intelligenza artificiale è diventata un elemento distintivo del panorama delle minacce. Si stima che, all'inizio del 2025, le campagne di phishing supportate dall'IA rappresentassero oltre l'80% delle attività di ingegneria sociale osservate a livello globale; gli attaccanti hanno sfruttato modelli "jailbroken"[11], contenuti multimediali sintetici e tecniche di avvelenamento dei modelli per accrescere la propria efficacia operativa.
- Il panorama delle minacce delineato riflette una transizione verso pressioni miste e potenzialmente convergenti, caratterizzate da un minor numero di singoli incidenti ad alto impatto a fronte di campagne più continue, diversificate e convergenti che, nel loro insieme, ne-ro-dono la resilienza.
- Crescenti attacchi ai fornitori di servizi digitali. Ad esempio, nel marzo 2025, Plus Service, un fornitore esterno che gestisce la piattaforma Telemaco per diverse aziende di trasporto italiane, ha subito una violazione dei dati che ha comportato l'esfiltrazione non autorizzata di informazioni verso un cloud remoto; ciò ha reso necessarie restrizioni temporanee all'accesso, in attesa del completamento delle operazioni di ripristino. L'episodio ha causato, in particolare, il blocco per due giorni dei sistemi di bigliettazione di Mobilità di Marca (MoM), con ripercussioni su diverse migliaia di pendolari. La stessa campagna ha interessato l'app e il portale per gli abbonamenti di Busitalia Veneto, nonché ATM Milano. Altri esempi significativi includono l'attacco, nel maggio 2025, a un fornitore di servizi esterno della Berliner Verkehrsbetriebe (BVG) — che ha coinvolto i dati di 180.000 clienti della società — e l'accesso non autorizzato ai dati dei clienti della compagnia energetica spagnola Repsol, a seguito della compromissione di uno dei fornitori dell'azienda.
- Significativi attacchi alle supply chain informatizzate. Il gruppo Lazarus, legato alla Corea del Nord, ha sfruttato la compromissione della catena di fornitura (supply chain); le sue attività più recenti hanno

[11]I modelli "jailbroken" di Intelligenza Artificiale sono Large Language Model (LLM) modificati o manipolati per aggirare le barriere di sicurezza, i filtri etici e le restrizioni imposte dai loro sviluppatori originari. il termine "jailbreak" indica che il modello è stato "liberato dalla sua prigione etica", ossia che vengono rimosse le barriere alla generazione di contenuti dannosi e/o illegali, che un modello standard (come ChatGPT o Claude) rifiuterebbe di produrre. Gli attaccanti sfruttano la totale assenza di filtri di questi modelli per automatizzare e scalare i propri attacchi con la produzione di malware, di phishing iper realistici, di disinformazione massiva, e con la ricerca di dati e di vulnerabilità sui sistemi informativi e sulle organizzazioni target.

riguardato il rilascio di pacchetti malevoli su Node Package Manager (npm) all'interno di repository GitHub, camuffati da librerie legittime al fine di compromettere gli ambienti di lavoro degli sviluppatori.

- La convergenza di gruppi di attaccanti. I confini tra hacktivism, criminalità informatica e attività legate ad attori statali continuano a farsi sempre più labili. Gruppi di intrusione, storicamente distinguibili in base al livello di sofisticazione delle proprie TTP (tattiche, tecniche e procedure), alle attività condotte o agli obiettivi perseguiti, condividono sempre più spesso strumenti e modus operandi. Un aspetto rilevante di questa tendenza è il cosiddetto "faketivism", in cui gruppi di intrusione vicini ad apparati statali adottano l'identità e le modalità operative tipiche degli hacktivist. Esempi significativi includono il gruppo "Cyber Army of Russia Reborn", associato a Sandworm (attore legato alla Russia) e il gruppo "CyberAv3ngers", collegato al Corpo delle Guardie della Rivoluzione Islamica (IRGC) dell'Iran.
- Parallelamente, gli strumenti utilizzati dagli hacktivist e gli ecosistemi della criminalità informatica si intersecano sempre più frequentemente.
- Un altro aspetto di questa tendenza è rappresentato dalle operazioni "false-flag" (sotto falsa bandiera), come quella condotta dal gruppo Turla, che ha preso il controllo dell'infrastruttura di "Transparent Tribe". Analogamente, alcuni criminali informatici si sono finti altri gruppi criminali o ne hanno contraffatto il "marchio"; un esempio eclatante è costituito da campagne di estorsione via e-mail in cui gli autori si sono spacciati per il gruppo ransomware CL0P. Gruppi di intrusione legati ad attori statali hanno inoltre fatto ricorso a tecniche e competenze tipiche della criminalità informatica.
- È stato riscontrato un impiego costante dell'intelligenza artificiale (IA) da parte di svariati gruppi di intrusione, sia come strumento per agevolare o potenziare le attività offensive, sia come bersaglio da sfruttare. In particolare:
    - I modelli linguistici di grandi dimensioni (LLM) vengono utilizzati per creare e-mail di phishing più convincenti. Modelli linguistici come WormGPT, EscapeGPT e FraudGPT vengono impiegati per automatizzare attività di ingegneria sociale e accelerare lo sviluppo di strumenti malevoli.
    - L'IA viene utilizzata anche come esca: si registra una proliferazione di siti web fraudolenti che imitano strumenti di IA legittimi, come Kling AI, Luma AI, Canva Dream Lab e DeepSeek-R1, al fine di distribuire malware.
    - La crescente integrazione di sistemi basati sull'IA negli ambienti aziendali introduce una nuova superficie di attacco, potenzialmente vulnerabile.

🔍 Sull'importanza dell'IA nella sicurezza digitale, sia come strumento di attacco che di difesa, ENISA a luglio 2026 ha pubblicato il documento "ENISA's view on Cybersecurity in the Frontier AI Era"[12], che fornisce un primo insieme di raccomandazioni per affrontare rischi ed attacchi che ormai sono condotti alla velocità dei potenti computer odierni.

[12] https://www.enisa.europa.eu/sites/default/files/2026-07/ENISA%20view%20on%20cybersecurity%20in%20the%20frontier%20AI%20era_en_0.pdf

3.3 Il quadro a livello italiano

La fonte principale ed istituzionale di informazioni è l'**ACN**, Agenzia per la Cybersicurezza Nazionale (https://www.acn.gov.it/), grazie soprattutto al CSIRT, Computer Security Incident Response Team, che da lei dipende.

In estrema sintesi la situazione dei rischi e degli attacchi in Italia, per i sistemi critici ed essenziali (prevalentemente quelli che devono ottemperare alla norma NIS2) sono sintetizzati nella fig. 3.3-1

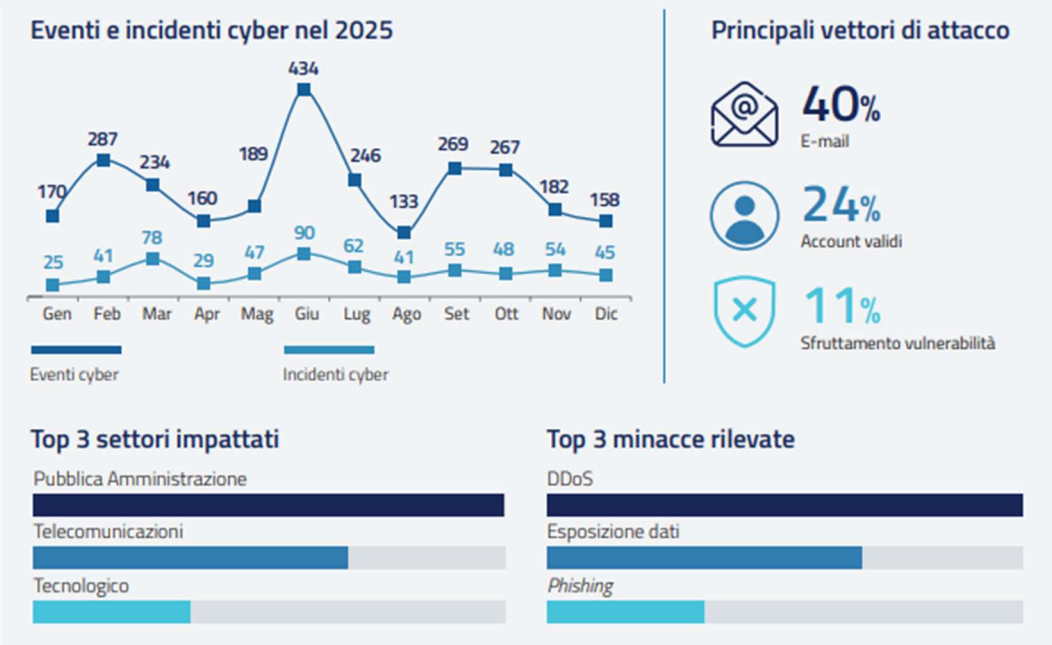


Fig. 3.3-1 (Fonte: ACN)

È bene chiarire la distinzione che ACN fa tra eventi e incidenti cyber:

- **Evento cyber:** "Un avvenimento d'interesse per il CSIRT Italia con potenziale impatto su almeno un soggetto nazionale". Individua un rischio con potenziale impatto: ad esempio un'attività malevola rilevata, una possibile compromissione o un'attività ostile che viene individuata e magari neutralizzata prima che produca conseguenze
- **Incidente cyber:** "Un evento cyber con impatto confermato dalla vittima o dal CSIRT Italia". L'evento cyber diventa **incidente** quando viene accertata una perturbazione: indisponibilità di un servizio, compromissione di sistemi, esfiltrazione di dati, cifratura, alterazione ecc. ACN definisce infatti l'**impatto** come la "perturbazione causata da un evento cyber". In pratica l'attacco è andato a buon fine ed ha avuto impatti sull'attaccato.

Nel 2025 il CSIRT Italia ha gestito complessivamente **2.729 eventi cyber**, ma solo **615 sono stati classificati come incidenti**.

Nel 2026 il CSIRT ha pubblicato su base mensile, con "Operational Summary ACN/CSIRT Italia", il numero di eventi ed incidenti rilevati, sintetizzati nella tabella di fig. 3.3-2

Mese 2026	Eventi cyber	Incidenti cyber
Gennaio	225	39
Febbraio	436	174
Marzo	436	313
Aprile	265	174
Maggio	390	158
Giugno	424	184
Luglio	305	188
Totale gen.–lug.	**2.481**	**1.230**

Fig. 3.3-2 (Fonte: ACN-CSIRT)

Dall'analisi della tabella con dati solo fino a fine luglio 2026, rispetto al 2025:

- gli **eventi** hanno già raggiunto circa il **91%** dell'intero 2025;
- gli **incidenti** sono già circa il **200%** del totale 2025, cioè **il doppio**;
- pertanto, salvo anomalie molto forti negli ultimi mesi, il numero annuale di eventi 2026 **supererà certamente o quasi certamente** quello del 2025;
- **per gli incidenti**, invece, il superamento non è una previsione: **è già avvenuto**.

I dati disponibili per il 2026 indicano quindi una **significativa crescita** del numero di eventi e, soprattutto, **degli incidenti cyber rilevati** da ACN/CSIRT Italia **rispetto all'anno precedente**. Nei primi sette mesi del 2026 sono stati infatti registrati 2.481 eventi e 1.230 incidenti, a fronte dei 2.729 eventi e 615 incidenti rilevati nell'intero 2025. Già a luglio 2026, pertanto, il numero degli incidenti risulta doppio rispetto a quello registrato nell'intero anno precedente, mentre il numero degli eventi ha già raggiunto circa il 91% del totale 2025.

Sulla base dell'andamento osservato, è pertanto ragionevole attendersi che, a fine 2026, anche il numero complessivo degli eventi risulti superiore a quello dell'anno precedente.

Tali dati devono tuttavia essere interpretati con cautela: l'incremento degli incidenti rilevati non è necessariamente riconducibile a un corrispondente aumento della minaccia cyber, ma risente anche della maggiore capacità di rilevazione e segnalazione e, in particolare, dell'entrata a regime dei nuovi obblighi di notifica previsti dalla normativa NIS2.

Il forte incremento di attacchi nei primi mesi del 2026 rispetto al 2025 è anche confermato dalle risposte delle organizzazioni che hanno compilato il questionario OAD 2026, e che sono riportati nella fig. 4-2 nel prossimo capitolo.

Il quadro fornito da ACN evidenzia inoltre come le modalità di attacco continuino a concentrarsi su vettori ormai consolidati. Nel 2025 le e-mail, soprattutto di phishing, rappresentano il principale vettore di attacco, con il 40% dei casi, seguite dall'utilizzo di account validi, quindi ottenuti con il loro furto, con il 24%, e dallo sfruttamento di vulnerabilità, con l'11%. Tra i settori maggiormente impattati figurano la Pubblica Amministrazione, le telecomunicazioni e il comparto tecnologico, mentre tra le principali minacce rilevate emergono in particolare gli attacchi DDoS, l'esposizione di dati e il phishing.

Questi elementi confermano come il rischio cyber in Italia sia caratterizzato non solo dalla crescita quantitativa degli eventi rilevati, ma anche dalla persistenza di tecniche di attacco consolidate, spesso in grado di produrre impatti operativi significativi sui soggetti maggiormente critici per il funzionamento del Sistema Paese.

Va infine sottolineato che i dati ACN rappresentano una vista istituzionale del fenomeno, particolarmente significativa per i soggetti e i sistemi maggiormente critici ed essenziali e, più in generale, per il perimetro interessato dagli obblighi previsti dalla normativa NIS2. Essi non esauriscono quindi il fenomeno degli attacchi digitali che interessano aziende ed enti italiani.

Il successivo Capitolo 4 integra questo quadro attraverso i risultati dell'indagine OAD 2026, basati sulle esperienze direttamente dichiarate dalle organizzazioni rispondenti, consentendo così di confrontare la prospettiva istituzionale con quella rilevata sul campo dall'Osservatorio.

3.3.1 Il confronto dei dati CSIRT Italia-ACN con quelli del CNAIPIC del Servizio Polizia Postale e per la Sicurezza Cibernetica

Facendo riferimento ai dati forniti dal CNAIPIC del Servizio Polizia Postale e per la Sicurezza Cibernetica, riportati nel successivo Cap. 8, emergono valori diversi da quelli rilevati da ACN.

Nel 2025 il CSIRT Italia dell'ACN ha trattato complessivamente 2.729 eventi cyber, dei quali 615 sono stati classificati come incidenti, ossia eventi per i quali è stato confermato un impatto sui soggetti coinvolti. Nello stesso periodo, la Polizia Postale e per la Sicurezza Cibernetica ha rilevato 9.440 casistiche/eventi informatici. Di questi, 967 hanno riguardato Infrastrutture Critiche (I.C.), Operatori di Servizi Essenziali (OSE) e Pubbliche Amministrazioni Locali (PAL), mentre le restanti casistiche hanno interessato imprese e soggetti privati.



Il marcato scostamento quantitativo non deve tuttavia essere interpretato come una divergenza nella valutazione del livello della minaccia cyber in Italia. I dati delle due istituzioni non sono infatti direttamente confrontabili, in quanto derivano da differenti perimetri di osservazione, modalità di rilevazione, criteri di classificazione e, soprattutto, dalle diverse funzioni istituzionali svolte.

In particolare:

- **il CSIRT Italia dell'ACN** svolge prevalentemente funzioni tecnico-operative di prevenzione, monitoraggio, allertamento e gestione degli incidenti cyber. Riceve notifiche e segnalazioni, analizza gli eventi, allerta i soggetti potenzialmente esposti, fornisce indicazioni di mitigazione e, nei casi più significativi, interviene direttamente a supporto delle organizzazioni colpite. Nel 2025, oltre ai 2.729 eventi trattati e ai 615 incidenti con impatto confermato, il CSIRT Italia ha inviato oltre 46.000 comunicazioni di allertamento, segnalato più di 31.000 dispositivi e servizi a rischio e condiviso oltre 800.000 indicatori di compromissione;
- **il CNAIPIC della Polizia Postale e per la Sicurezza Cibernetica** opera invece nell'ambito delle funzioni di prevenzione e contrasto dei reati informatici e di protezione delle infrastrutture critiche. Le sue attività comprendono monitoraggio, prima risposta e risposta all'incidente, ma anche attività di polizia giudiziaria, acquisizione delle evidenze digitali, individuazione degli autori degli attacchi e cooperazione investigativa nazionale e internazionale.

Ne consegue che un medesimo attacco può rientrare nell'attività di entrambe le istituzioni, ma essere acquisito e classificato secondo criteri differenti. Allo stesso modo, non tutte le casistiche rilevate dalla Polizia Postale corrispondono necessariamente a un "evento cyber" secondo la classificazione utilizzata da ACN, così come non tutti gli eventi trattati dal CSIRT Italia diventano "incidenti": nel 2025 soltanto 615 dei 2.729 eventi gestiti dal CSIRT hanno infatti prodotto un impatto confermato.

CSIRT Italia-ACN e Polizia Postale-CNAIPIC non costituiscono sistemi alternativi o indipendenti di rilevazione degli attacchi. Essi rappresentano componenti differenti e complementari dell'architettura nazionale di cybersicurezza. La cooperazione tra Polizia di Stato e ACN è stata inoltre formalizzata attraverso specifici accordi che prevedono lo scambio di informazioni, la collaborazione operativa e l'attivazione di sinergie tra le rispettive strutture specialistiche.

La seguente tabella in fig. 3.3.1-1 inquadra e confronta, sui temi di interesse OAD, ACN-CSIRT verso Polizia Postale-CNAIPIC

Tema	ACN-CSIRT	Polizia Postale-CNAIPIC
Funzione prevalente	Prevenzione e risposta tecnico-operativa	Prevenzione, contrasto e investigazione
Perimetro	Eventi e incidenti di interesse per il CSIRT, prevalentemente soggetti NIS2	Eventi rilevati nell'attività istituzionale di CNAIPIC (infrastrutture critiche) e denunce di attacchi digitali
Classificazioni	Eventi cyber e incidenti con impatto confermato	Categorie proprie delle rilevazioni della Polizia Postale
Possibili sovrapposizioni di eventi	SI	SI
Confrontabilità diretta	NO	NO

Fig. 3.3.1-1

La differenza quantitativa tra i dati pubblicati dalle due istituzioni deve quindi essere ricondotta principalmente ai differenti **perimetri di osservazione, criteri di classificazione e finalità istituzionali**, e non interpretata come una diversa valutazione dell'intensità della minaccia cyber nazionale.

4. Gli attacchi digitali in Italia dall'indagine OAD 2026

Il questionario OAD 2026 ha posto due sole domande sugli attacchi digitali subiti nel 2025, e due nel 1° quadrimestre 2026, dai Sistemi Informativi (SI) delle aziende/enti rispondenti, in modo da poter continuare l'analisi dei trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 ad oggi.

La prima domanda riguarda le **tipologie di attacco** (**che cosa si attacca**), che includono i seguenti 15 raggruppamenti (famiglie) di attacco (per ulteriori dettagli si veda Allegato A.1):

- Distruzione e/o compromissione FISICA di dispositivi ICT FISSI o di loro parti
- Furto dispositivi FISSI ICT o di loro parti
- Furto di dispositivi ICT MOBILI di proprietà dell'azienda/ente e in uso presso i suoi dipendenti/collaboratori
- Furto Informazioni da singoli specifici sistemi FISSI ICT (PC, server, storage system, etc.) del Sistema Informativo, anche terziarizzati/in cloud
- Furto Informazioni relative all'azienda/ente da sistemi MOBILI (palmari, smartphone, tablet, ecc.) sia di proprietà dell'azienda/ente sia dell'utente finale che li usa in logica BYOD
- Attacchi all'identificazione, autenticazione e controllo accessi degli utenti finali e privilegiati
- Attacchi alle RETI locali e geografiche, fisse e wireless, inclusi i collegamenti ad Internet, e ai DNS
- Attacco e/o uso non autorizzato di SISTEMI IT NEL LORO COMPLESSO (dal PC agli host fisici e virtuali). anche terziarizzati o in cloud
- Modifiche malevoli e/o non autorizzate ai PROGRAMMI APPLICATIVI e alle loro configurazioni, del Sistema Informativo anche terziarizzate e in cloud
- Modifiche malevoli e/o non autorizzate alle INFORMAZIONI trattate dalle applicazioni del Sistema Informativo, anche quelle terziarizzate/in cloud
- Saturazione (DoS, DDoS) risorse digitali del Sistema Informativo, anche quelle terziarizzate/in cloud
- Attacchi ai propri sistemi/servizi digitali in CLOUD o comunque TERZIARIZZATI presso Fornitori terzi
- Attacchi a dispositivi dei sistemi OT, Operational Technology, ivi inclusi i sistemi IoT/IIoT, i sistemi per l'automazione industriale (SCADA, DCS, PLC, strumenti di diagnosi medica informatizzati, ecc.) e la robotica
- Attacchi alla "Supply Chain" causati da vulnerabilità di fornitori e/o clienti interconnessi
- Attacchi a sistemi/servizi/applicativi basati su Intelligenza Artificiale.

La seconda domanda riguarda le famiglie di **tecniche di attacco** considerate (**come si attacca**), che includono:

- Attacco fisico
- Raccolta malevola e non autorizzata di informazioni
- Script e programmi maligni
- Agenti autonomi
- Toolkit
- Botnet e simili
- Utilizzo di strumenti e tecniche di Intelligenza Artificiale
- Utilizzo di due o più tecniche di attacco, inclusi gli APT, Advanced Persistent Threat.

A parte queste due domande che consentono la continuità storica con quanto rilevato nelle indagini OAD dei precedenti anni, si veda fig. 4.1-1, le altre domande del questionario 2026 erano in gran parte diverse da quelle degli anni precedenti.

La fig. 4-1 mostra che il **66,30%** delle organizzazioni rispondenti ha rilevato attacchi intenzionali nel 2025, e la fig. 4-2 mostra che **l'84,02%** delle organizzazioni rispondenti ha rilevato attacchi intenzionali nel 1° quadrimestre 2026.



Fig. 4-1

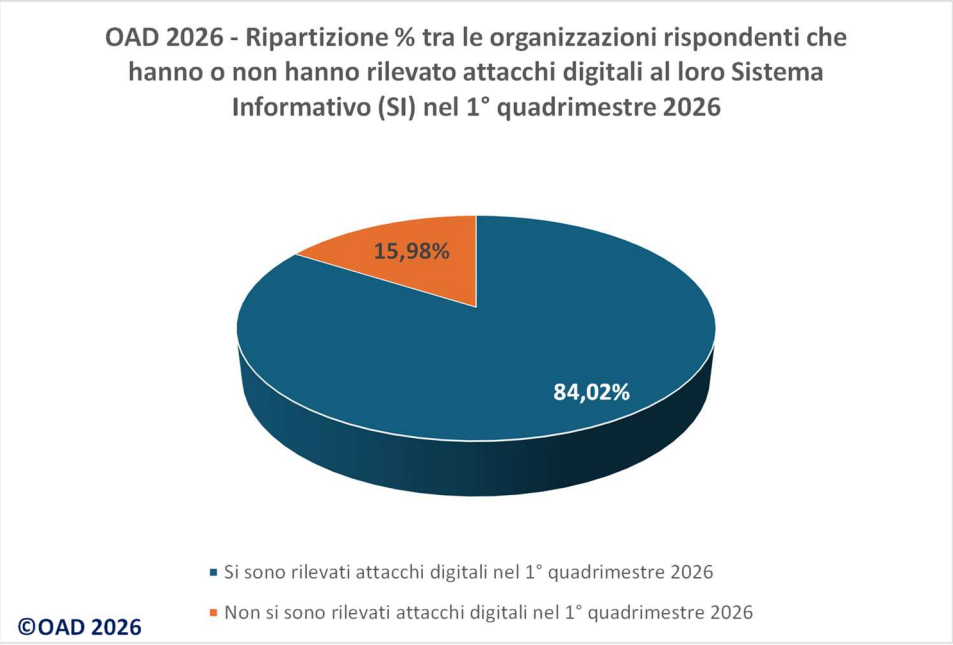


Fig. 4-2

Il confronto evidenzia un incremento particolarmente marcato della percentuale di organizzazioni rispondenti che dichiarano di aver rilevato attacchi digitali: dal 66,30% nell'intero 2025 all'84,02% nei soli primi quattro mesi del 2026. Pur riferendosi a periodi di diversa durata, il dato segnala un'elevata diffusione degli attacchi rilevati nel bacino OAD 2026 e merita particolare attenzione.

4.1 La tendenza negli anni degli attacchi digitali in Italia dalle indagini OAD

La fig. 4.1-1 mostra la percentuale di organizzazioni che hanno rilevato attacchi nei diversi Rapporti OAI/OAD **dall'anno 2007 al 1° quadrimestre 2026**.

Tale confronto non ha valenza statistica ed è da considerare come tendenza indicativa del trend della diffusione di attacchi digitali in Italia, dato che i campioni dei rispondenti nei diversi anni sono diversi come mix e come numero.

La figura evidenzia come, a parte il 2008 (che rappresentò il primo *annus horribilis* per la quantità di attacchi digitali subiti), dal 2007 al 2016 si è avuta una piccola variazione (+/-5 punti percentuali circa) del numero di attacchi rilevati rispetto ad un trend che si attesta attorno al 40% dei rispondenti come evidenziato in figura dalla riga rossa. Le piccole variazioni, in positivo e negativo, rispetto a questa tendenza, sostanzialmente piatta delle percentuali di attacchi digitali rilevati dalle indagini OAI/OAD, evidenzia il rincorrersi di guardie e ladri: si avvicendano periodicamente l'innovazione sulle modalità d'attacco, e le conseguenti "nuove" (o semplicemente attuate) misure di difesa atte a contrastarli. In questo periodo la percentuale di attacchi rilevati risulta sempre minore, e di non poco, rispetto agli attacchi non subiti/rilevati da parte delle organizzazioni rispondenti al questionario OAD.

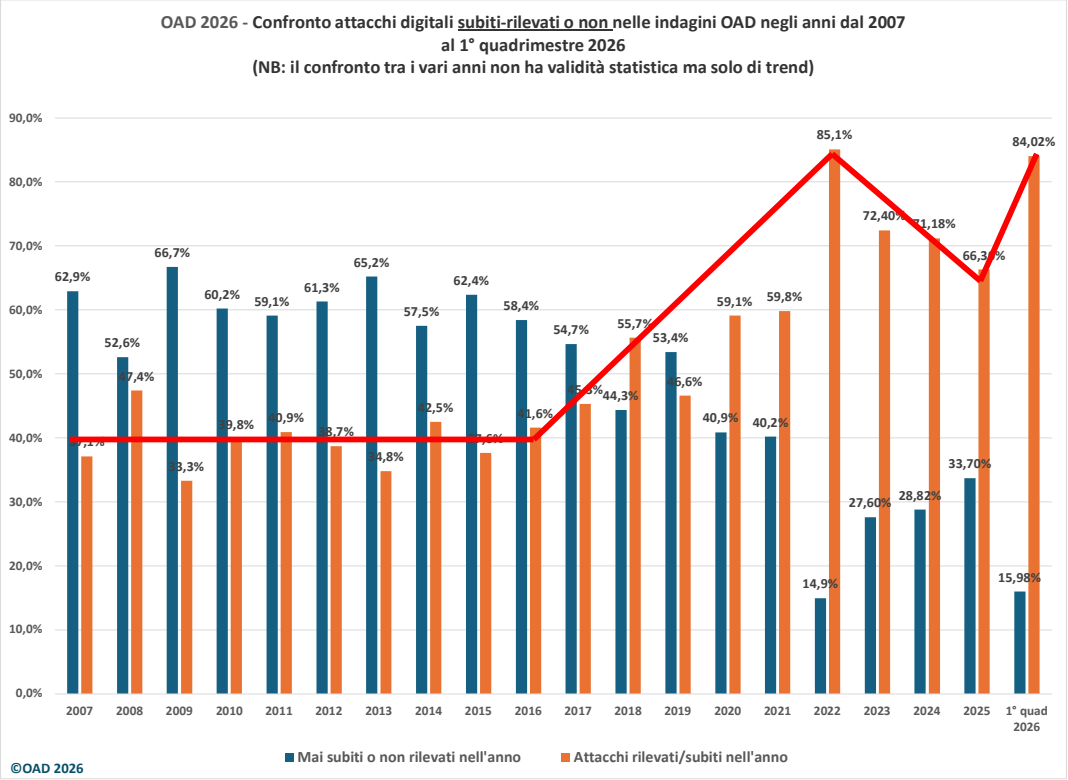


Fig. 4.1-1

Dal 2017, la percentuale degli attacchi rilevati inizia a crescere, e nel 2018 si evidenzia il primo picco di 55,7%, che porta la percentuale di attacchi rilevati a superare la percentuale di quelli non occorsi/rilevati. Nel 2019 la crescita dei precedenti tre anni si arresta, probabilmente confermando un significativo rafforzamento delle misure di sicurezza digitali, sempre in riferimento al bacino delle organizzazioni rispondenti a OAD.

⚠ **Dal 2020 ad oggi**, sempre nel campione dei rispondenti, la percentuale di chi ha rilevato attacchi digitali risulta sempre superiore a quella degli attacchi non subiti.

Nel 2022 si riscontra la percentuale più alta, 85,1%, di attacchi digitali rilevati nel bacino di compilatori.

Secondo l'interpretazione dell'autore, la persistenza di percentuali elevate di organizzazioni colpite o che hanno rilevato attacchi digitali costituisce un segnale di quella che può essere definita **insicurezza digitale sistemica** (systemic cyber insecurity): una condizione nella quale la crescente esposizione alle minacce rende sempre più difficile garantire una protezione completa dei SI. Da un lato gli attacchi intenzionali sono sempre più sofisticati e difficili da individuare e contrastare, dall'altro le misure di sicurezza di contrasto in essere non risultano essere ancora adeguate e sufficienti, neppure per i SI più critici e quindi più protetti. Questo comporta che tutti i SI, di qualsiasi dimensione, devono essere soprattutto **resilienti**, ossia essere in grado, comunque, di garantire la continuità operativa (business continuity), dei processi e delle attività fondamentali per il funzionamento dell'organizzazione.

4.2 Tipologie e tecniche di attacco emerse da OAD 2026

Le fig. 4.2-1 e 4.2-2 mostrano la **diffusione**, in percentuale, dei diversi **tipi di attacchi** subiti e rilevati tra il bacino di aziende/enti rispondenti, rispettivamente nell'intero anno 2025 e nel 1° quadrimestre 2026.

Come precisato all'inizio del presente capitolo, e dettagliato nell'Allegato A, OAD distingue nettamente "**il che cosa si attacca"** (indicata come "tipologia di attacco") dal **come si attacca** (indicata come "tecnica di attacco").

Nel questionario OAD sono considerate 15 diverse "famiglie di tipologie", e tra queste, dall'edizione dell'anno scorso, è inclusa la famiglia di **attacchi alle applicazioni e ai servizi ICT basati su IA, Intelligenza Artificiale.**

Nel 2025 le percentuali più alte, e quasi simili, riguardano l'attacco e/o uso non autorizzato di singoli sistemi ICT, fissi o virtualizzati, con un 23,76%, e le modifiche malevoli o non autorizzate alle configurazioni di sistemi ICT e delle applicazioni informatiche da questi supportati, con un 23,20%. Al terzo posto gli attacchi ai sistemi e servizi ICT terziarizzati, con un 20,99%. Al quarto posto si posiziona, con un 16,57%, la saturazione delle risorse ICT, ossia il DoS/DDoS, Denial of Service/Distributed Denial of Service, che può avvenire sia sui sistemi terziarizzati sia su quelli on premise, ossia operanti in locale.

Tutte le altre tipologie di attacco hanno percentuali in decremento dal 12% in giù. Interessante notare come:

- Gli attacchi ai sistemi/servizi/applicativi di Intelligenza Artificiale (IA) siano all'ultimo posto, con un 3,31%. Questa relativamente bassa percentuale potrebbe dipendere sia dalla diffusione ancora limitata di applicazioni proprie basate su IA presso le organizzazioni rispondenti, sia dalla difficoltà di individuare e riconoscere specifici attacchi ai sistemi e ai servizi basati su IA, in particolare quando questi sono erogati da fornitori esterni.
- Non trascurabile l'8,84% di attacchi alla supply chain informatizzata, tenendo conto che solo la metà circa delle organizzazioni rispondenti ne ha una; si veda anche fig. 6.2-9 sulla percentuale di rispondenti che hanno supply chain informatizzate.

- Analogo discorso per gli attacchi ai sistemi OT, Operational Technology[13]: il 9,39% dipende dal relativamente basso numero di organizzazioni rispondenti che dispone di questi sistemi.
- Risultano relativamente alte, rispetto alle edizioni precedenti, le percentuali sul furto di dispositivi ICT, sia fissi che mobili, rubati, e del furto di informazioni da questi dispositivi.



Fig. 4.2-1

Per **il 1°quadrimestre 2026**, che ha avuto un alto carico di attacchi come mostrato in fig. 4-4, la diffusione delle tipologie di attacco è **profondamente cambiata rispetto al 2025**, e con gli stessi rispondenti.

[13] Il termine **OT, Operational Technology**, indica un ampio insieme di sistemi ICT per controllare, monitorare ed automatizzare processi fisici ed i dispositivi e le infrastrutture che effettuano e/o supportano tali processi fisici. Tipici esempi di tali processi sono quelli manifatturieri, quelli chimici, quelli nucleari, quelli del controllo del territorio, delle reti di distribuzione dell'energia, del gas, dell'acqua, e così via. Rientrano nell'OT anche i robot ed i sistemi informatizzati/robotizzati di analisi e diagnosi medica, oltre che per le operazioni chirurgiche.

⚠ Al primo posto, con **il 55,41%**, il **furto di informazioni da singoli specifici sistemi fissi ICT** del Sistema Informativo (SI) anche terziarizzati/in cloud, tipologia di attacco che nel 2025 si posiziona al terz'ultimo posto con un **5,52%**. Questo significa che più della metà dei SI dei rispondenti ha subito attacchi digitali che hanno comportato un data breach con l'esportazione di informazioni dai **sistemi fissi**, non mobili.

È inoltre significativo che tutte le altre famiglie di attacco hanno percentuali inferiori al **14%**, e che l'attacco alle reti informatiche sia al secondo posto, come diffusione percentuale, con un 14,01% (nel 2025 6,63%). Al terzo posto la saturazione di risorse ICT con un **12,74%** (nel 2025 16,67%), ed al quarto, con un 12,1%, gli attacchi ai sistemi OT (nel 2025 9,39%)

Le fig. 4.2-3 e 4.2-4 riportano la **diffusione**, in percentuale, delle **tecniche di attacco** riscontrate nei più gravi attacchi subiti nel corso del 2025 e del 1° quadrimestre 2026.

Data la differenza e la molteplicità delle tecniche usate per i diversi attacchi, e la numerosità di questi ultimi, per avere risposte credibili si è richiesto nel questionario OAD 2026 di fare riferimento al più grave attacco subito.

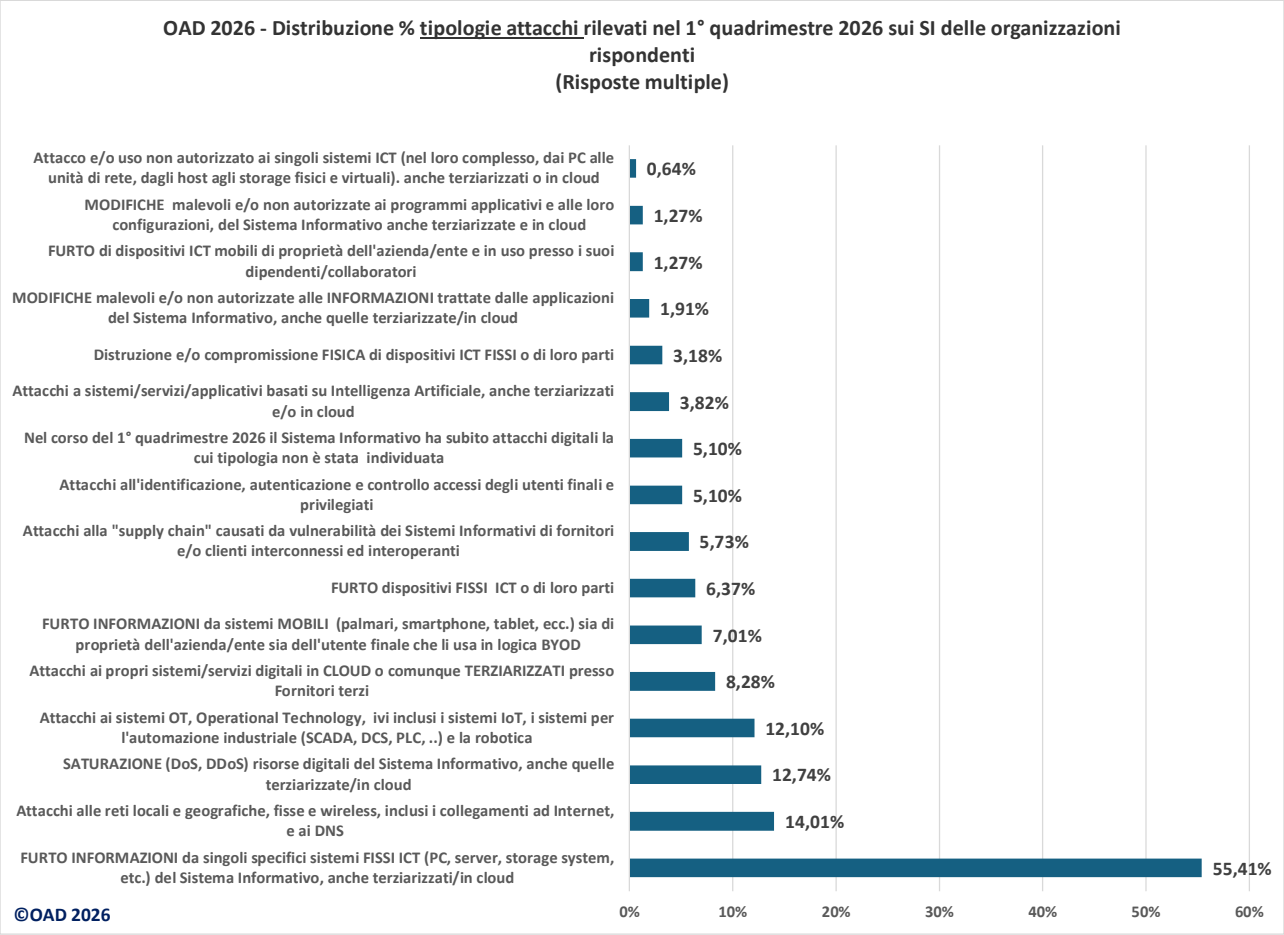


Fig. 4.2-2

Nelle fig. 4.1-3 e 4 emerge che risultano percentualmente pochi i rispondenti che non sanno fornire una risposta., o perché non hanno specifiche informazioni o perché non sono state individuate le tecniche usate per l'attacco più grave subito.

Sia per il 2025 che per il 1° quadrimestre 2026, l'uso di **più tecniche per lo stesso attacco digitale** risulta il metodo percentualmente più diffuso, rispettivamente con un **59,09%** ed un **57,14%**.

L'uso nello stesso attacco di più tecniche, sia in parallelo che sequenzialmente, è ormai una prassi consolidata, e non solo per gli attacchi più complessi e sofisticati.

Si parte da un "entry point", costituito normalmente da vulnerabilità personali di un utente, che fornisce involontariamente dati tramite tecniche di social engineering: ad esempio dal furto del cellulare con informazioni sui suoi account non protetti, o dall'apertura di e-mail di phishing con attivazione di un malware, e così via. L'entry point può essere fornito anche da vulnerabilità tecniche del sistema, che consentono l'inserimento e l'attivazione di un malware o di prendere il controllo del sistema "di ingresso". Con queste tecniche l'attaccante riesce ad entrare in una risorsa ICT del SI oggetto dell'attacco, e da qui analizzare le risorse e le loro vulnerabilità, individuando gli asset per lui più interessanti in funzione dei suoi scopi e da attaccare con le tecniche più idonee. Dopo questa analisi viene sferrato uno o più attacchi finali, talora in periodi diversi, qualora i gestori del SI non si fossero accorti di essere sotto attacco.

Come tecniche più diffuse al secondo posto si colloca, in entrambi i periodi, la **raccolta illegale di informazioni**, ottenute tipicamente con il **social engineering**, sfruttando la poca attenzione del soggetto interlocutore, con un **43,18** ed un **38,18%** rispettivamente. Nel 2025, al terzo posto, con il **21,59%,** si posiziona l'attacco fisico, e con una percentuale di poco inferiore, il **19,32%,** strumenti di attacco basati sull'Intelligenza Artificiale. Quest'ultima tecnica nel 1° quadrimestre 2026 è al terzo posto, con il **22,62%**, mentre gli attacchi fisici sono al quarto posto, con il **19,05%.**

L'Intelligenza Artificiale (IA) è ormai un potentissimo mezzo sia per gli attacchi digitali sia per gli strumenti di difesa: le organizzazioni rispondenti all'indagine OAD iniziano ad evidenziarlo. Si tenga conto che nella precedente edizione OAD 2025, quindi per l'anno 2024, l'IA come strumento di attacco aveva solo un **3,06%.** Nel 2025 è passata a **9,09%** e nel 1° quadrimestre 2026 a **17,86%.**

I due bacini di rispondenti sono almeno in parte diversi, ma una differenza così alta in percentuale indica come l'uso di IA si in forte crescita ed è pure aumentata la capacità delle organizzazioni di individuare l'IA come strumento di attacco.

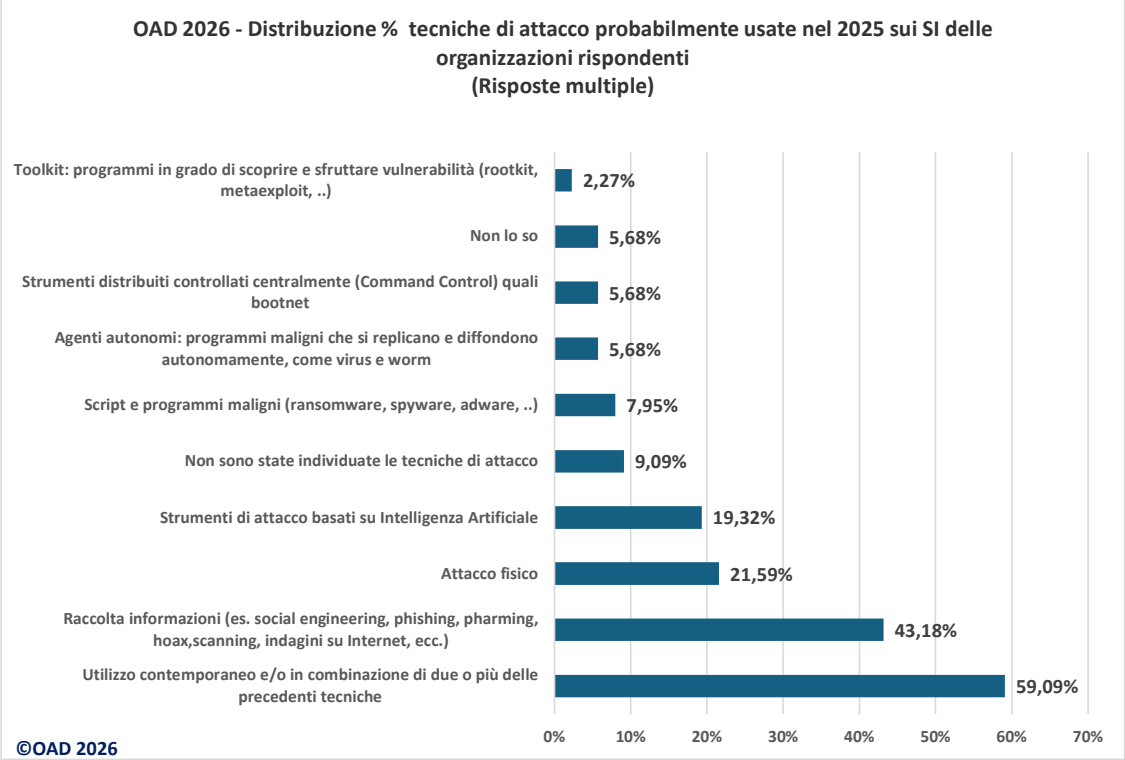


Fig. 4.2-3

Cresce la difficoltà di identificare le tecniche di attacco. La quota di rispondenti che non è stata in grado di individuare le tecniche utilizzate negli attacchi più gravi passa dal 3,49% nel 2024 al 9,09% nel 2025, raggiungendo il 17,86% nel primo quadrimestre 2026. Questa evoluzione potrebbe riflettere sia una crescente sofisticazione degli attacchi sia difficoltà nell'analisi e nella ricostruzione degli incidenti.

È opportuno ricordare nuovamente che i dati emersi dall'indagine OAD 2026 dipendono strettamente dall'insieme di aziende/enti che hanno risposto al questionario online. Questa indagine non intende, e non può, fornire dati in assoluto sul numero di attacchi portati in Italia per le varie tipologie e per gli strumenti di attacchi considerati. Sulla base dei rispondenti emergono indicazioni, soprattutto per le piccole e micro-organizzazioni, sui trend degli attacchi e degli strumenti di attacco.

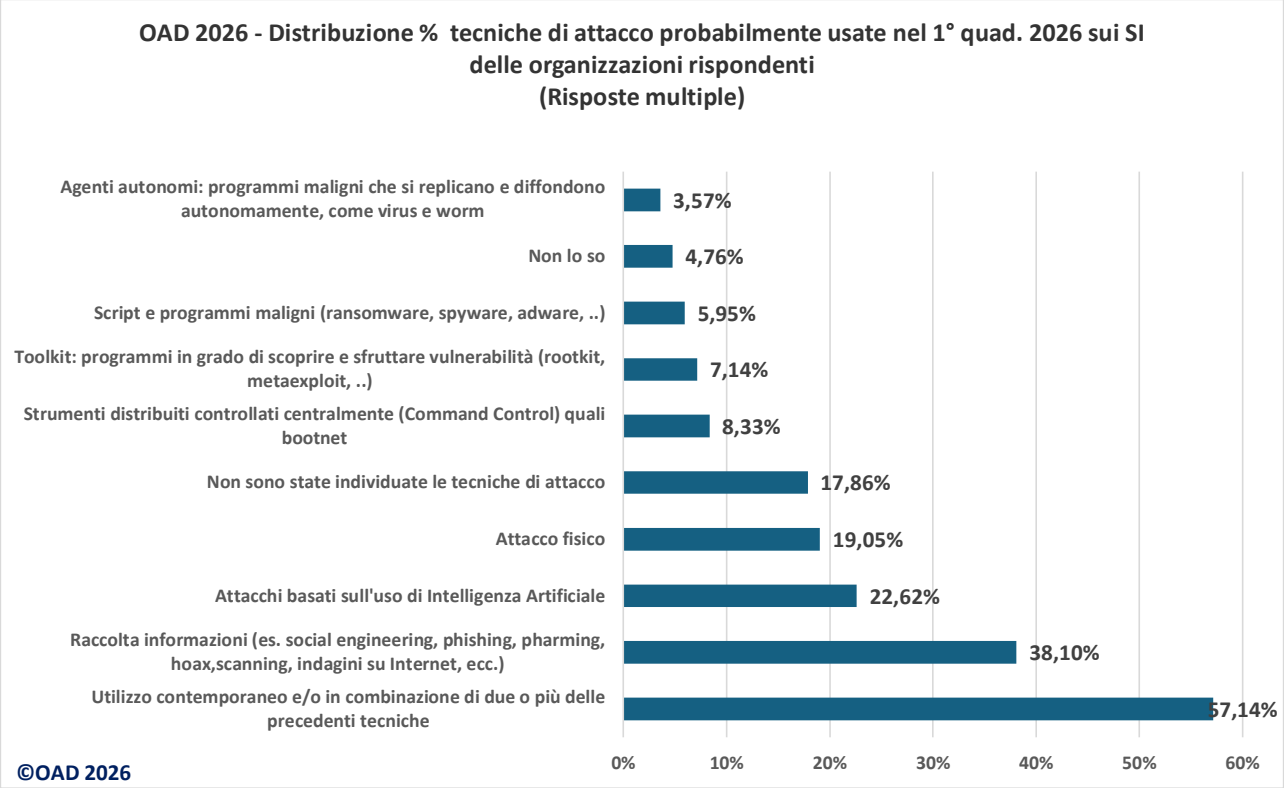

OAD 2026 - Distribuzione % tecniche di attacco probabilmente usate nel 1° quad. 2026 sui SI delle organizzazioni rispondenti
(Risposte multiple)
Agenti autonomi: programmi maligni che si replicano e diffondono autonomamente, come virus e worm
3,57%
Non lo so
4,76%
Script e programmi maligni (ransomware, spyware, adware, ..)
5,95%
Toolkit: programmi in grado di scoprire e sfruttare vulnerabilità (rootkit, metaexploit, ..)
7,14%
Strumenti distribuiti controllati centralmente (Command Control) quali bootnet
8,33%
Non sono state individuate le tecniche di attacco
17,86%
Attacco fisico
19,05%
Attacchi basati sull'uso di Intelligenza Artificiale
22,62%
Raccolta informazioni (es. social engineering, phishing, pharming, hoax,scanning, indagini su Internet, ecc.)
38,10%
Utilizzo contemporaneo e/o in combinazione di due o più delle precedenti tecniche
57,14%
0%
10%
20%
30%
40%
50%
60%
©OAD 2026

Fig. 4.2-4

5. Tipologie di attacchi digitali e tecniche di attacco più temute nel prossimo futuro

Come già evidenziato in §4 e nell'Allegato A, OAD distingue nettamente le tipologie di attacco, ossia che cosa si attacca, dagli strumenti di attacco. Questa logica viene applicata anche per richiedere quali sono gli **attacchi più temuti nel prossimo futuro 2027-2030**, e tendenzialmente le risposte sono influenzate, per chi ha risposto, dagli attacchi subiti nel 2025 e nel 1° quadrimestre 2026.

La fig. 5-1, con risposte multiple, mostra che per il **50,84%** la tipologia di attacco più temuta nel prossimo futuro è data dagli "**Attacchi ai propri sistemi in cloud o in hosting",** seguita con il **46,37%** dalle "**Modifiche non autorizzate ai dati e alle informazioni trattate dal sistema informativo"**. Al terzo posto, con il **33,52%** "**Uso non autorizzato di risorse ICT**".

Tutte le altre tipologie di attacco scendono a scalare in % sotto il 30%, ma con percentuali abbastanza alte.

Le prime tre tipologie di attacchi più temuti sono quelle che, pur in posizioni diverse, sono ai primi tre posti come diffusione negli attacchi rilevati nel 2025, come indicato nella precedente fig. 4.2-1.

Queste tre tipologie di attacco più temute evidenziano alcune delle principali preoccupazioni per la sicurezza digitale delle organizzazioni rispondenti: la protezione dei sistemi ICT e dei servizi ICT esternalizzati, soprattutto in cloud, la salvaguardia dell'integrità dei dai e delle informazioni trattate, il controllo sull'utilizzo delle risorse ICT. Ormai quasi tutti i sistemi informativi sono ibridi, ossia con applicazioni terziarizzate, e questo spiega l'alta percentuale di timori per attacchi in tali ambiti, che pur con elevati livelli di protezione non sono affatto immuni da attacchi digitali[14].

Questi timori riflettono la crescente dipendenza delle organizzazioni dai sistemi informativi e dai servizi digitali, la cui compromissione può determinare conseguenze rilevanti sulla continuità operativa, sull'affidabilità delle informazioni e sul funzionamento dei processi aziendali.

Le modifiche non autorizzate ai dati trattati da un sistema informativo è uno degli attacchi più gravi che si possano subire, dato che va ad **alterare i dati** che costituiscono un "asset", un bene aziendale, tra i più essenziali in questa epoca digitale, per qualsiasi tipo di organizzazione, pubblica o privata.

Per le altre tipologie di attacchi temuti nel prossimo futuro, da evidenziare che:

- l'attacco alla **supply chain,** tipologia introdotta per la prima volta nel questionario OAD 2024, raggiunge un non trascurabile **22,91%;** questa percentuale conferma la criticità di questo attacco individuato tra i primi più gravi rischi del futuro da ENISA;
- l'attacco ai **sistemi OT** è temuto da quasi il **20%** dei rispondenti, ed è un dato molto alto considerando che solo una piccola parte delle organizzazioni rispondenti utilizza sistemi OT;
- gli "**Attacchi a propri sistemi o a servizi di terze parti basati su Intelligenza Artificiale**", introdotti per la prima volta nel questionario OAD 2025, raggiungono un significativo **15%**, altra percentuale alta, considerando che molte delle organizzazioni rispondenti dichiarano di non utilizzare applicazioni basate su IA;
- rimangono alte le percentuali per il furto "fisico" di dispositivi ICT fissi e mobili, e dei dati in essi contenuti.

[14] Anche i principali provider di hosting e cloud, a livello mondiale, hanno subito attacchi digitali nonostante le potenti misure di sicurezza in essere, In Italia sono presenti numerosi provider di ben più piccole dimensioni, molti dei quali non hanno misure paragonabili a quelle dei "big". Indipendentemente dalle misure di sicurezza in essere, un'applicazione in hosting/cloud se ha delle vulnerabilità può comunque essere attaccata, si veda ad esempio OAD Insight #10 – Attacco e compromissione del sito web di una piccola azienda italiana in https://www.oadweb.it/it/comunita-oad/oad-insight/oad-insight-10-attacco-e-compromissione-del-sito-web-di-una-piccola-azienda-italiana.html.

La fig. 5-2, con risposte multiple, mostra **le famiglie di tecniche di attacco** più temute per il prossimo futuro.

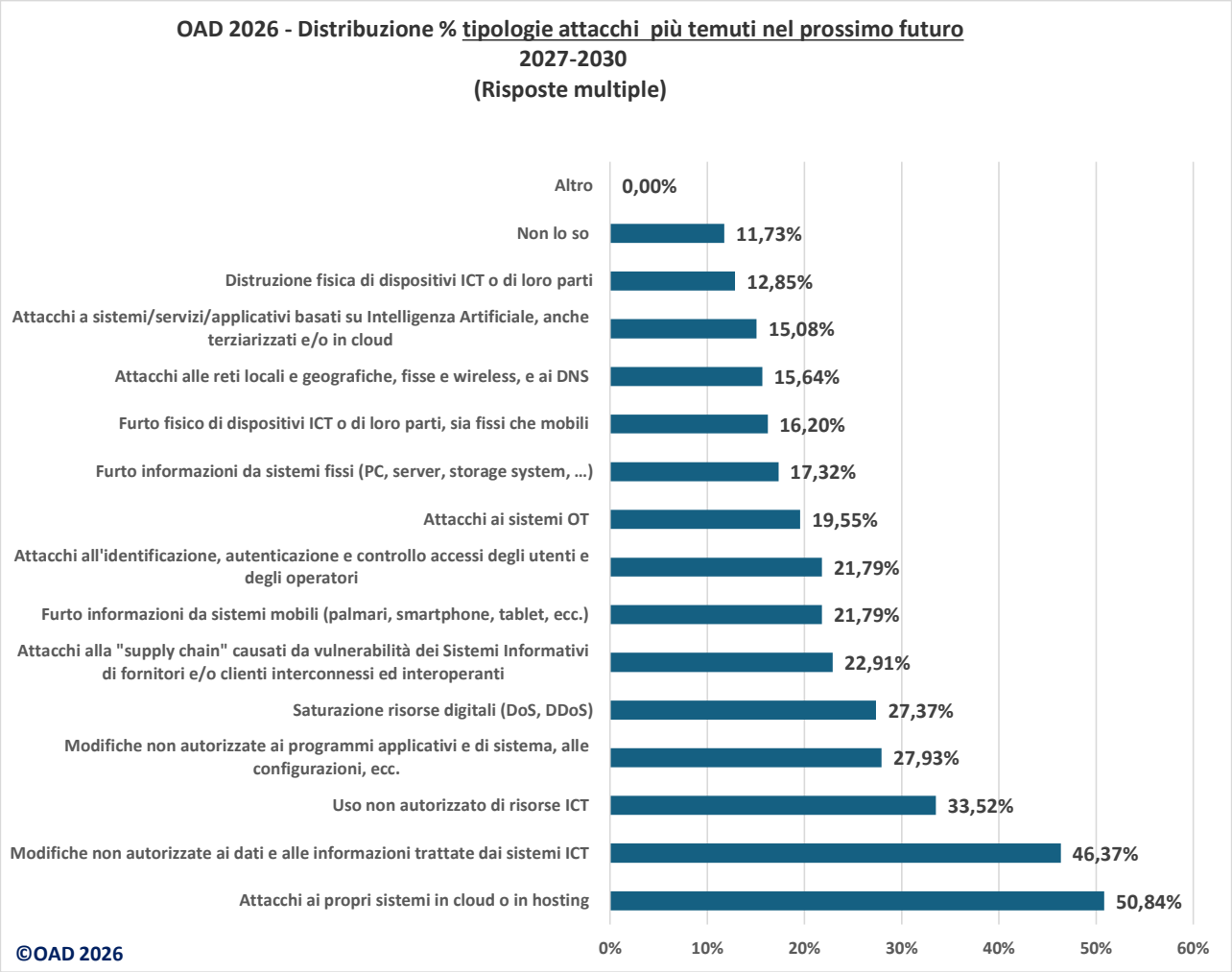


Fig. 5-1

Al primo posto, con un **73,74%**, l'uso di "**Strumenti di attacco basati su Intelligenza Artificiale**", una percentuale nettamente superiore a quella delle altre tecniche considerate. Questo risultato evidenzia una forte preoccupazione per l'utilizzo dell'IA da parte degli attaccanti, sia per automatizzare e rendere più veloci ed efficaci gli attacchi, o alcune delle loro fasi, sia per sviluppare tecniche di ingegneria sociale più sofisticate e difficilmente riconoscibili. È bene evidenziare che questo dato esprime la percezione dei rischi futuri da parte dei rispondenti, e non la diffusione effettiva di tali strumenti negli attacchi già subiti.

Al secondo posto segue con un 60,34% "**l'utilizzo di più tecniche**", come ormai avviene per la maggior parte degli attacchi digitali; ed infatti questa modalità di attacco risulta la più diffusa anche per gli attacchi subiti, come evidenziato nella fig. 4.1-2.

Al terzo posto, con un 46,37%, si pone la "**Raccolta non autorizzata di informazioni**", tipicamente con tecniche di social engineering, che costituiscono uno dei principali entry point per un attacco digitale. Gli altri strumenti di attacco hanno percentuali gradualmente decrescenti, a partire dal 20%, con valori comunque non trascurabili.

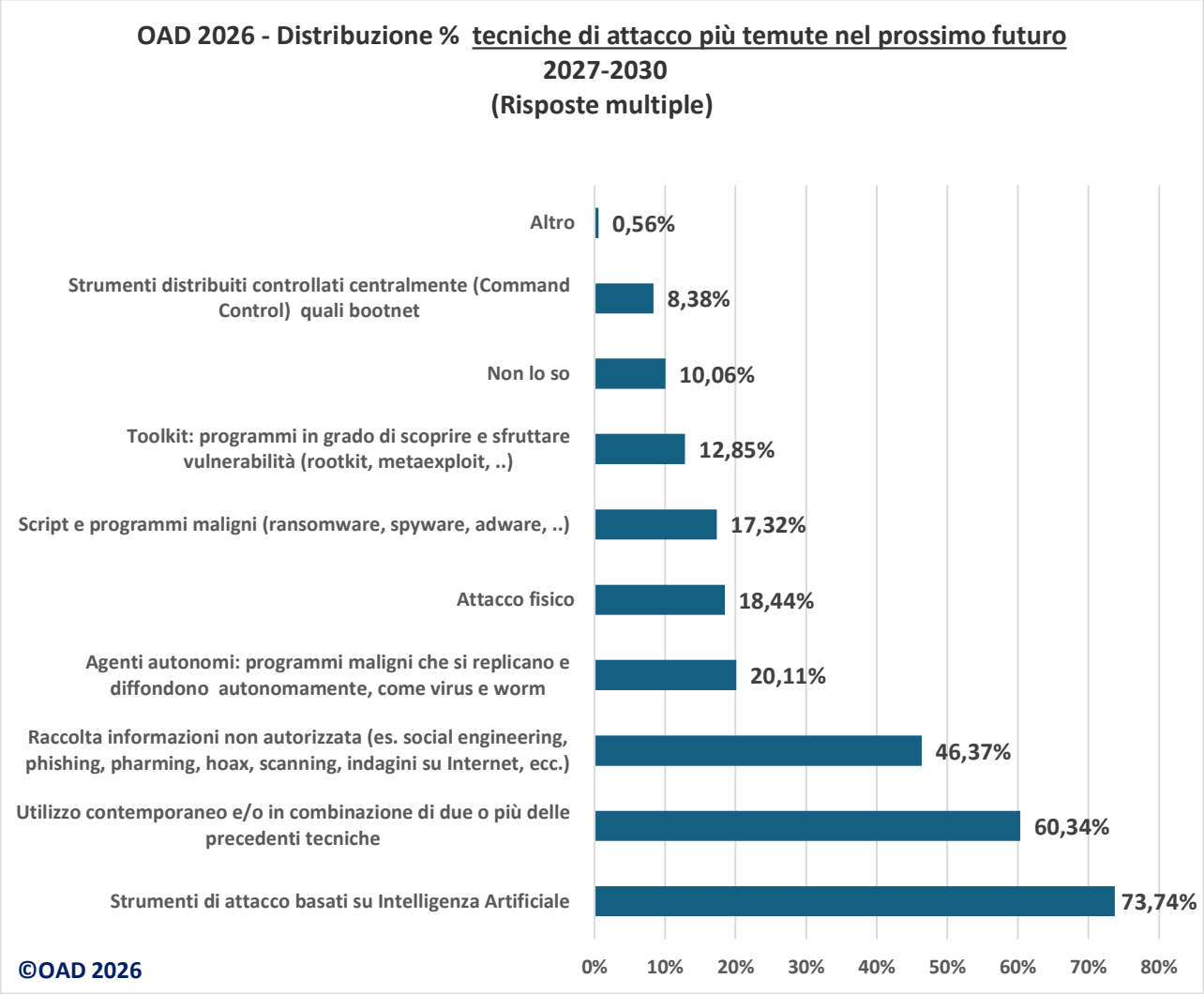


Fig. 5-2

La fig. 5-3, con risposte multiple, evidenzia le **possibili motivazioni** ipotizzate per gli attacchi digitali più temuti del prossimo futuro. In cima alla lista **le frodi**, con un 71,19%, seguite con il 56,50% dal **ricatto** e con il 52,54% dal **sabotaggio**. Al quarto posto si posiziona in questa classifica **l'hacktivism** con il 45,76%, seguito dalla **guerra digitale** con il 31,64%.

Percentuali abbastanza alte, considerando che il campione emerso di aziende/enti rispondenti include per più della metà dei rispondenti medie e piccole organizzazioni, ed il numero di Pubbliche Amministrazioni, tipici target per hacktivism e guerre digitali, hanno purtroppo risposto in numero relativamente limitato.

Quest che per il futuro le aziende/enti rispondenti iniziano ad essere preoccupate, oltre che da attacchi causati da frodi, ricatti e sabotaggi, anche da quelli causati dall'attivismo ideologico (che talvolta sconfina nel fanatismo) e dalle guerre digitali che si stanno ampliando con le crescenti tensioni geopolitiche a livello mondiale e dalle guerre in atto. Hacktivism e guerre digitali possono infatti effettuare attacchi "di massa", che investono anche piccole organizzazioni.

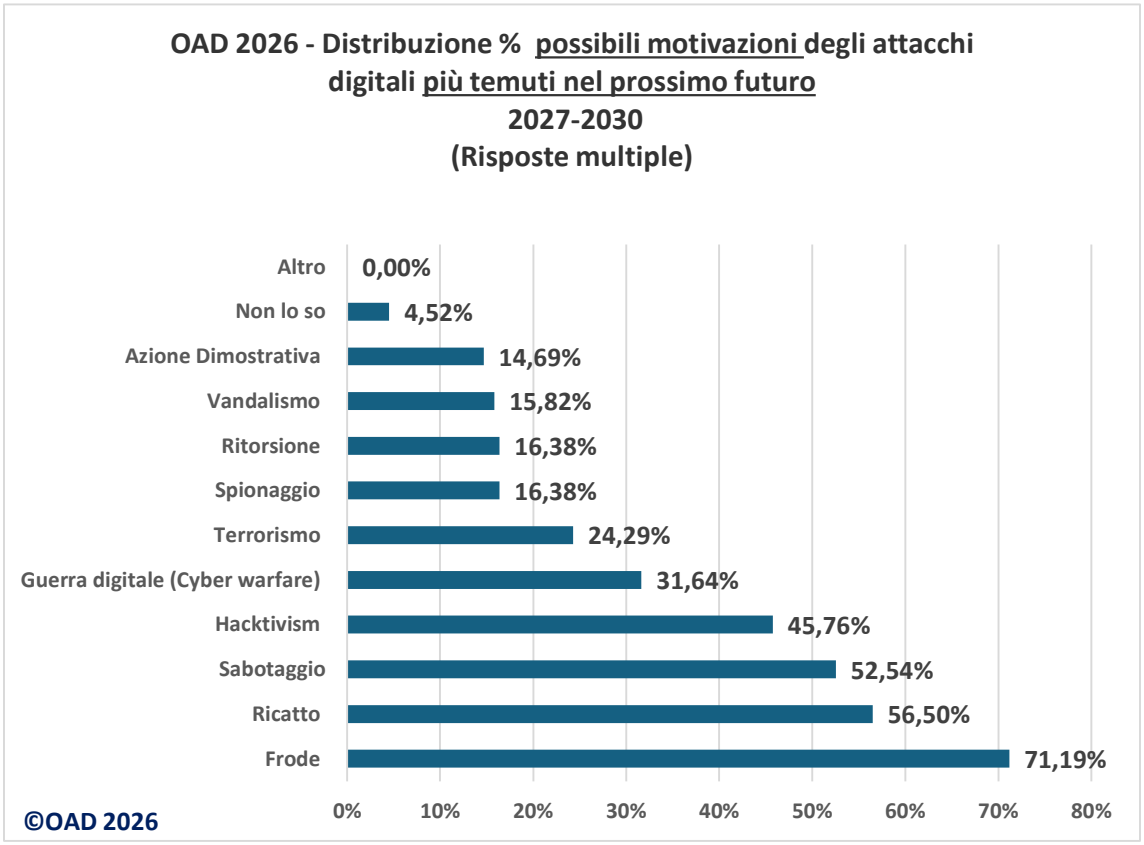


Fig. 5-3

⚠ I risultati emersi sulle minacce digitali più temute nel prossimo futuro evidenziano tre tendenze significative:

- crescente preoccupazione per l'IA, i cui strumenti di attacco sono temuti dal 73,74% dei rispondenti;
- centralità della sicurezza dei sistemi terziarizzati/cloud e dell'integrità dei dati;
- aumento dei timori sulle motivazioni degli attacchi.

Le risposte suggeriscono una percezione delle future minacce ICT nella quale ai rischi e agli impatti economici e operativi si affiancano quelli associati alle nuove tecnologie e alle tensioni geopolitiche.

6. Il campione delle organizzazioni rispondenti e dei loro Sistemi Informativi emerso dall'indagine OAD 2026

Il presente capitolo fornisce una macro-descrizione dei Sistemi Informativi (SI) delle aziende/enti rispondenti, e delle aziende/enti stesse. Questa rilevazione consente di contestualizzare le misure di sicurezza digitale poste in essere per contrastare i possibili attacchi digitali e quelli effettivamente rilevati descritti in §4, mentre le misure di sicurezza, tecniche ed organizzative, in essere nei SI dei rispondenti sono analizzate in §7.

Le risposte avute al questionario OAD 2026 sono state 309, sostanzialmente dello stesso ordine di grandezza rispetto alle precedenti edizioni delle indagini OAD.

6.1 L'Azienda/Ente rispondente

La fig. 6.1-1 mostra la distribuzione percentuale dei rispondenti per le macro-famiglie dei settori merceologici considerati.

Due i macrosettori che più hanno contribuito con le loro risposte a OAD 2026: il mondo dell'istruzione e quello ICT. Per il primo fondamentale è stata la collaborazione di OAD con AICA, analogamente a quanto successe con l'edizione OAD 2024. Tutti gli altri settori hanno registrato valori percentuali assolutamente inferiori alle attese, nonostante ci fossero associazioni patrocinanti specifiche per taluni settori.

Rispetto agli anni precedenti, il settore industriale manifatturiero ha valori significativamente inferiori. Questa è una ulteriore conferma della difficoltà nel far compilare un questionario online pur semplificato come numero e tipo di domande, e pur con significati servizi per chi lo completa: servizi gratuiti offerti da AICA e di interesse per una ben più ampia potenziale platea di rispondenti.

Si rammenta poi, come già dettagliato nel Capitolo 2, che il campione OAD è costituito da rispondenti che hanno partecipato volontariamente all'indagine e che non è, e non può essere, rappresentativo della distribuzione delle organizzazioni italiane per settore e/o dimensione.

La fig. 6.1-2 mostra la ripartizione delle aziende/enti rispondenti in base al numero di dipendenti, possibilmente come valore medio anno per il 2025.

Come dimensioni di un'organizzazione per numero di dipendenti, come per le ultime edizione di OAD, il questionario 2026 ha considerato tre classi per organizzazioni con meno di 250 dipendenti, nell'ambito privato le PMI, Piccole Medie Imprese: fino a 10, tra 11 e 50, tra 51 e 250. Per le organizzazioni maggiori dimensioni si sono considerate analogamente tre classi: tra 251 e 1000, tra 1001 e 5000, con più di 5000 dipendenti

Hanno risposto il 63,67% di piccole e medie organizzazioni, ossia quelle fino a 250 dipendenti (le PMI, Piccole Medie Imprese, in ambito aziende private), confermando ormai una tradizione dell'indagine OAD che fin dalla sua prima edizione, è riuscita a coinvolgere tra i suoi rispondenti le piccole e piccolissime organizzazioni.



Fig. 6.1-1

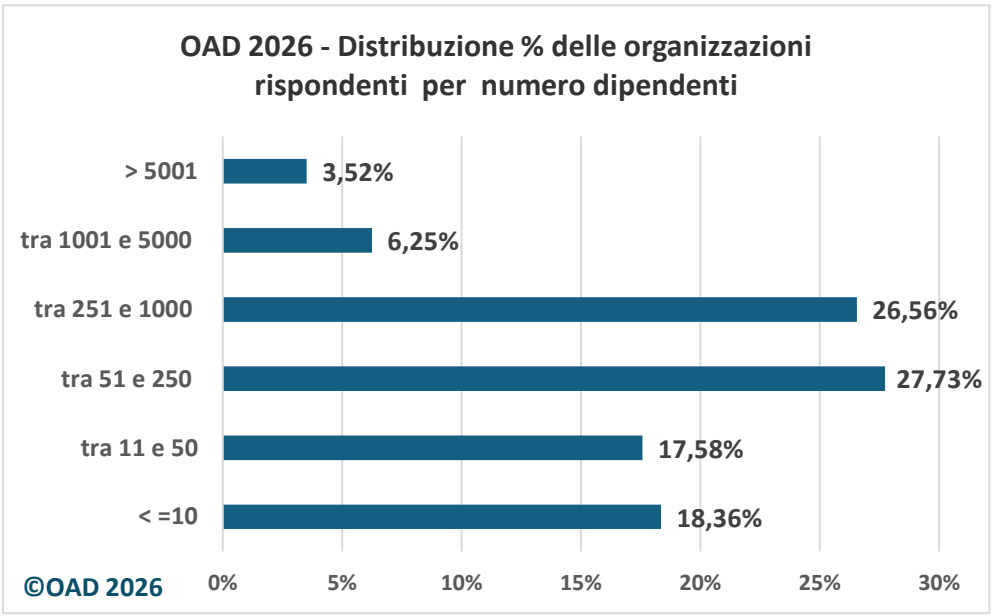


Fig. 6.1-2

La fig. 6.1-3 mostra la ripartizione delle aziende/enti rispondenti in base al loro ultimo fatturato, e per le PA per le entrate del loro ultimo bilancio.

La percentuale più alta, 35,66%, è data da aziende/enti che non possono/vogliono fornire questo dato, pur con la totale anonimità realmente garantita da OAD.

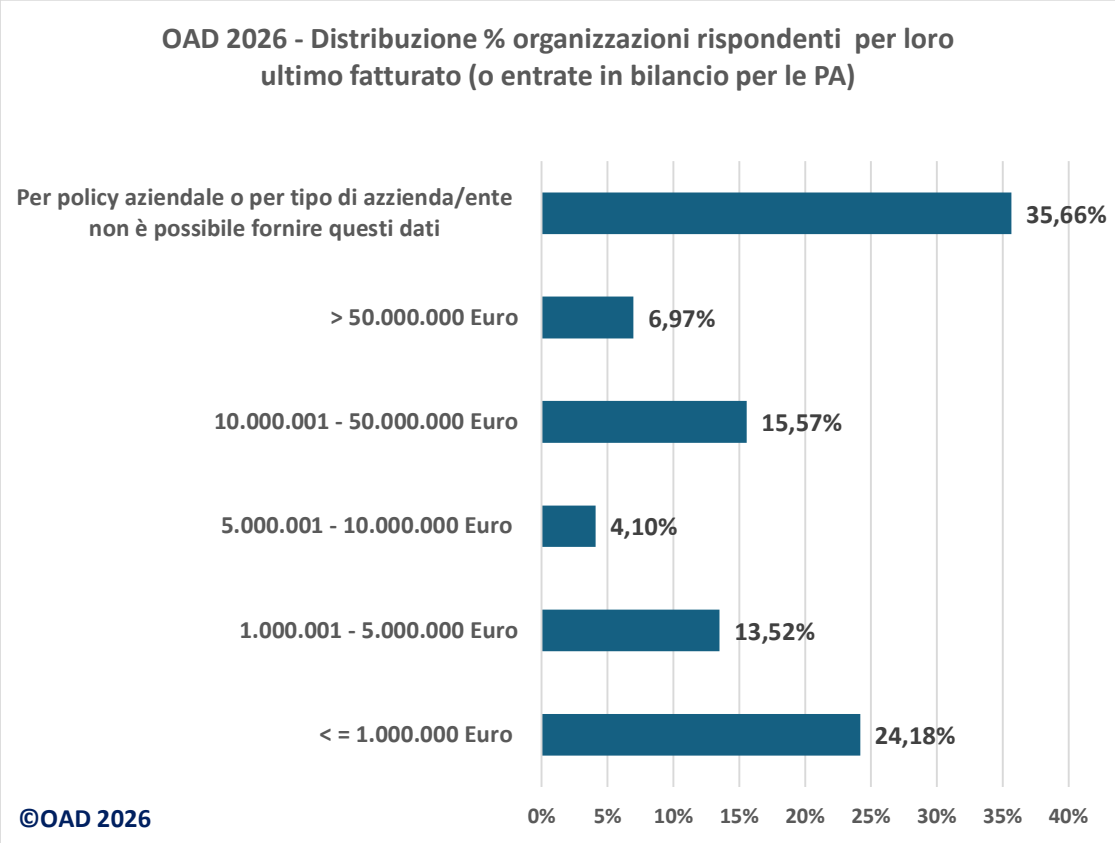


Fig. 6.1-3

6.2 Tipologie, ruoli e principali caratteristiche dei Sistemi Informativi delle organizzazioni rispondenti

La fig. 6.2-1 mostra la tipologia dimensionale del SI oggetto delle risposte al questionario OAD 2026.

La suddivisione dei SI a livello dimensionale fa riferimento al numero di utenti dello stesso, tipicamente quelli registrati, ossia con uno specifico account individuale, ed indipendentemente dal loro ruolo, interno o esterno all'organizzazione. Nella domanda si sono considerate le seguenti classi:

- SI medio/piccolo: decine di utenti; sono il 28,32% del totale dei rispondenti;
- SI medio-grande; centinaia di utenti; sono il 37,57% del totale dei rispondenti;
- Grande SI a livello nazionale: migliaia di utenti; sono il 24,28% del totale dei rispondenti;
- SI a livello nazionale che fa parte di una multinazionale e del SI di quest'ultima: in totale migliaia di utenti; sono il 9,83% del totale dei rispondenti.

Complessivamente **più del 70%** dei rispondenti dichiara di **far riferimento ad un SI di medie o grandi dimensioni**, con centinaia o migliaia di utenti

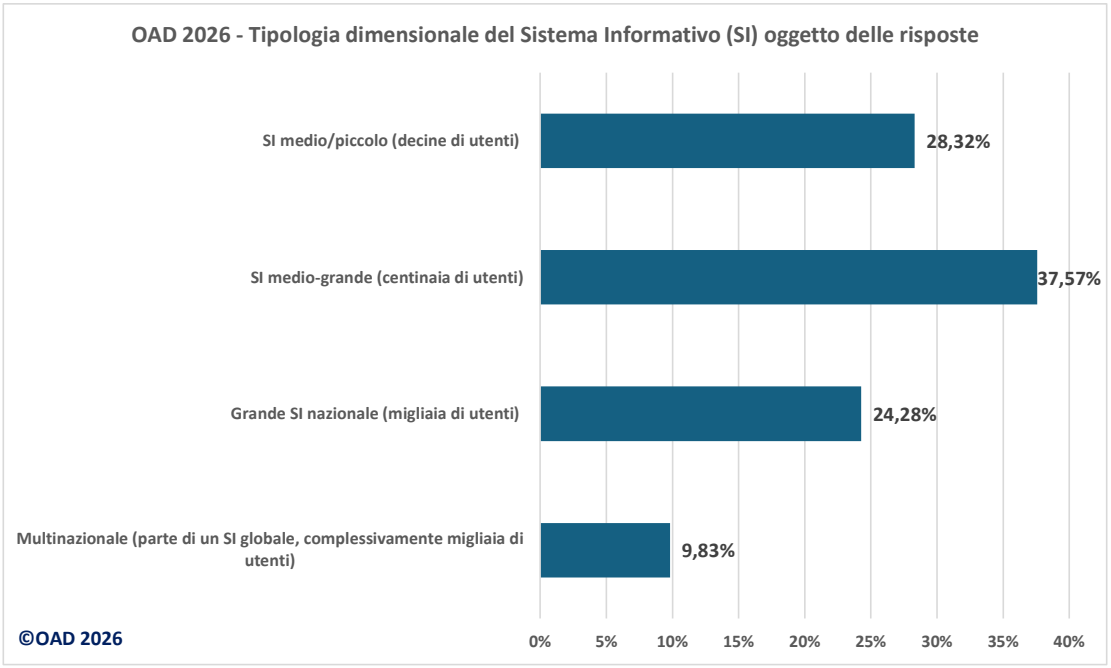


Fig. 6.2-1

Questo dato viene confermato dalla fig. 6.2-2, che evidenzia come il 41,52% delle organizzazioni disponga almeno di un Data Center[15], in Italia o all'estero.

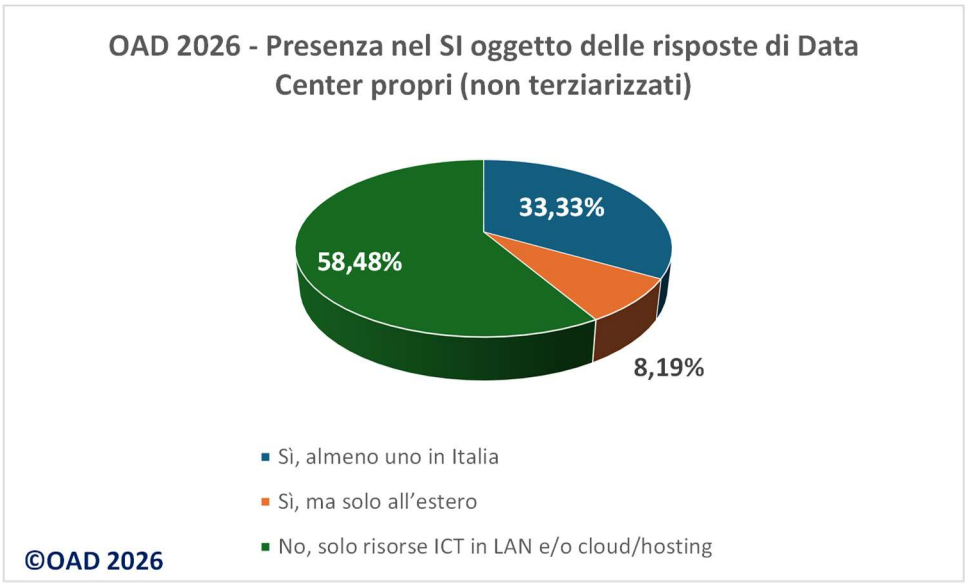


Fig. 6.2-2

[15] Il Data Center, in italiano definito anche come CED, Centro Elaborazioni Dati, è il luogo fisico dove sono centralizzati server, storage ed apparati di rete, ed al quale si collegano i sistemi ICT dipartimentali distribuiti sul territorio. Un grande SI può avere più Data Center. Un medio o piccolo SI non ha normalmente un Data Center, ma il più delle volte uno o più locali ove sono posti i sistemi ICT "centrali" operanti presso quella sede fisica. Questi locali sono sovente chiamati con il termine di "computer room".

La fig. 6.2-3 mostra che la stragrande maggioranza delle organizzazioni rispondenti, il 95,35%, gestisce in Italia il proprio SI, o la parte operante in Italia nel caso di un SI di una multinazionale.

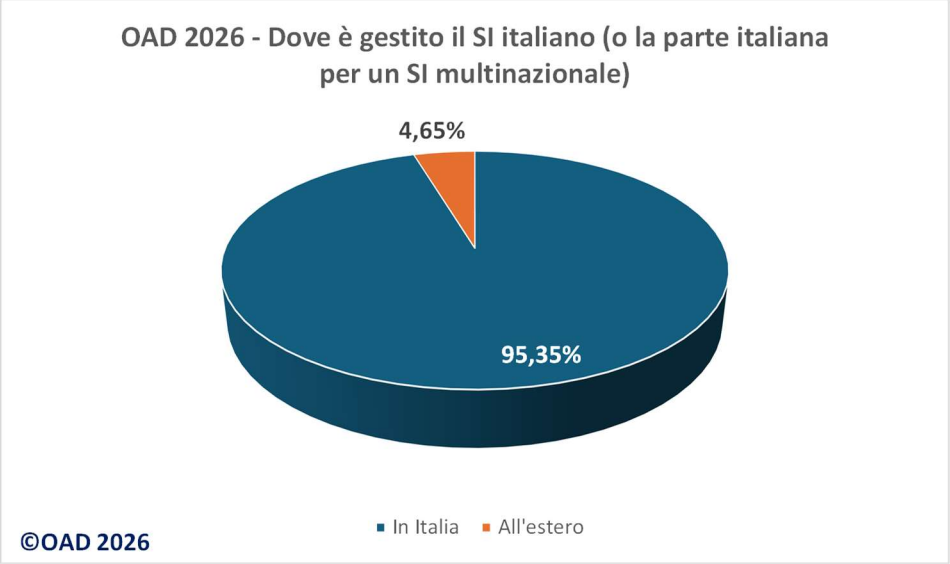


Fig. 6.2-3

La fig. 6.2-4 mostra, come distribuzione percentuale delle risposte avute, dove è situata in Italia, a livello regionale, la sede principale del SI (non la sede principale dell'organizzazione!), che può contenere un Data Center o una computer room "primaria". La figura elenca le regioni in ordine alfabetico.

La maggior parte dei "centri" dei SI delle aziende/enti rispondenti è in Lombardia, con un 23,67%, cui seguono, percentualmente a distanza, il Veneto con un 10%, e tutte le altre regioni, a scalare, con percentuali inferiori all'8%.

Si noti come questo dato è solo indicativo sulle organizzazioni che hanno risposto, e non è particolarmente significativo sul fenomeno degli attacchi digitali. Ha quindi una valenza statistica per OAD 2026 sull'ubicazione del "centro" del SI delle organizzazioni rispondenti.

È bene poi evidenziare come tale distribuzione % fa riferimento solo a chi ha risposto al questionario OAD 2026, e non è una indicazione assoluta di dove in Italia si concentrano i Data Center o le computer room principali.

La fig. 6.2-5 indica l'effettiva importanza del Sistema informativo (SI) per l'espletamento delle attività e del business delle organizzazioni rispondenti.

Il livello di importanza viene classificato secondo queste tre voci:

- **essenziale**: le attività più importanti sono tutte on line e dipendono dal corretto funzionamento del SI
- **importante**: le principali attività/processi non dipendono totalmente dal buon funzionamento del SI
- **di supporto**: alle attività ed ai processi dell'azienda/ente.

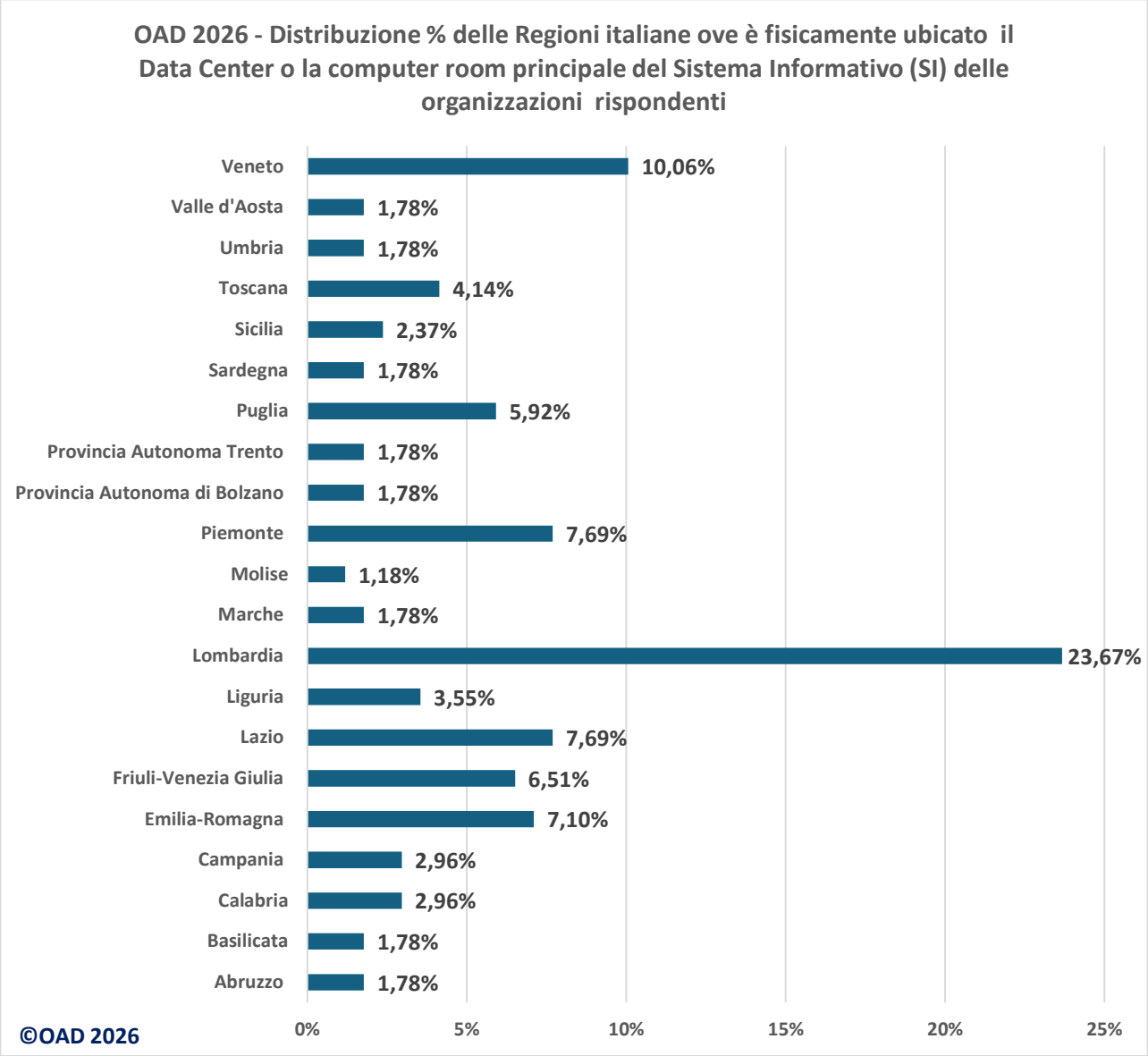

OAD 2026 - Distribuzione % delle Regioni italiane ove è fisicamente ubicato il Data Center o la computer room principale del Sistema Informativo (SI) delle organizzazioni rispondenti
Veneto 10,06%
Valle d'Aosta 1,78%
Umbria 1,78%
Toscana 4,14%
Sicilia 2,37%
Sardegna 1,78%
Puglia 5,92%
Provincia Autonoma Trento 1,78%
Provincia Autonoma di Bolzano 1,78%
Piemonte 7,69%
Molise 1,18%
Marche 1,78%
Lombardia 23,67%
Liguria 3,55%
Lazio 7,69%
Friuli-Venezia Giulia 6,51%
Emilia-Romagna 7,10%
Campania 2,96%
Calabria 2,96%
Basilicata 1,78%
Abruzzo 1,78%
0% 5% 10% 15% 20% 25%
©OAD 2026

Fig. 6.2-4

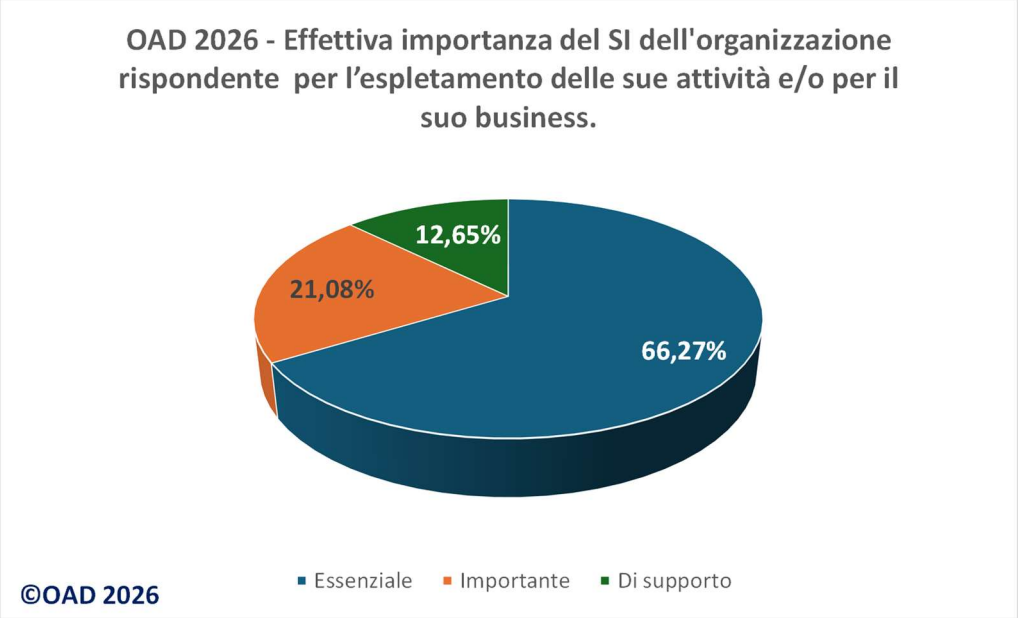


Fig. 6.2-5

È molto significativo che ben i **2/3 delle organizzazioni** rispondenti considerino **essenziale il loro SI** per il funzionamento delle loro attività. È una chiara indicazione della forte dipendenza di gran parte delle organizzazioni rispondenti dalle tecnologie digitali.

La Fig. 6.2-6 fa riferimento al trattamento dei dati ed informazioni personali da parte del Sistema Informativo (SI) dell'azienda/ente, almeno nella sua parte gestitala in Italia, nel caso di ambienti multinazionali. Il trattamento dei dati personali e da anni oggetto della normativa europea GDPR, ed ha un forte impatto sulle misure di sicurezza digitali richieste.

La domanda nel questionario prevedeva tre possibili risposte:

- Il SI tratta o può trattare dati "sensibili" per la privacy e quindi da proteggere fortemente;
- Il SI tratta dati personali ma non "sensibili", e comunque soggetti alla normativa privacy del GDPR;
- Il SI NON tratta dati personali

Il concetto di dato personale "**sensibile**" non è ripreso dal GDPR, ma rimane un elemento determinante per la protezione dei dati personali, e quindi soggetti alle normative sulla privacy. I dati personali "sensibili" includono i dati genetici, i dati biometrici, i dati relativi alla salute, i dati di orientamento politico, sindacale, filosofico, sessuale e di genere.

La figura evidenzia che per **quasi il 95%** dei rispondenti, il loro SI tratta, o può trattare, anche dati personali, e che quindi dovrebbe seguire quanto imposto dalla normativa GDPR anche in termini di sicurezza digitale. Il condizionale è d'obbligo, in quanto il trattamento di dati personali non dimostra di per sé la conformità normativa, e probabilmente una parte di questi rispondenti di fatto non è conforme.

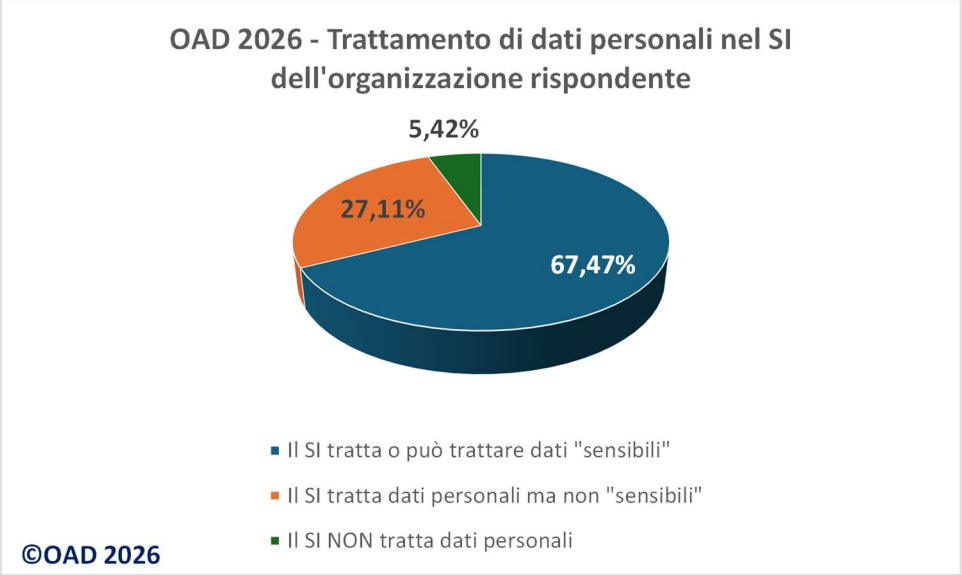


Fig. 6.2-6

La fig. 6.2-7 fa riferimento ad altre informazioni riservate e/o critiche trattate dal SI dell'organizzazione rispondente, e richiede se è un soggetto della normativa europea **NIS2**.

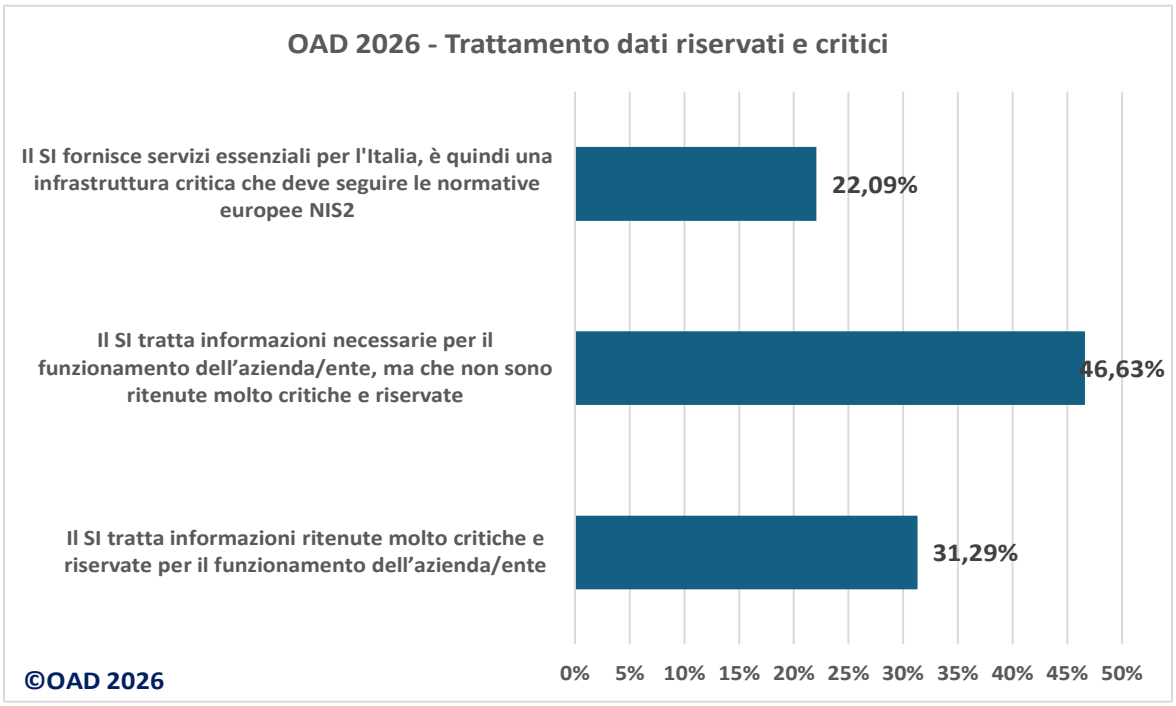


Fig. 6.2-7

Le informazioni molto critiche e riservate per il funzionamento dell'azienda/ente includono, ad esempio, segreti industriali, documenti strategici a livello nazionale/internazionale, accordi commerciali, gare d'appalto ed offerte di elevato valore economico.

Le organizzazioni che erogano e gestiscono servizi essenziali ed infrastrutture critiche per il sistema paese sono incluse tra i "soggetti" (essenziali o importanti) che devono seguire la normativa europea NIS2, in Italia

impostata, supervisionata e controllata da ACN secondo il D.Lgs 138/2024 e le varie “Determinazioni” che la stessa ACN emana. In generale i soggetti della NIS2 sono le diverse organizzazioni partenenti ai settori previsti dal decreto sopra citato.

Nel bacino di rispondenti emersi con l’indagine OAD 2026, il 22,09%, più di 1/5 del totale, è un soggetto NIS2, che quindi deve avere un elevato livello di sicurezza digitale congruente coi rischi ICT cui è soggetto, mentre il 46,63% non tratta informazioni particolarmente critiche e riservate.

Un’altra importante caratteristica di un moderno SI è l’uso di risorse ICT terziarizzate, quindi hosting e tipicamente i servizi in cloud.

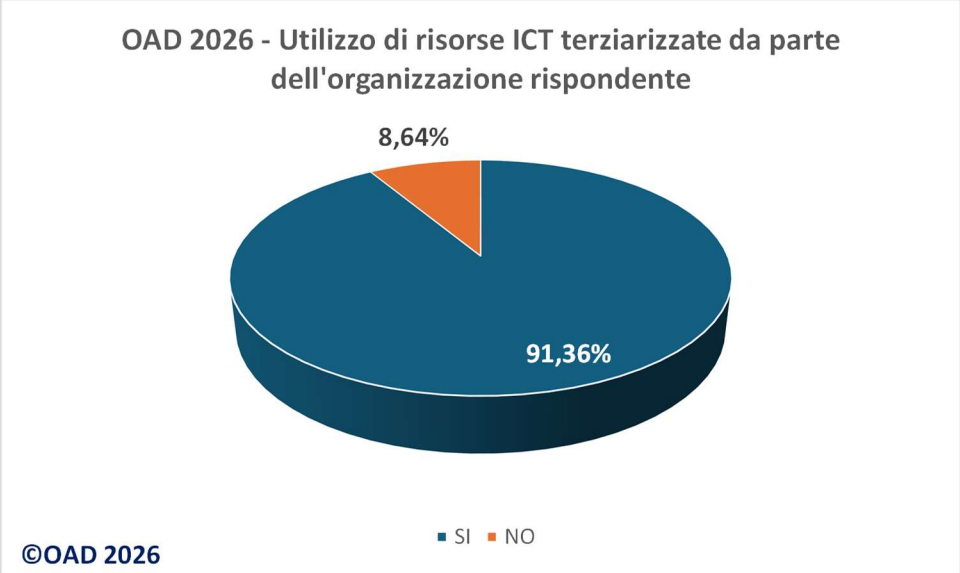


Fig. 6.2-8

La stragrande maggioranza delle organizzazioni rispondenti, il **91,36%**, utilizza anche risorse ICT terziarizzate, confermando la crescente diffusione di modelli di gestione dei Sistemi Informativi basati, in misura diversa, su servizi esterni, quali hosting e cloud. Tale evoluzione comporta una crescente dipendenza da fornitori ICT e rende particolarmente importanti la valutazione della sicurezza dei servizi acquisiti, la gestione delle responsabilità condivise e la continuità operativa.

La tendenza, soprattutto per le piccole organizzazioni, è quella di usare sistemi, applicazioni e servizi ICT in cloud, soprattutto come SaaS (Software as a Service). Alcune organizzazioni tendono quindi ad avere il loro SI completamente terziarizzato tra più fornitori, il così detto multi-cloud.

Ulteriore aspetto significativo di un moderno SI è la sua interazione e la sua interoperabilità con i SI dei suoi fornitori e talvolta anche con i suoi principali clienti, creando una "supply chain" informatizzata. Aspetto significativo anche in termini di sicurezza digitale, in quanto attacchi ad un SI avvengono anche tramite la supply chain, partendo da un SI meno sicuro e con vulnerabilità per accedere a quello target ben più sicuro.

La fig. 6.2-9 indica che poco più della metà dei rispondenti, 50,62%, ha realizzato una supply chain informatizzata, ma di questi circa il 42% la utilizza solo con alcuni interlocutori.

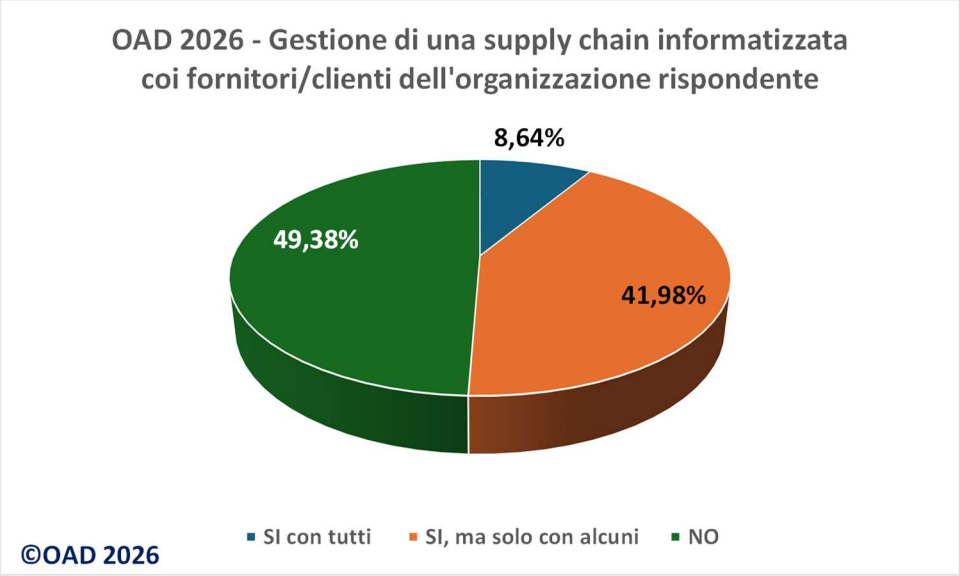


Fig. 6.2-9

6.2.1 Ruolo della persona rispondente

La fig. 6.2.1-1 mostra la ripartizione % del ruolo professionale di chi ha compilato il questionario online OAD 2026 per l'organizzazione per la quale opera.

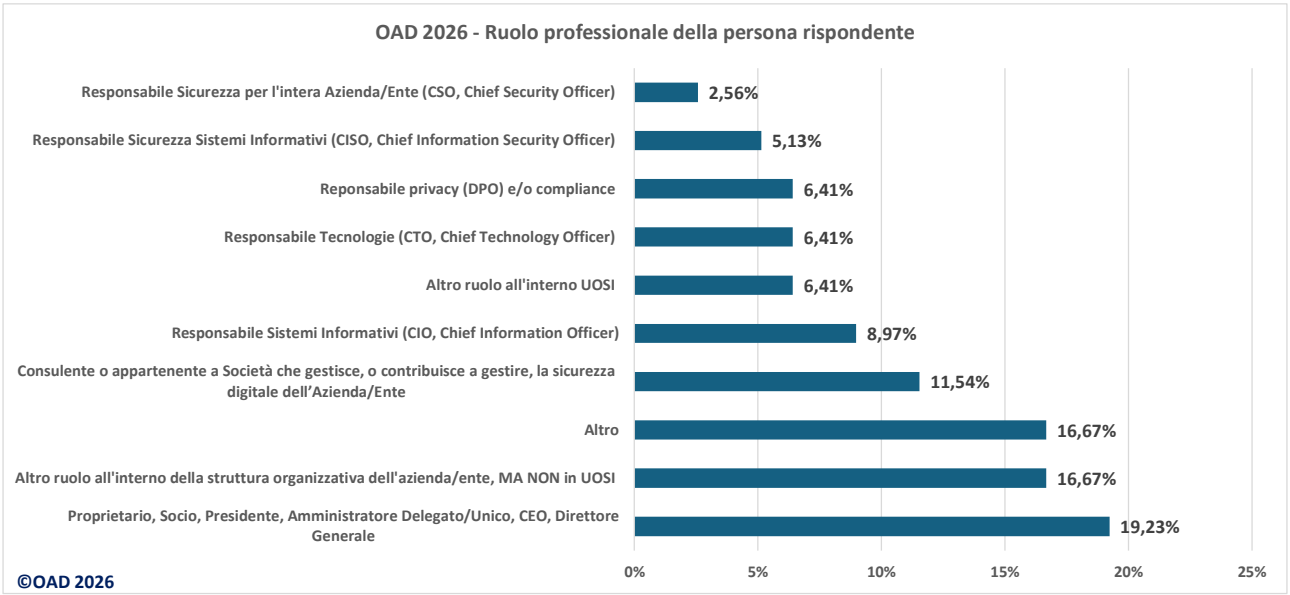


Fig. 6.2.1-1

Al primo posto, con il 19,23%, il proprietario/socio o i vertici manageriali dell'azienda/ente, al secondo posto, con un 16,67%, personale della struttura dell'organizzazione ma che non appartiene a ruoli nell'ambito UOSI, Unità Organizzativa Sistemi Informativi, o correlati ad essa, come il CISO, il CSO, il CTO, il DPO.

L'alta percentuale di proprietari/soci deriva dall'alta percentuale di organizzazioni rispondenti con meno di 50 dipendenti, come negozi, studi professionali, officine e piccole fabbriche, piccole PAL, dove chi decide sul sistema informativo, per quanto piccolo possa essere, è la proprietà o chi dirige e controlla l'intera organizzazione.

Al terzo posto "Altro": in questa voce molti hanno inserito il ruolo di consulente, di dirigente, di quadro, di leader o staff per la formazione ICT, di progettisti e di sviluppatori software.

Al quarto posto, con il 11,54%, la persona "esperta", consulente autonomo o dipendente di una società specializzata, cui l'azienda/ente rispondente ha terziarizzato, in toto o in parte, la gestione del sistema informativo e/o della sua sicurezza. Questo dato conferma la tendenza alla terziarizzazione della gestione operativa del SI (o di una sua parte) oltre che della sua cybersicurezza.

Il ruolo del responsabile del SI, il CIO, è solo al quinto posto con un 8,97%, ed al penultimo posto il CISO, con il 5,13%.

Queste due figure dovrebbero essere ai primi posti nel compilare un questionario sulla sicurezza digitale, ma in Italia sia il CIO che il CISO sono ruoli presenti e ufficializzati prevalentemente nelle medio-grandi organizzazioni. E più del 60% delle organizzazioni rispondenti a OAD 2026 sono medio-piccole.

L'autore si sarebbe aspettato, ed augurato, per queste figure qualche punto percentuale in più.

La fig. 6.2.1-1 evidenzia una caratteristica dell'indagine OAD, e non solo di questa edizione 2026: le risposte non provengono soltanto dagli specialisti della cybersecurity, ma anche da imprenditori, dirigenti, consulenti e personale con responsabilità differenti.

Questa caratteristica implica che il ruolo del compilatore potrebbe influenzare la conoscenza degli attacchi effettivamente subiti e delle misure di sicurezza adottate. Ovviamente la conoscenza e la competenza di un CIO o di un CISO sulla sicurezza digitale differiscono da quelle di un imprenditore, o di un avvocato, o di un notaio. Ma il fatto che anche queste figure professionali rispondano al questionario OAD, che ha quasi tutte le risposte predefinite e da selezionare, significa che nel farlo queste persone acquisiscono conoscenza dei problemi, delle conseguenze e delle possibili soluzioni nel campo della sicurezza digitale.

È un modo di creare "cultura" in questo campo, ed è questo l'obiettivo primario di OAD, che dal 2026 affianca all'indagine annuale altre iniziative, come la rubrica settimanale **OAD Insight**, si veda: https://www.oadweb.it/it/comunita-oad/oad-insight.html

7. Le misure di sicurezza in essere nei Sistemi Informativi dei rispondenti

Nel questionario dell'indagine OAD 2026 le domande sulle misure di sicurezza erano opzionali, si potevano cioè saltare, anche se erano raccomandate perché i rispondenti potessero ottenere, alla fine della compilazione, una macro-valutazione del livello di sicurezza del sistema informativo oggetto delle loro risposte al questionario. Valutazione effettuata contestualizzando le misure di sicurezza digitale in essere con le esigenze di sicurezza digitale dell'azienda/ente, con riferimenti e le relative pesature al settore merceologico, al ruolo più o meno essenziale del sistema informativo nel supporto alle attività dell'organizzazione, e nella complessiva necessità di sicurezza digitale.

Hanno risposto alle domande sulle misure di sicurezza il **47%** delle organizzazioni rispondenti, quindi quasi la metà di tutte le organizzazioni che hanno compilato il questionario OAD 2026.

Trattandosi di una sezione opzionale, non si può escludere che le organizzazioni che hanno scelto di compilarla presentino un interesse o un'attenzione alla sicurezza digitale differenti rispetto alle altre organizzazioni rispondenti. I risultati devono pertanto essere interpretati tenendo conto anche di questa possibile autoselezione.

Rispetto alle precedenti edizioni dell'indagine, le domande e le relative modalità di risposta sono state profondamente modificate e semplificate, al fine di rendere più agevole e rapida la compilazione. Tale modifica non consente confronti diretti e omogenei con i risultati delle precedenti edizioni.

I risultati presentati in questo capitolo descrivono pertanto le misure di sicurezza digitale dichiarate dalle organizzazioni che hanno compilato questa parte opzionale del questionario. Essi costituiscono utili indicatori delle misure adottate nei sistemi informativi considerati, ma non possono essere interpretati come rappresentativi della diffusione delle diverse misure di sicurezza digitale nelle organizzazioni italiane.

Le principali caratteristiche delle organizzazioni rispondenti e dei loro sistemi informativi sono descritte nel precedente Capitolo 6.

🔍 Nelle varie figure di questo capitolo, c'è la risposta "**Non lo so**", che talvolta ha valori percentuali non trascurabili. Come mai? Come evidenziato dalla fig. 6.3-1 del Capitolo precedente**,** molte delle persone che hanno compilato il questionario non sono esperti di sicurezza digitale, e svolgono altri ruoli e professioni. A domande specificatamente tecniche, come quelle di questo capitolo, non sono in grado di rispondere, o non hanno avuto tempo e opportunità di chiedere eventualmente ai loro tecnici e/o consulenti. Quindi, correttamente, hanno selezionato "Non lo so". Questa scelta può contribuire a evitare risposte non attendibili, rendendo l'indagine più corretta e autorevole.

I risultati che emergono da questa parte "opzionale" del questionario OAD 2026, e riportati nei paragrafi di questo capitolo, hanno validità solo come indicatori della situazione della sicurezza digitale **nei SI dei rispondenti**, e **non** come analisi della diffusione dei vari strumenti di sicurezza digitale in Italia: per questo occorre fare riferimento alle specifiche indagini di mercato.

Nel seguito, gli strumenti e le misure per la sicurezza digitale sono raggruppati in due sezioni: misure organizzative e misure tecniche per la sicurezza digitale.

7.1 Le misure organizzative per la sicurezza digitale in essere nelle aziende/enti rispondenti

Gli aspetti organizzativi sono determinanti per l'attuazione e la gestione di una effettiva ed efficace sicurezza digitale, dato che le maggiori vulnerabilità, e le più difficili da eliminare o ridurre, sono proprio quelle delle persone e delle organizzazioni nelle quali operano.

Gli aspetti organizzativi sono talvolta trascurati, soprattutto dalle piccole organizzazioni, perché considerati prevalentemente come oneri burocratici e/o come spese di consulenza non necessarie: di interesse, di fatto, solo per le grandi organizzazioni. Al contrario, **sono misure essenziali** per l'effettivo funzionamento della sicurezza digitale, e **necessarie per qualsiasi tipo di organizzazione**, indipendentemente dalle sue dimensioni e dal settore merceologico di appartenenza: devono però essere commisurate e calate nelle specifiche realtà di ogni azienda/ente.

La fig. 7.1-1 mostra che per **l'86,11**% delle organizzazioni rispondenti è definito e conosciuto chi è il responsabile della sicurezza digitale, il **CISO, Chief Information Security Officer**, e quali sono i suoi compiti e le sue responsabilità. Questo ruolo può essere svolto da persone interne all'organizzazione o da consulenti o fornitori esterni. Se la sicurezza digitale è esternalizzata, deve essere chiaro chi decide e chi coordina all'interno e chi opera come fornitore. L'alta percentuale emersa tra le organizzazioni rispondenti è un indicatore che queste, indipendentemente dalle loro dimensioni e del settore merceologico di appartenenza, stanno affrontando "con il piede giusto" il tema della sicurezza digitale al loro interno.

> 🔍 Si deve sempre tener conto che non si può delegare/terziarizzare all'esterno dell'organizzazione la responsabilità complessiva della sicurezza digitale; si può terziarizzare solo la sua gestione operativa.

Sul tema della terziarizzazione della gestione della sicurezza digitale si veda anche "OAD Insight #7 – Cybersecurity in outsourcing: si può esternalizzare il servizio, non la responsabilità": https://www.oadweb.it/it/comunita-oad/oad-insight/oad-insight-7-cybersecurity-in-outsourcing-esternalizzabile-il-servizio-non-la-responsabilita.html.

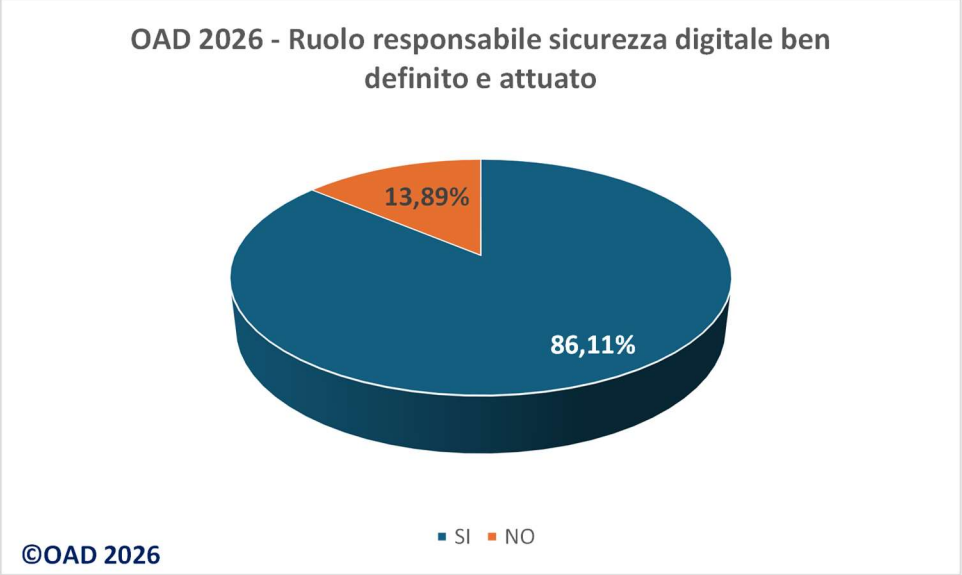


Fig. 7.1-1

La fig. 7.1-2 evidenzia che il 37,5% delle organizzazioni rispondenti gestisce internamente la sicurezza digitale, e quindi non la terziarizza. Un 15,28% dei rispondenti non sa se la sua organizzazione terziarizza, in toto o in parte, questa gestione.

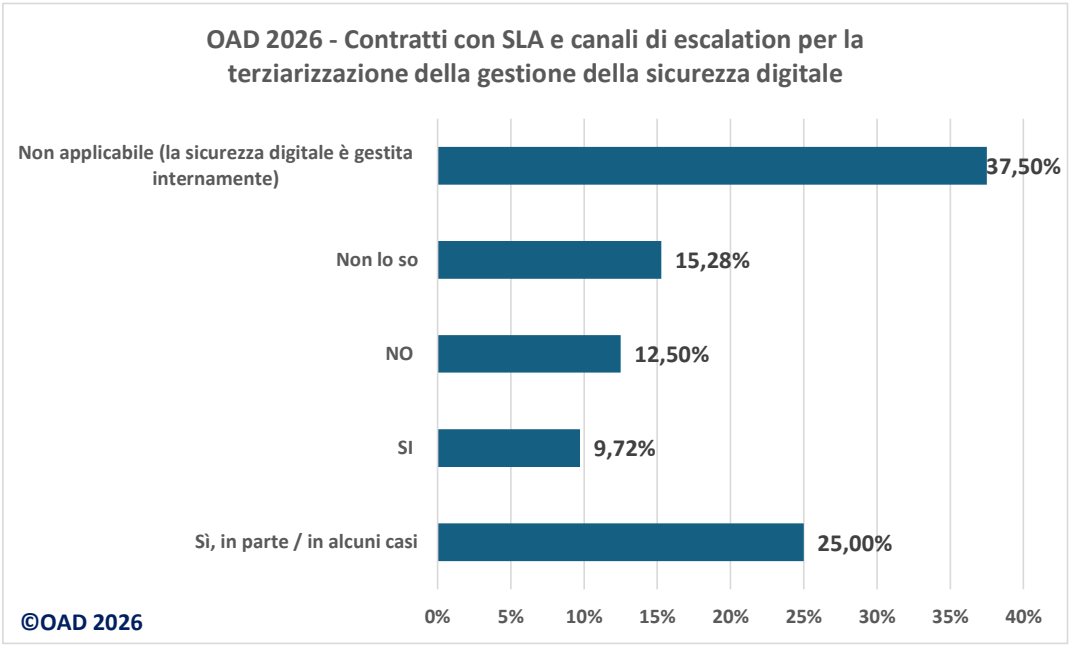


Fig. 7.1-2

Il 47,22% terziarizza la gestione della sicurezza digitale, in toto o in parte: praticamente quasi la metà dei rispondenti. Ma di questi il 12,5% non ha contratti ben definiti con SLA, Service Level Agreement, e con chiari canali di escalation in caso di incidenti o di crisi. Il 34,72% ha ben definito, in alcuni casi o per tutti i contratti, SLA e canali di escalation.

SLA/escalation sono fondamentali per specificare i tempi di risposta e i contatti per urgenze, quali incidenti o crisi, con il o con i fornitori.

Nel questionario OAD 2026, per questa domanda era precisato che “se esiste un contratto ma non è chiaro come gestire le urgenze, selezionare ‘in parte’”.

La fig. 7.1-3 mostra che ben il **93,06%** delle organizzazioni rispondenti, quasi tutti, dispone di regole scritte e diffuse al suo personale, in pratica delle procedure organizzative, su come utilizzare e gestire le password, gli accessi alle varie risorse ICT, l’uso dei dispositivi ICT (in particolare i PC/posti di lavoro) e dell’e-mail. Queste regole/procedure possono anche essere minime, ma è importante che esistano e siano diffuse.

La stragrande maggioranza dei rispondenti afferma di averle e, si immagina e spera l’autore, di seguirle. Un ulteriore indicatore che il bacino di rispondenti a OAD 2026 sembra affrontare correttamente gli aspetti organizzativi della sicurezza digitale, almeno per quanto dichiara con le risposte dele questionario selezionate.

Nel questionario OAD 2026, per questa domanda era precisato che “Se sono solo “a voce” e non sempre seguite, selezionare ‘in parte’.” Ed infatti il 37,5% ha selezionato questa risposta.

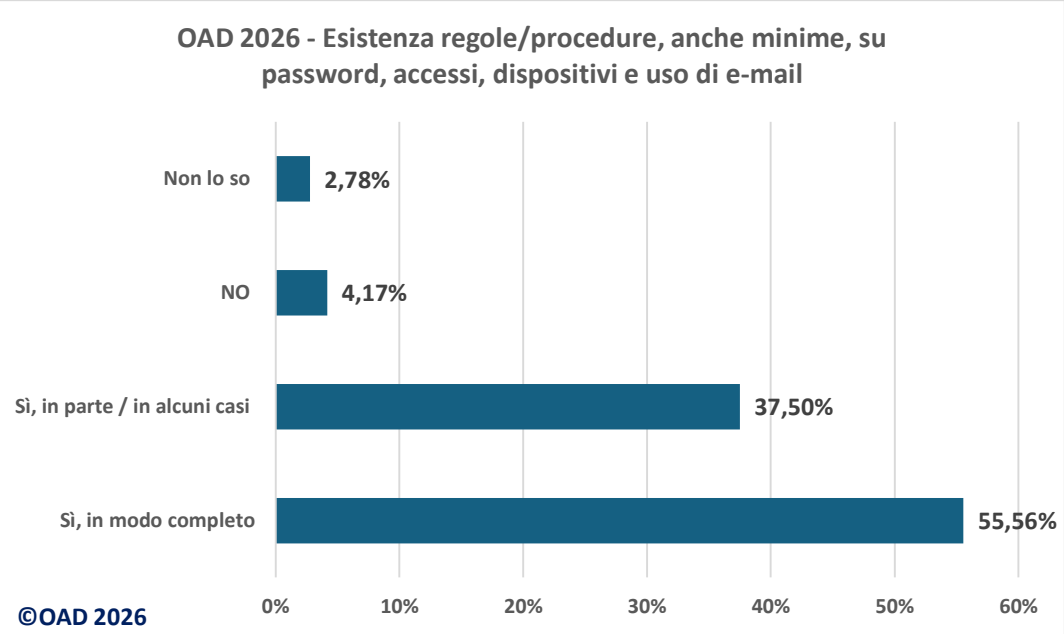


Fig. 7.1-3

La fig. 7.1-4 fa riferimento all’esistenza di regole/procedure organizzative, presso i rispondenti, sulla gestione dei dati e al loro accesso, ossia alla gestione della profilatura dei diritti d’accesso da parte dei vari utenti, finali e privilegiati. In altri termini definire “chi può vedere cosa”.

La regola/procedura può anche essere semplice, ma deve esistere ed essere realmente seguita. Essa può ad esempio, far riferimento a cartelle condivise con permessi, ai ruoli e alle profilature per gli accessi a CRM/gestionale, alla condivisione dati con organizzazioni e persone esterne.

La figura evidenzia che la quasi totalità dei rispondenti, il **93,06%**, ha definito ed utilizza questo tipo di regole: ma di questi il 30,56% lo fa solo per alcuni sistemi, servizi ed applicazioni ICT, probabilmente per quelle più critiche.

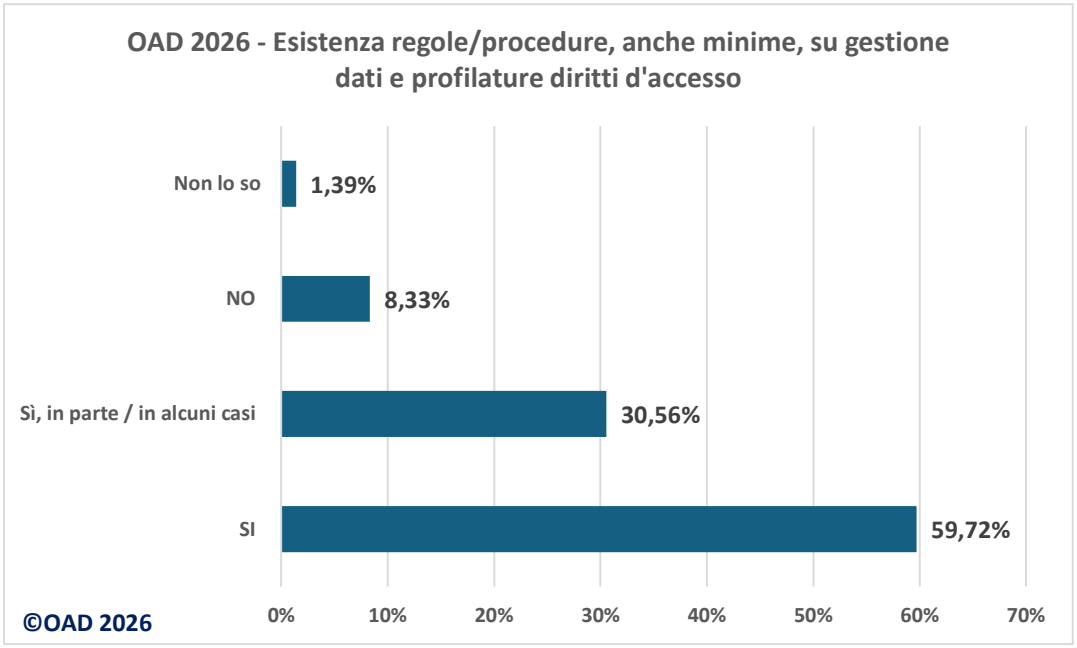


Fig. 7.1-4

Il **70,83%** delle organizzazioni rispondenti fa formazione/sensibilizzazione, ma in modalità e tempi differenti, come dettagliato nella fig. 7.1-5: solo il 27,78% lo fa sistematicamente, in maniera periodica e obbligatoria per tutti. Il 13,89% dei rispondenti ha risposto che fino ad oggi non l'ha fatto, ma che a breve lo farà.

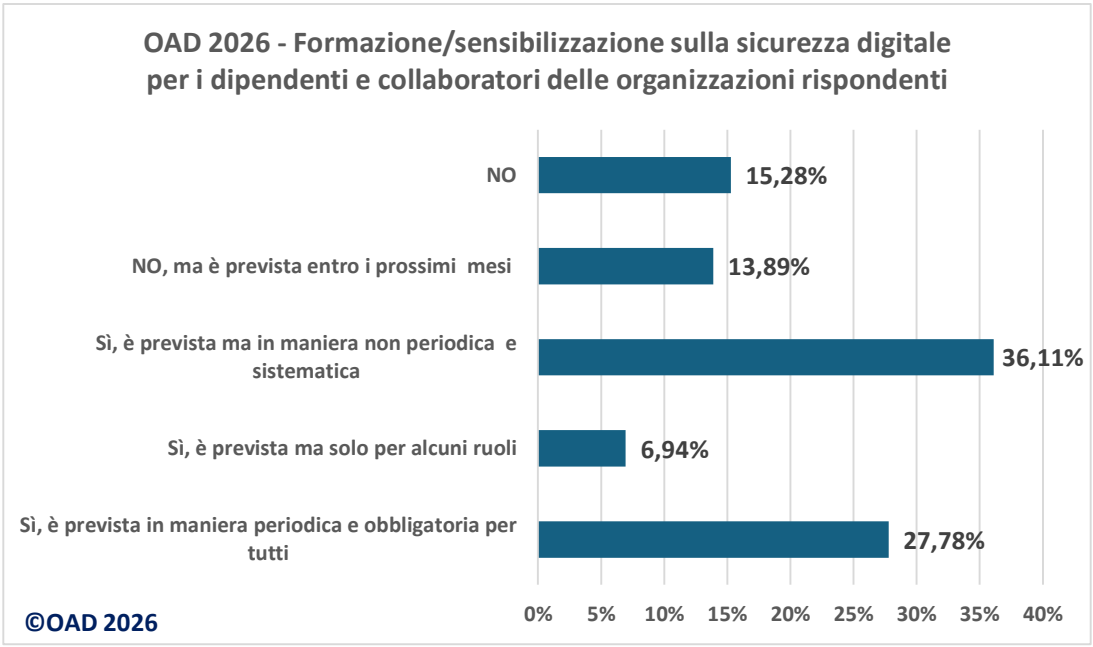


Fig. 7.1-5

Il dato che emerge dall'indagine è realistico, e solo in parte positivo, a giudizio dell'autore. Il 27,78% delle organizzazioni rispondenti effettua formazione/sensibilizzazione sistematica in maniera periodica e per tutti.

Tenendo conto dell'alto numero di piccole organizzazioni rispondenti, il dato è credibile ma dovrebbe essere ben più alto, a giudizio dell'autore. Con deepfake e spear phishing sempre più raffinate e credibili, nell'uso dei sistemi informativi occorre stare sempre più in guardia, dato che è come se fossimo sempre sotto attacco. Una sistematica formazione e sensibilizzazione, anche con brevi spot video, può mantenere più vigile l'attenzione (e la tensione) degli utenti.

La conoscenza dei rischi ICT e la consapevolezza di che cosa possono comportare questi rischi sono sempre più necessarie per tutti gli utenti di un sistema informativo: e devono essere periodicamente ripetute ed aggiornate, dato il continuo evolversi delle tecniche e delle modalità degli attacchi digitali.

Uno dei perenni problemi della sicurezza digitale è la corretta ed efficace gestione degli incidenti digitali. Troppo spesso, e soprattutto nelle piccole organizzazioni, l'incidente è gestito in emergenza, indipendentemente dalla sua gravità, e senza un approccio sistemico, razionale e documentato, o documentabile/ tracciabile.

Anche questa procedura organizzativa, come le altre considerate in precedenza, può essere un documento breve o una lista di controlli da effettuare (checklist): l'importante è che chiaramente specifichi, quando avviene ed è rilevato un incidente digitale, **che cosa fare**, soprattutto nelle fasi inziali, **chi avvisare, chi coinvolgere e in che tempi**.

Su questo tema, la fig. 7.1-6 mostra che quasi il **70%** delle organizzazioni rispondenti ha una procedura, ma di questi il 27,78% l'ha solo per alcuni tipi di incidenti, o per quelli sui sistemi e sulle applicazioni più critiche.

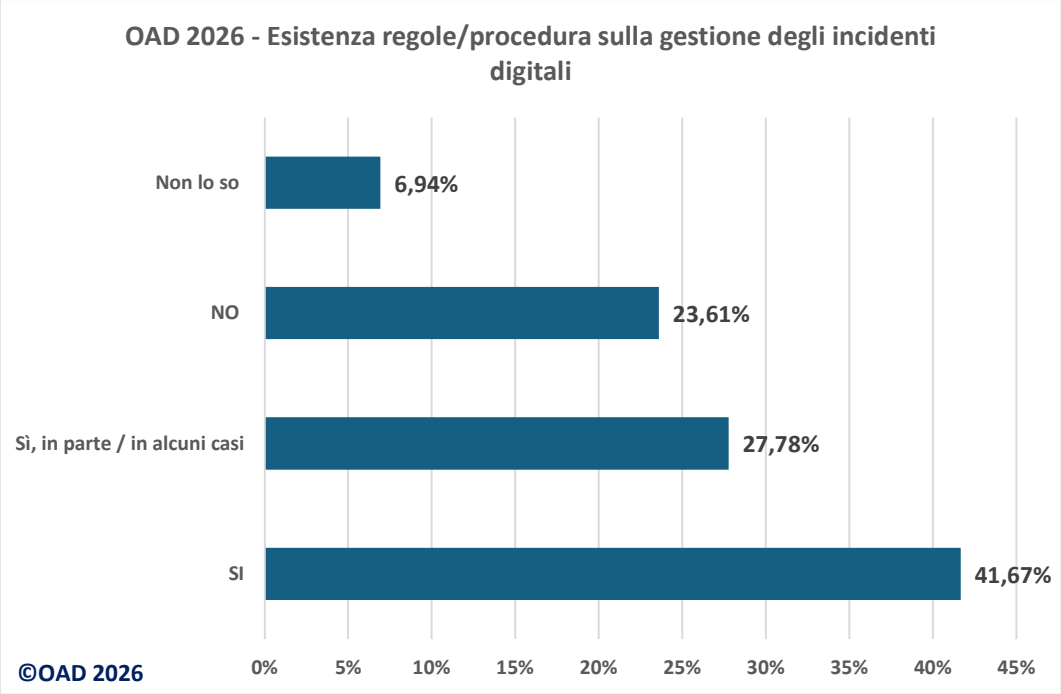


Fig. 7.1-6

Dopo aver gestito i momenti iniziali di incidenti informatici, e soprattutto di quelli più gravi che possono mettere in crisi il funzionamento dell'organizzazione, **è necessario ripristinare il funzionamento delle risorse ICT compromesse**. Occorre quindi disporre di un piano e delle procedure organizzative per il ripristino almeno per le risorse ICT, in particolare le applicazioni, con tempi ed obiettivi specificati, anche in maniera semplice, ad esempio "entro X ore/giorni". In caso di gravi compromissioni di queste risorse ICT critiche, quindi in caso di disastro di parte o di tutto il sistema informativo, occorre passare dal ripristino dai back-up ad un effettivo piano di Disaster Recovery, che richiede l'allocazione delle risorse ICT alternative necessarie. Erroneamente viene sovente ritenuto che piani e procedure di ripristino siano solo per grandi organizzazioni. Non è vero, sono necessarie per organizzazioni anche piccole e piccolissime, dato che anch'esse hanno la quasi totalità delle loro attività e dei loro processi basati su sistemi informativi. Non serve un piano complesso: **basta sapere quali servizi ripristinare per primi e in che tempi massimi**. Ma è fondamentale avere le **risorse ICT "alternative"** da utilizzare per il Disaster Recovery.

La fig. 7.1-7 mostra la situazione dei piani e delle procedure di ripristino, ivi incluso il Disaster Recovery.

Si noti che nel questionario OAD 2026 era indicato che "Se tali risorse non sono pre-allocate, scegliere 'in parte'".

La situazione che emerge dalle organizzazioni rispondenti **è ancora piuttosto critica**, come lo era dalle indagini OAD delle edizioni precedenti: ma ora è più grave, con un 2026 con guerre ibride sempre più diffuse. Solo il **12,5%** dichiara di **avere piani di ripristino con disponibilità di risorse ICT alternative**.

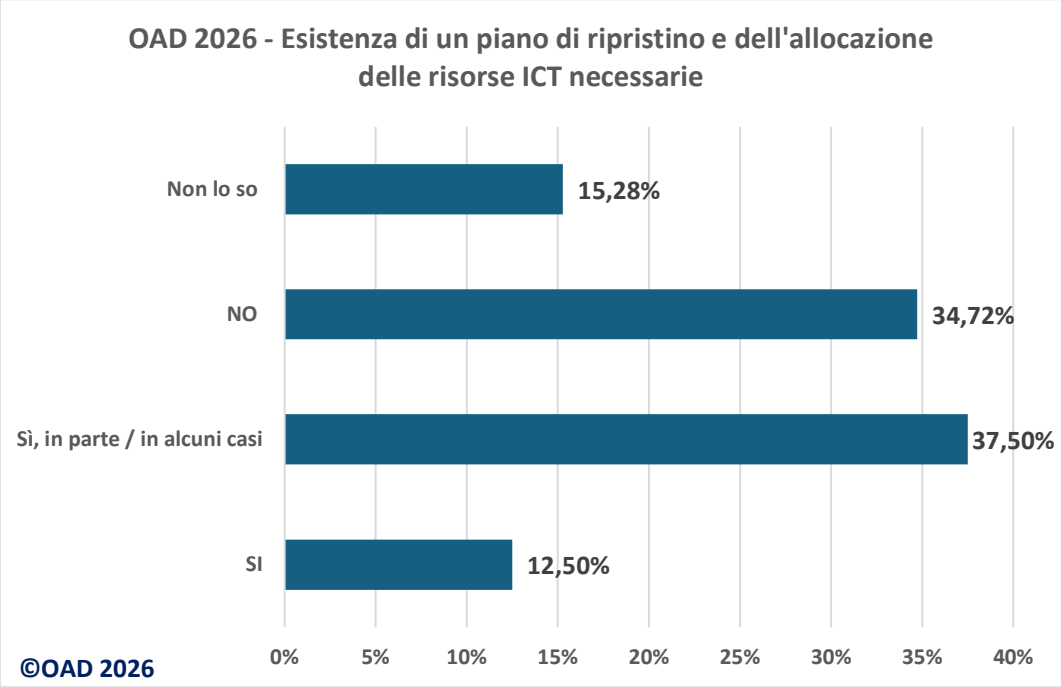


Fig. 7.1-7

Il 37,5% dispone solo parzialmente di piani e procedure per il ripristino, e probabilmente non ha disponibilità di risorse ICT alternative da utilizzare in caso di disastro. Più di 1/3 dei rispondenti dichiara di non avere nessun piano e/o procedura per il ripristino: nel 2026 questo non è confortante.

Sul tema si veda anche "OAD Insight #3 – Il backup non basta": https://www.oadweb.it/it/comunita-oad/oad-insight/oad-insight-3-il-backup-non-basta.html

Tra le misure organizzative sulla sicurezza digitale, è basilare, secondo l'autore, il periodico controllo delle misure in essere e l'auditing[16] anche sul loro corretto utilizzo da parte degli utenti del sistema informativo.

Tra i tipici controlli che si dovrebbero **periodicamente** effettuare, internamente o esternamente con affidabili terze parti, e che possono essere svolti anche nell'ambito di auditing, si includono ad esempio il controllo del ripristino da back up, l'aggiornamento periodico degli account e delle profilature dei diritti di accesso, l'aggiornamento dei vari software in uso, l'aggiornamento e la pubblicazione delle procedure organizzative, il controllo dei log dei sistemi e degli utenti (in particolare per gli utenti privilegiati quali gli amministratori di sistema), l'analisi delle vulnerabilità (vulnerability scan), i controlli coi fornitori ICT, in particolare in riferimento alle SLA, Service Level Agreement, specificate nel contratto.

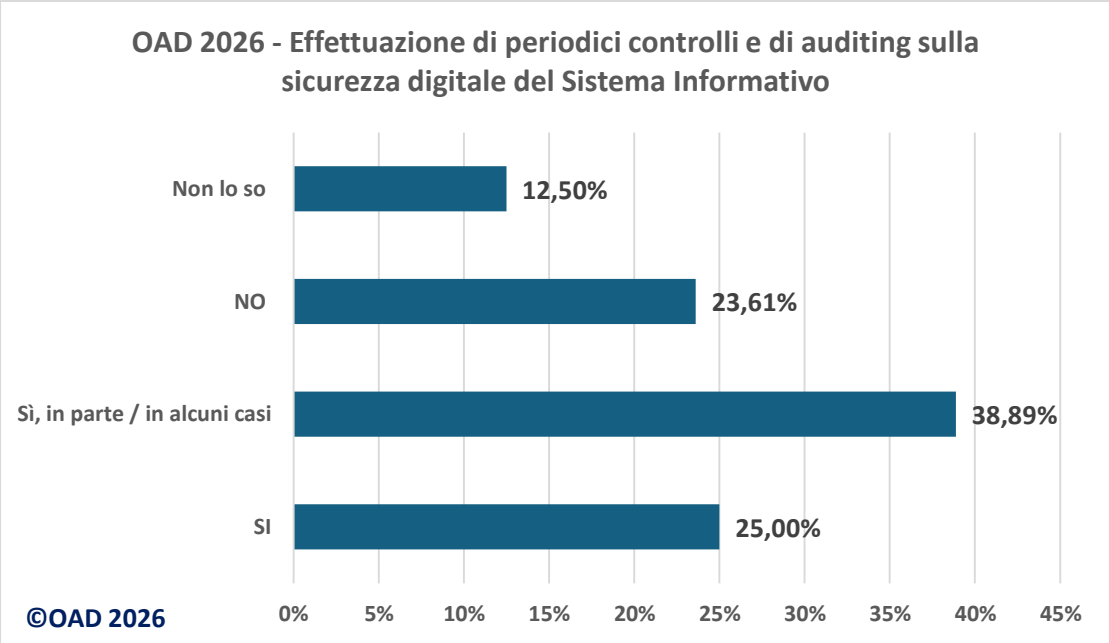


Fig. 7.1-8

Nell'ambito dei controlli periodici, anche quello sui fornitori è fondamentale, almeno per quanto stabilito a livello contrattuale.

Dall'indagine emerge che il **63,89%** delle organizzazioni rispondenti effettua periodici controlli e/o auditing, ma quasi ¼ no. Eppure, basterebbe solo un semplice elenco di controlli (check list) da effettuare periodicamente, soprattutto per le piccole organizzazioni.

Sul tema si veda anche "OAD Insight #17 - Auditing della sicurezza digitale: verificare che le misure in essere funzionino davvero": https://www.oadweb.it/it/comunita-oad/oad-insight/oad-insight-17-auditing-sicurezza-digitale.html.

[16] L'**auditing della sicurezza digitale** è un'attività sistematica e documentata di verifica, finalizzata a valutare se le misure di sicurezza previste dall'organizzazione siano state effettivamente attuate, siano correttamente gestite e risultino adeguate rispetto ai rischi che devono fronteggiare.

La sicurezza digitale è un processo continuo, dato il veloce evolversi dei rischi, degli strumenti di attacco e di difesa, delle modalità operative e del business delle organizzazioni. Questo comporta la necessità di una continua analisi dei rischi, richiesta anche da numerose normative quali la NIS2, e ad un aggiornamento, evoluzione e miglioramento continuo della sicurezza digitale. Questo tema non è appannaggio solo delle grandi organizzazioni, ma dovrebbe essere attuato anche dalle medie, piccole e piccolissime. Basta tenere traccia dei problemi riscontrati e delle relative azioni, ed individuare chi ne è responsabile e quale è la scadenza delle azioni che devono essere effettuate.

La fig. 7.1-9 mostra la situazione emersa dall'indagine.

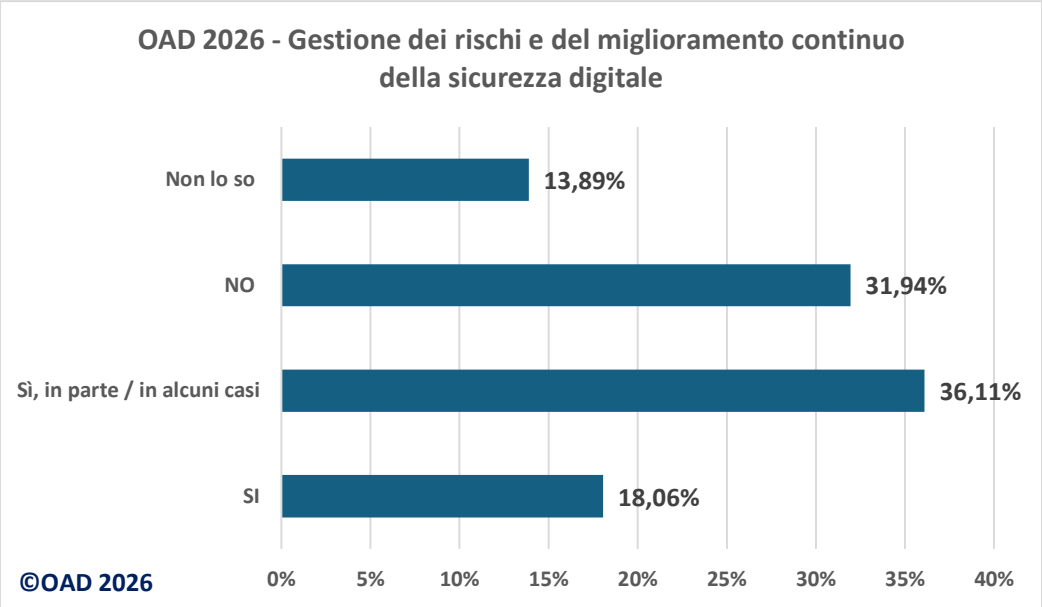


Fig. 7.1-9

Più della metà dei rispondenti, il 54,17%, effettua tali attività, in toto o in parte, ma quasi 1/3 non lo fa. Ed è alta la percentuale dei "Non lo so".

Uno dei temi più problematici, in particolare in Italia, è quello delle effettive competenze sulla sicurezza digitale per chi se ne deve occupare, sia per il personale interno all'organizzazione, sia per i fornitori (che includono i consulenti), che gestiscono per l'organizzazione specifici servizi ICT, inclusa eventualmente la stessa gestione della sicurezza digitale.

Uno degli indicatori del livello di competenza per persone e per organizzazioni è l'acquisizione e il periodico aggiornamento di autorevoli **certificazioni sulla sicurezza digitale**.

La fig. 7.1-10 indica che solo il **23,61%** delle organizzazioni rispondenti ha una o più certificazioni (ad esempio: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 15408 / EUCC, ANSI/TIA - 942, CCSK di CSA, etc.) per la **sicurezza digitale del suo sistema informativo**.

Per chi ha risposto positivamente, tutti hanno la ISO/IEC 27001, qualcuno dispone anche della ISO/IEC 27017 e della ANSI/TIA – 942.

Si deve tener presente che queste sono solo le certificazioni sulla sicurezza digitale dei sistemi informativi e delle organizzazioni indicate dai rispondenti, e non rappresentano una possibile distribuzione delle certificazioni di questo tipo in Italia.

La fig. 7.1-11 fa riferimento alle certificazioni individuali che l'organizzazione rispondente richiede al suo il personale interno che si occupa di sicurezza digitale. Numerose sono queste certificazioni individuali: quelle indipendenti includono e-CF security manager, e-CF security specialist, CISSP, CISSP, CISM, CEH, CCSP, SSCP, ICDL; quelle dei produttori ICT includono quelle specifiche in ambiti AWS, Cisco, Google, IBM, Microsoft, ecc.

La figura indica che quasi il 30% richiede certificazioni al suo personale interno coinvolto nella sicurezza digitale: la richiesta per questi è variegata e dipende anche dalla tipologia del sistema informativo e delle sue applicazioni. Gli esempi indicati includono e-CF, ICDL, Google, Veeam, VMWare, Fortinet.

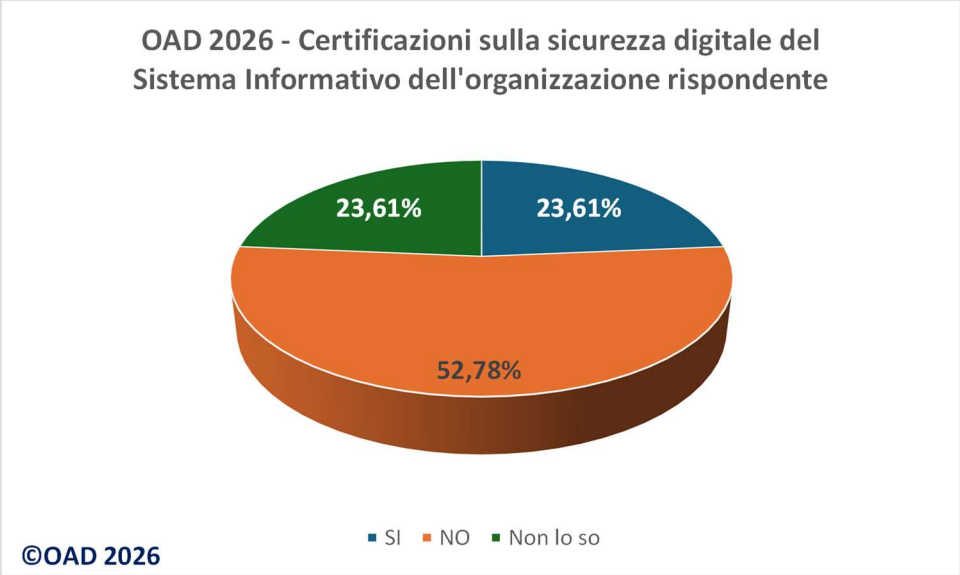


Fig. 7.1-10

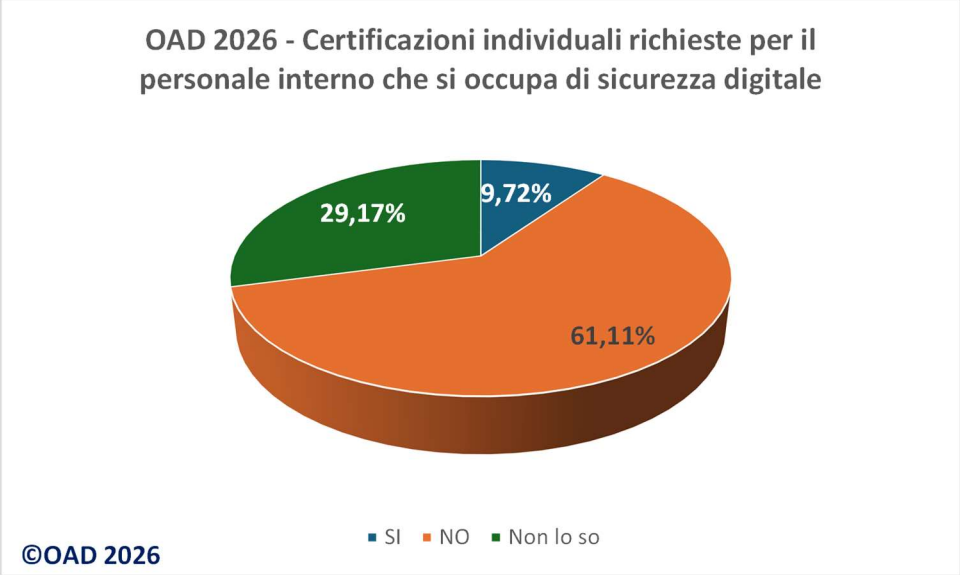


Fig. 7.1-11

Un ulteriore tema per le certificazioni sulla sicurezza digitale riguarda quelle richieste dall'organizzazione rispondente alle sue Terze Parti (Fornitori, Consulenti, ecc.) e al loro personale.

La fig. 7.1-12 mostra la situazione in merito per le organizzazioni rispondenti:

- Il 40% non richiede nulla;
- Il 9,72% richiede certificazioni sia a livello aziendale sia a livello del loro personale che interagisce con l'Azienda/Ente
- L'11,11% richiede certificazioni solo per il loro personale che interagisce con l'organizzazione.

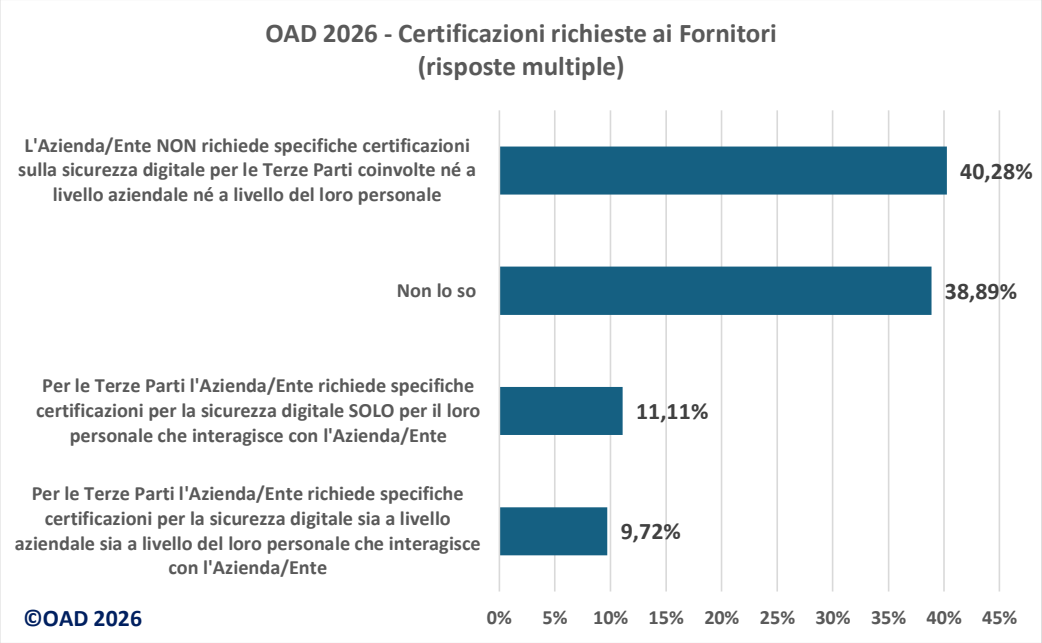


Fig. 7.1-12

Circa un 20% dei rispondenti richiede certificazioni ai fornitori e/o al loro personale. A giudizio dell'autore, è un dato che indica poco interesse e, forse, una limitata credibilità/reputazione sull'utilità di queste certificazioni, che il più delle volte sono acquisite solo se obbligatorie per qualche norma.

Il 39% di risposte "Non lo so" è una ulteriore conferma della poca attenzione/reputazione in merito.

7.2 Le misure tecniche

Con l'edizione 2026 le domande del questionario OAD 2026 sulle misure tecniche per la sicurezza digitale sono diverse da quelle delle precedenti edizioni, per non richiedere a chi lo compila troppo tempo e troppe specifiche competenze tecniche. Come per le precedenti edizioni, non si fa riferimento a specifiche soluzioni proprietarie, a prodotti e servizi commerciali, e le domande del questionario non sono di dettaglio.

Le domande sulle misure tecniche sono state articolate per:

- architettura della sicurezza digitale ed inventario risorse ICT;
- controllo degli accessi e protezione degli account;
- patch, anti-malware, anti-virus, EDR, protezione endpoint;
- reti, firewall, accessi da remoto;
- backup e continuità operativa;

- monitoraggio della sicurezza digitale e gestione log.

7.2.1 Inventario e controllo risorse ICT

Nell'ambito della sicurezza digitale, un elemento fondamentale è conoscere tutte le risorse ICT che costituiscono il sistema informativo (SI): in particolare PC, server, cloud, e-mail, firewall, switch, connessioni a Internet, applicazioni, servizi terziarizzati (in cloud).

La fig. 7.2.1-1 evidenzia che più di ¾ dei rispondenti dispone di un inventario aggiornato più o meno completo di tutte le risorse ICT, e solo il 10% riconosce di non averlo. Considerando la maggioranza dei rispondenti appartenenti a medie-piccole organizzazioni, questo è un dato positivo che indica che i rispondenti conoscono le risorse dei loro SI

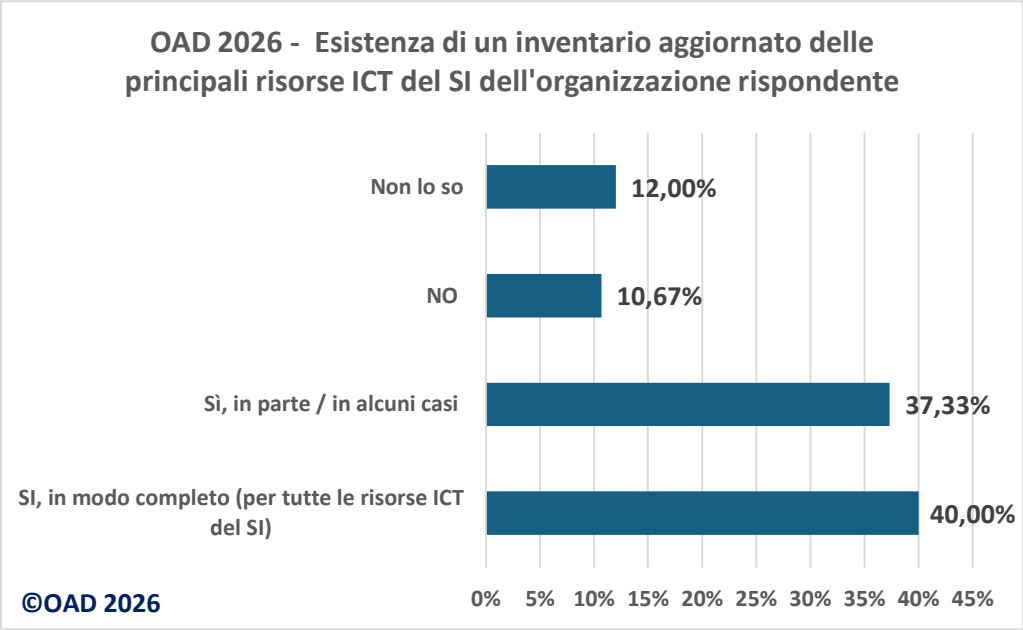


Fig. 7.2.1-1

La fig. 7.2.1-2 mostra, percentualmente, quante delle organizzazioni hanno identificato i sistemi ICT critici del loro SI, e chi li gestisce. I sistemi ICT sono critici nell'ottica del funzionamento dell'organizzazione stessa, o per la confidenzialità dei dati trattati. Alcuni possono essere poi critici per motivi tecnici, ad esempio perché operanti su sistemi obsoleti, perché non aggiornati, e così via. Tipi esempi di sistemi critici includono ad esempio la posta elettronica, i sistemi ERP, CRM, OT, i sistemi di monitoraggio e controllo dell'intero sistema informativo e della sua sicurezza. L'importanza di sapere quali siano i sistemi critici è basilare perché essi richiedono più elevati livelli di sicurezza digitale, ad esempio l'autenticazione multifattoriale, la crittografia dei dati trattati, la replica in tempo reale, ecc. È anche importante sapere chi gestisce tali sistemi, internamente o esternamente all'organizzazione, per potere meglio controllarli. Un effettivo controllo dei sistemi terziarizzati è sempre necessario, anche se di non facile attuazione.

Il dato che emerge dall'indagine è abbastanza positivo: **l'81,33%** dei rispondenti dichiara di saperlo, ed il 41,33 in modo completo.

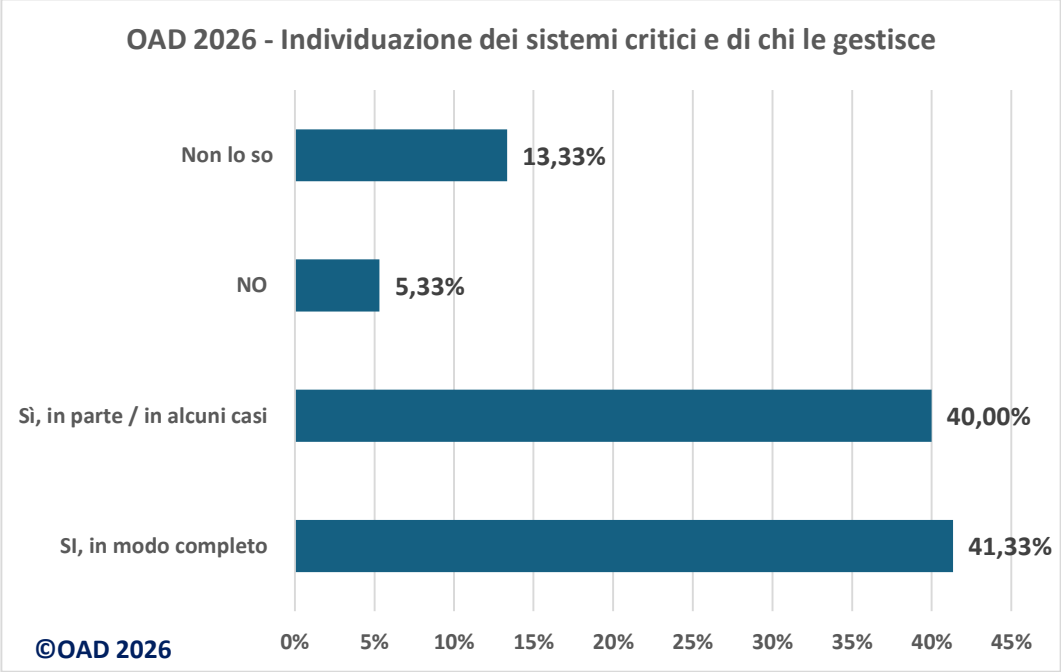


Fig. 7.2.1-2

La fig. 7.2.1-3 evidenzia che per il **56%** dei rispondenti la gestione della sicurezza digitale da loro effettuata (o effettuato tramite un loro fornitore) include, in toto o in parte, anche quella dei sistemi ICT terziarizzati.

È una percentuale alta, tenendo conto che molti fornitori di hosting/cloud non consentono controlli diretti della sicurezza digitale da loro implementata e gestita.

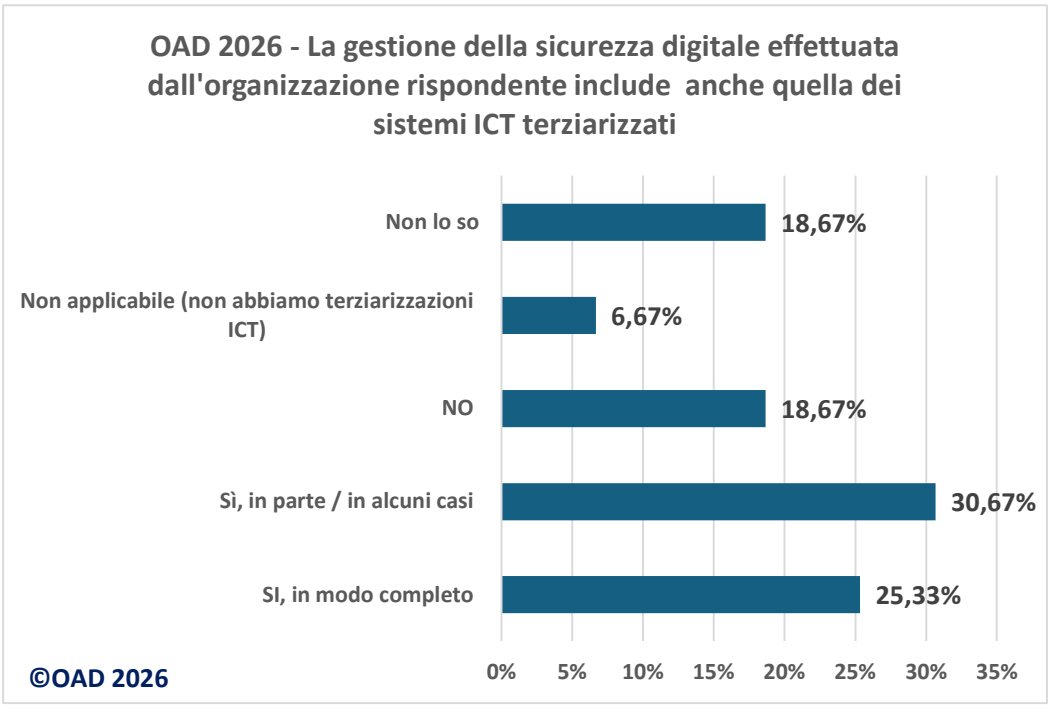


Fig. 7.2.1-3

7.2.2 Accessi e protezione account

La corretta autenticazione degli utenti per gli accessi alle risorse ICT è una misura fondamentale per la sicurezza digitale. Tradizionalmente basata su identificativo d'utente e password, per gli utenti e per le applicazioni più critiche questo tipo elementare di autenticazione non è sufficiente: deve essere più forte, e come minimo multifattoriale. Gli utenti più critici sono quelli privilegiati, che includono tipicamente gli amministratori di sistema, i manutentori di sistema, i sistemisti, i gestori delle banche dati, i gestori di rete, gli sviluppatori di software, gli installatori di pacchetti software

L'autenticazione verifica l'identità di un utente, garantendo che la persona o il dispositivo che tenta di accedere a un sistema sia effettivamente chi dichiara di essere, prima di concedere l'accesso a risorse, dati o applicazioni. L'autenticazione a più fattori, indicata spesso anche in italiano con l'acronimo **MFA,** Multi-Factor Authentication, richiede all'utente, persona o dispositivo, di verificare la propria identità fornendo due o più prove di identificazione, chiamati **fattori** di autenticazione, prima di poter accedere ai propri sistemi ed applicazioni. Tipico esempio, dopo aver inserito l'identificativo d'utente ed una password, la necessità di inserirne una seconda ricevuta sul proprio smartphone.

La fig. 7.2.2-1 mostra che **l'82,67%** dei rispondenti usa sistemi con MFA, e di questi il 34,67% in maniera completa, ossia per tutti gli utenti privilegiati e per tutte le applicazioni critiche. Anche questo un dato positivo, che indica come gran parte dei rispondenti dispone di un buon livello di sicurezza digitale sul proprio sistema informativo.

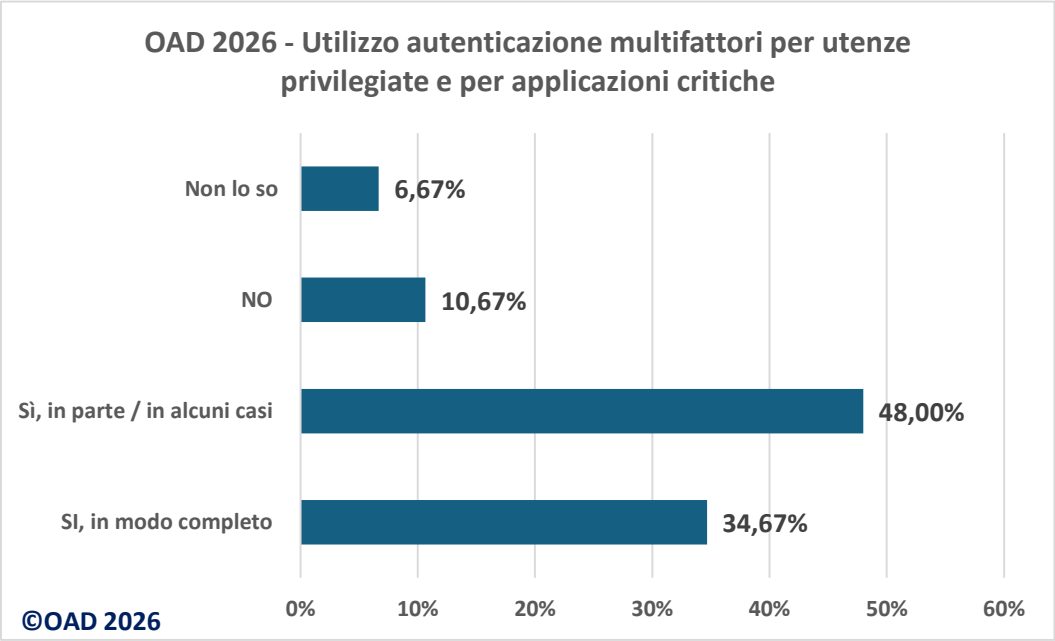


Fig. 7.2.2-1

Gli utenti privilegiati hanno elevatissimi diritti d'accesso e diritti d'azione sulle risorse ICT del sistema informativo. Devono pertanto essere sistematicamente controllati ed il loro numero limitato affiche possano essere effettivamente controllati.

La fig. 7.2.2-2 evidenzia che la quasi totalità dei rispondenti, il **94,59%**, gestisce in maniera controllata gli utenti privilegiati, che sono in numero limitato o comunque adeguato per poterli effettivamente controllare:

di questi, il 58,11% li controlla in maniera sistematica e completa. Anche questo dato è positivo e conferma, almeno per questa area, il buon livello della sicurezza digitale dichiarata dai rispondenti.

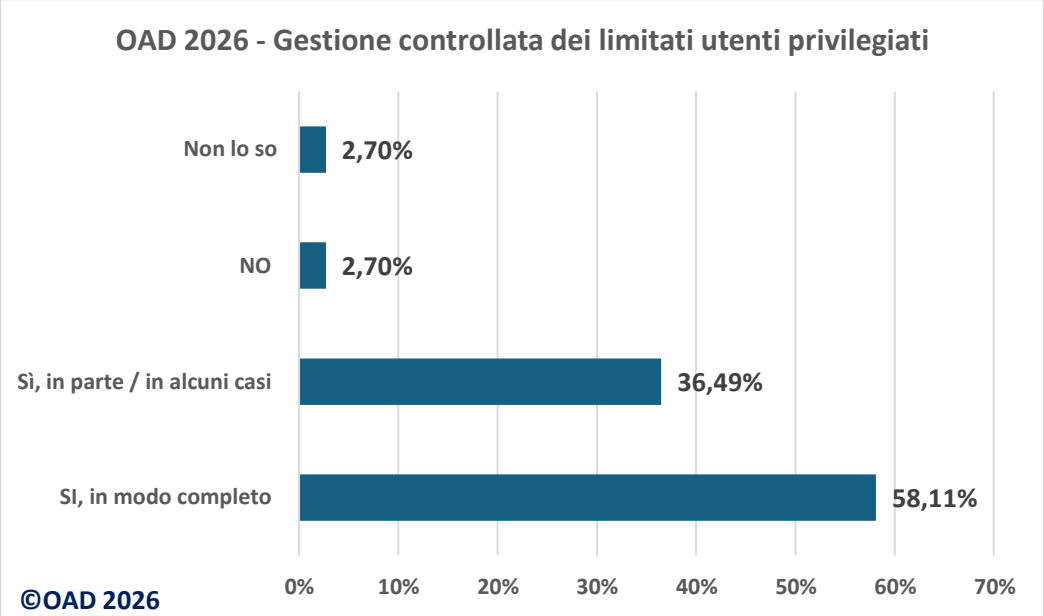


Fig. 7.2.2-2

7.2.3 Patch, anti-malware, anti-virus, EDR, protezione endpoint

Un elemento di base della sicurezza digitale è il tempestivo **aggiornamento del software**, appena disponibile, con priorità commisurata alla criticità delle vulnerabilità. Si deve infatti tener conto che un aggiornamento può richiedere verifiche di compatibilità e test, soprattutto nei sistemi critici. In altri casi, ad esempio l'aggiornamento di anti-malware, l'aggiornamento può e deve essere immediato**,** appena il produttore lo rende disponibile. L'aggiornamento può consistere nel cambio di versione, oppure nella installazione di una patch o di un fix. Una patch (letteralmente "toppa") è un pacchetto di aggiornamento software distribuito per correggere vulnerabilità di sicurezza, risolvere bug o migliorare le prestazioni di un programma software. Il fix ("riparazione") è invece la specifica soluzione tecnica a un singolo difetto del codice, che può essere inserita in una patch.

La fig. 7.2.3-1 mostra che **quasi il 90%** delle organizzazioni rispondenti effettua regolarmente gli aggiornamenti software, e di questi il 54% in maniera completa. A giudizio dell'autore, il 4% dei rispondenti che dichiarano che non aggiornano regolarmente, è dovuto probabilmente al non rinnovo dei contratti di manutenzione del software.

Altro elemento di base della sicurezza digitale è l'uso di sistemi **anti-virus/anti malware**[17] sui singoli sistemi ICT e delle loro evoluzioni in sistemi **EDR**[18] **,** Endpoint Detection and Response**.**

[17] I due termini sono usati talvolta come sinonimi, ma sono due sistemi differenti. Il virus è un codice maligno autoreplicante, ossia capace di diffondersi tra diversi computer (collegati in rete). Un anti-virus lo individua e lo elimina, impedendo che si diffonda e che attui le sue specifiche azioni dolose. Il malware è un codice maligno, che agisce dove viene installato, ed il sistema anti-malware lo individua e lo elimina (o fornisce le istruzioni su come eliminarlo).

[18] EDR è un sistema per monitorare, rilevare e bloccare le minacce informatiche direttamente sui singoli dispositivi, chiamati end-point, connessi alla rete dell'organizzazione (ad esempio laptop, server, sistemi di storage, dispositivi mobili). Un EDR: a) svolge un monitoraggio continuo in tempo reale di tutte le attività che avvengono sull'endpoint (apertura di file, esecuzione di processi, modifiche al registro di sistema, connessioni di rete); b) effettua una analisi comportamentale dell'end point, anche grazie all'IA, individuando comportamenti anomali o sospetti; c) rilevato un pericolo, può

La fig. 7.2.3-2 evidenzia che **l'81,25%** dispone di questi tipi di sistemi di protezione, e li gestisce o li fa gestire da fornitori specializzati, che talvolta sono anche i fornitori degli specifici software di sicurezza.

Un 5% dei rispondenti dichiara di non utilizzare questo tipo di sistemi. Al di là di possibili aspetti relativi ai costi di questi sistemi, alcuni tecnici, soprattutto nel passato e per ambienti ICT chiusi e molto controllati, affermavano di non voler usare questi tipi di protezione, poiché penalizzavano le prestazioni dei sistemi ICT sui quali erano installati.

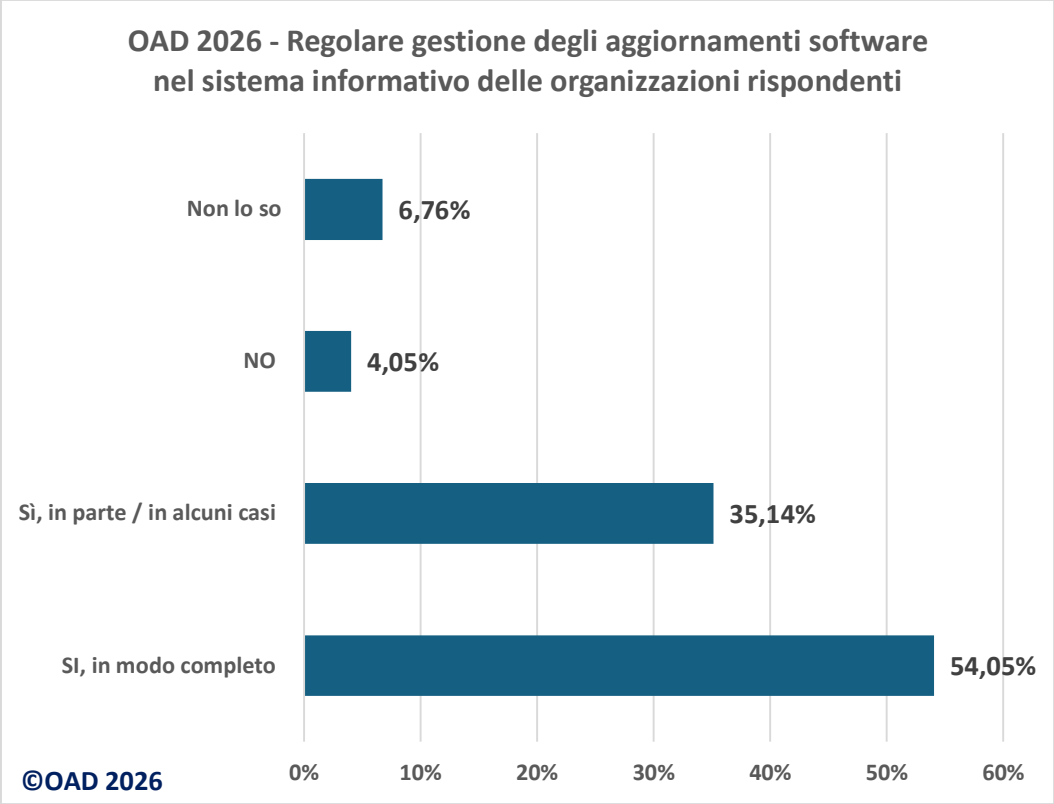


Fig. 7.2.3-1

intervenire in automatico o su indicazione dell'UOSI, Unità Organizzativa Sistemi Informativi; d) produce una cronologia dettagliata di cosa è successo per capire da dove è entrata la minaccia e come risolverla

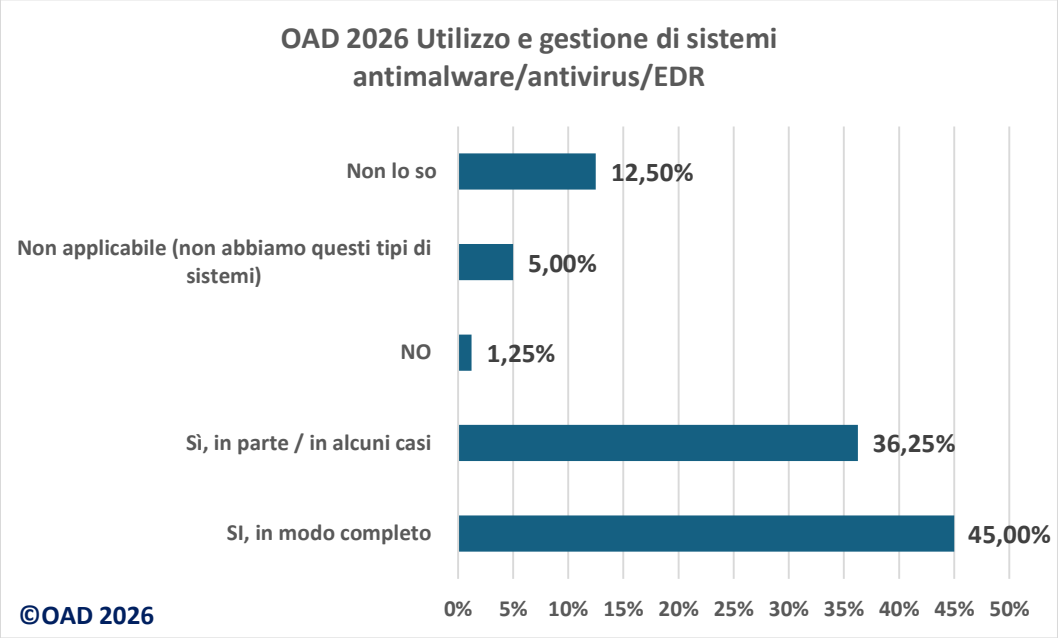


Fig. 7.2.3-2

7.2.4 Rete, firewall, accessi remoti

Per un sistema informativo sicuro, le reti devono essere "intrinsecamente" sicure, e gli accessi da remoto, che passano attraverso le reti, devono essere sicuri e con comunicazioni criptate.

Varie sono le misure di sicurezza applicabili ad una rete, a partire dalla duplicazione dei suoi nodi e dei suoi collegamenti/connessioni, in particolare ad Internet, e dal suo monitoraggio. Nel questionario OAD 2026 si sono considerati solo i firewall di rete, nell'ottica di semplificare il più possibile le domande "tecniche"

La fig. 7.2.4-1 mostra la larga diffusione, quasi il **92%** tra le organizzazioni rispondenti, dell'uso di firewall di rete regolarmente aggiornati e gestiti. Anche questo dato conferma un buon livello di sicurezza dei sistemi informativi dei rispondenti.

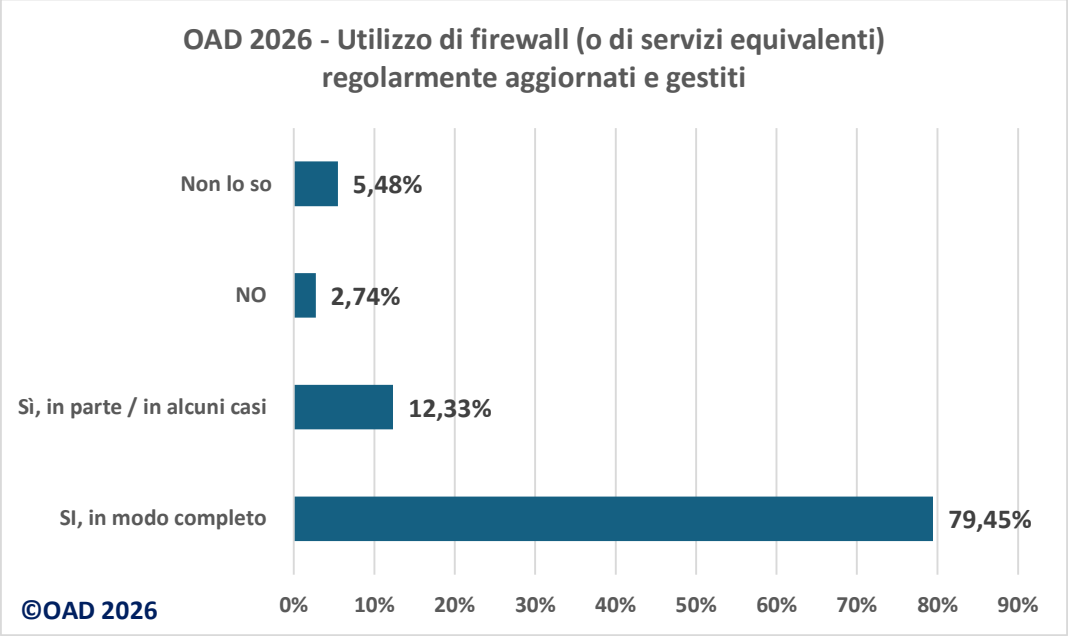


Fig. 7.2.4-1

La fig. 7.2.4-2 mostra che quasi il **70%** delle organizzazioni rispondenti utilizza accessi da remoto (VPN[19]/remote desktop[20]) sicuri, con autenticazione forte degli interlocutori, tipicamente con l'uso di autenticazione a più fattori (MFA) e collegamenti criptati, e con il tracciamento delle attività.

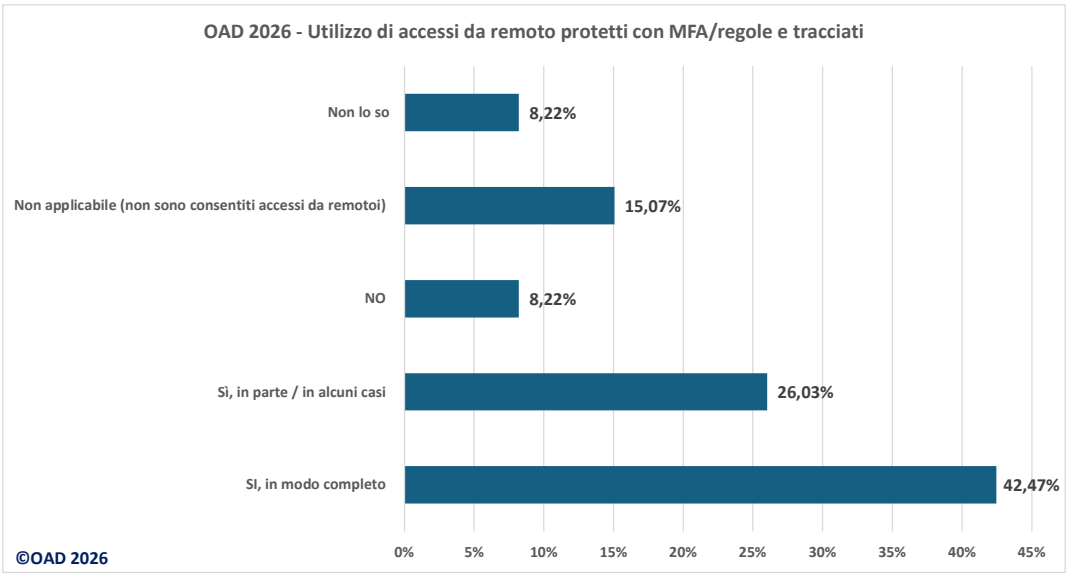


Fig. 7.2.4-2

[19] **VPN,** Virtual Private Network, consente di creare una connessione sicura e crittografata tra il dispositivo dell'utente e l'applicazione/servizio in internet.
[20] **Remote Desktop** permette di visualizzare e controllare un computer a distanza attraverso un altro dispositivo (un altro PC, un tablet o uno smartphone).

7.2.5 Backup e continuità operativa

Il backup consiste nella copia di sicurezza di dati, file, configurazioni o interi sistemi salvata su un supporto separato dall'originale per consentirne il ripristino in caso di perdita, danneggiamento o cancellazione. Serve a proteggere le informazioni da guasti hardware, errori umani, furti o attacchi digitali. Occorre effettuare backup per tutti i dati ed i programmi del sistema informativo, in maniera regolare e periodica. La frequenza del backup dipende dagli aggiornamenti dei dati e del software, e dalla loro criticità per le attività dell'organizzazione. Le copie dei backup devono essere adeguatamente protette e conservate in modo da evitare che un incidente informatico o un evento fisico che comprometta i sistemi originali possa compromettere anche le copie di sicurezza. A tal fine è opportuno prevedere copie dei backup in sedi geograficamente separate e/o copie isolate dai sistemi originali, ad esempio mediante supporti disconnessi o sistemi di backup immutabili. Se contengono dati confidenziali e critici, è inoltre opportuno che siano crittografate. Queste sono le regole principali per un corretto, sistematico e regolare backup. Ma non basta: occorre essere in grado di ripristinare il sistema ICT con i dati del backup.

La fig. 7.2.5-1 mostra che **l'83,56%** delle organizzazioni rispondenti effettua regolarmente backup su tutti i dati o almeno su quelli più critici. Dovrebbero farlo il 100% delle organizzazioni, ed è strano che quasi il 7% dichiari di non farlo: probabilmente ha risposto "no" in quanto non lo fa "regolarmente".

La fig. 7.2.5-2 mostra che quasi il 37% delle organizzazioni rispondenti ha effettuato negli ultimi 12 mesi almeno una prova di ripristino dei sistemi ICT coi dati di backup. Come già anticipato, non basta avere il backup. Dai dati di backup occorre saper ripristinare il sistema ICT, come anche descritto in "OAD Insight #3 - Il backup non basta", si veda https://www.oadweb.it/it/comunita-oad/oad-insight/oad-insight-3-il-backup-non-basta.html

La fig. 7.2.5-3 mostra che il 54,79% delle organizzazioni rispondenti protegge la copia di backup dei dati e del software in uso, tipicamente criptandoli.

La fig. 7.2.5-4 mostra che il 32,88% delle organizzazioni rispondenti dispone di un piano di Disaster Recovery (DR), e per esso ha previsto le risorse ICT alternative necessarie, prenotandole o già allocandole. Solo l'8,22% lo ha fatto in modo completo, ossia per (almeno) tutte le risorse ICT ritenute essenziali per il funzionamento dell'organizzazione stessa.

Il 38,36% di rispondenti dichiara di non avere un piano di DR: il dato dipende anche dal fatto che il 63,67% dei rispondenti sono medie-piccole organizzazioni, **ma in ogni caso è preoccupante**. La resilienza di un sistema informativo è necessaria ed essenziale anche per quelli di piccole e piccolissime organizzazioni.

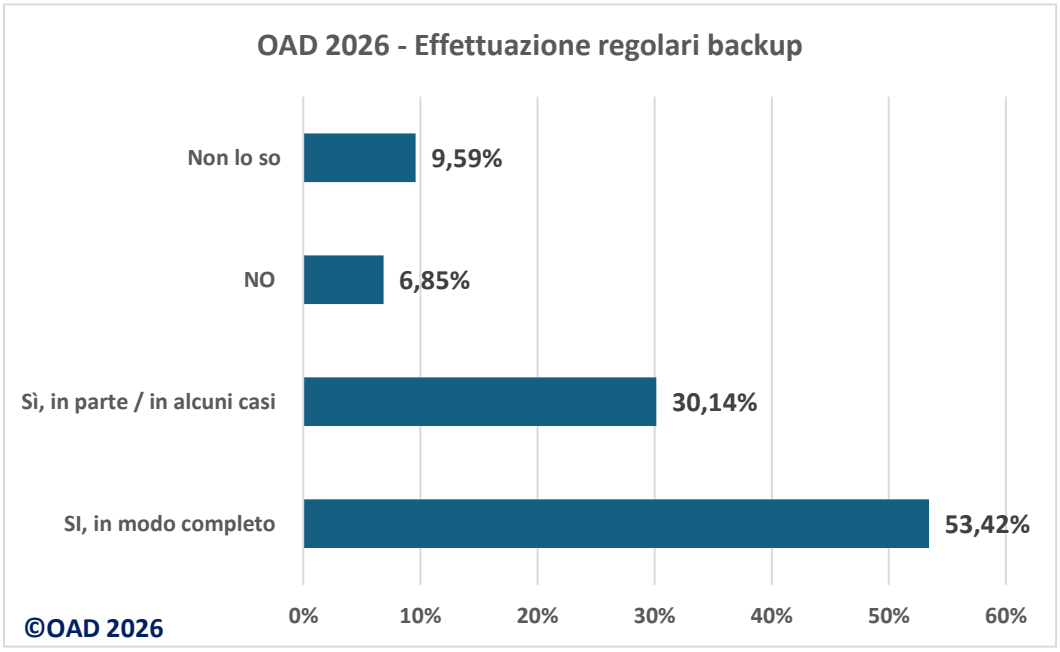


Fig. 7.2.5-1

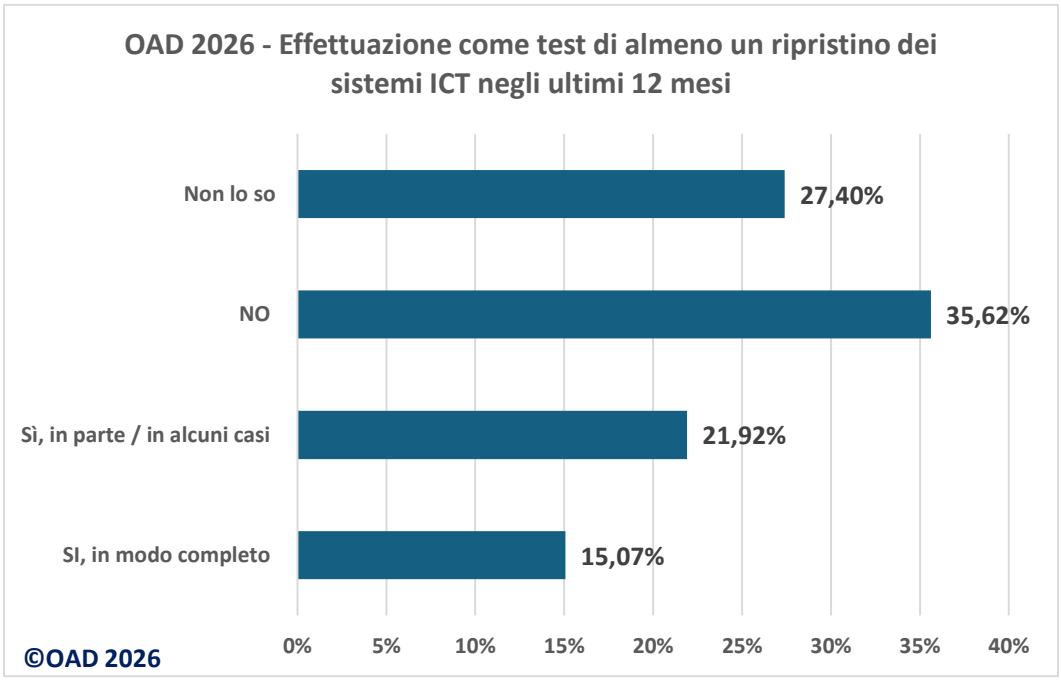


Fig. 7.2.5-2

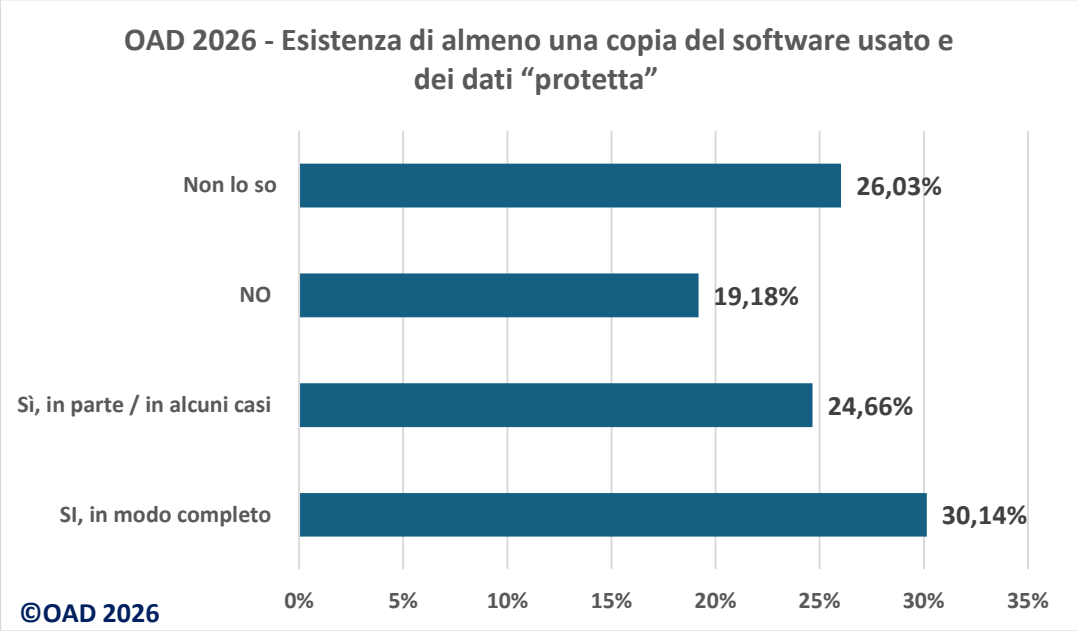


Fig. 7.2.5-3

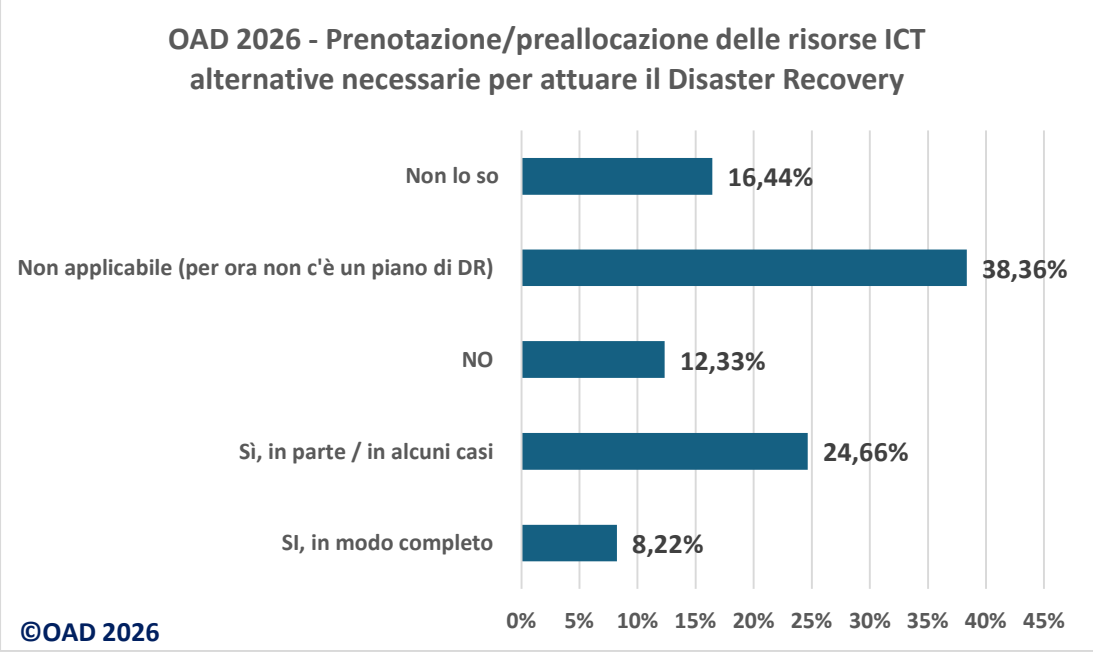


Fig. 7.2.5-4

🔍 **La diffusione delle misure di protezione non coincide necessariamente con la capacità di ripristino**. I risultati dell'indagine OAD 2026 evidenziano, tra i sistemi informativi dei rispondenti, una diffusione relativamente elevata di alcune misure tecniche tradizionali di sicurezza, quali firewall, sistemi di autenticazione multifattoriale e backup. Risultano invece meno diffuse le attività di verifica del ripristino e la predisposizione di piani di Disaster Recovery con adeguate risorse alternative. È una differenza significativa: **proteggere un sistema informativo è essenziale, ma lo è altrettanto essere in grado di ripristinarne tempestivamente il funzionamento dopo un incidente grave**.

7.2.6 Monitoraggio della sicurezza digitale e gestione Log

Si è già indicato in precedenza come il monitoraggio dei sistemi informativi (SI) e della loro sicurezza sia essenziale per la sicurezza digitale, dato che rileva, o può rilevare, non funzionamenti, anomalie e/o attacchi digitali del SI e segnalarle a chi di dovere perché possa intervenire tempestivamente. Questo tipo di servizio può essere gestito internamente all'organizzazione o può essere terziarizzato.

Il **70,83%** delle organizzazioni rispondenti dispone ed utilizza questo servizio per l'intero SI o per sue parti, si veda fig. 7.2.6-1.

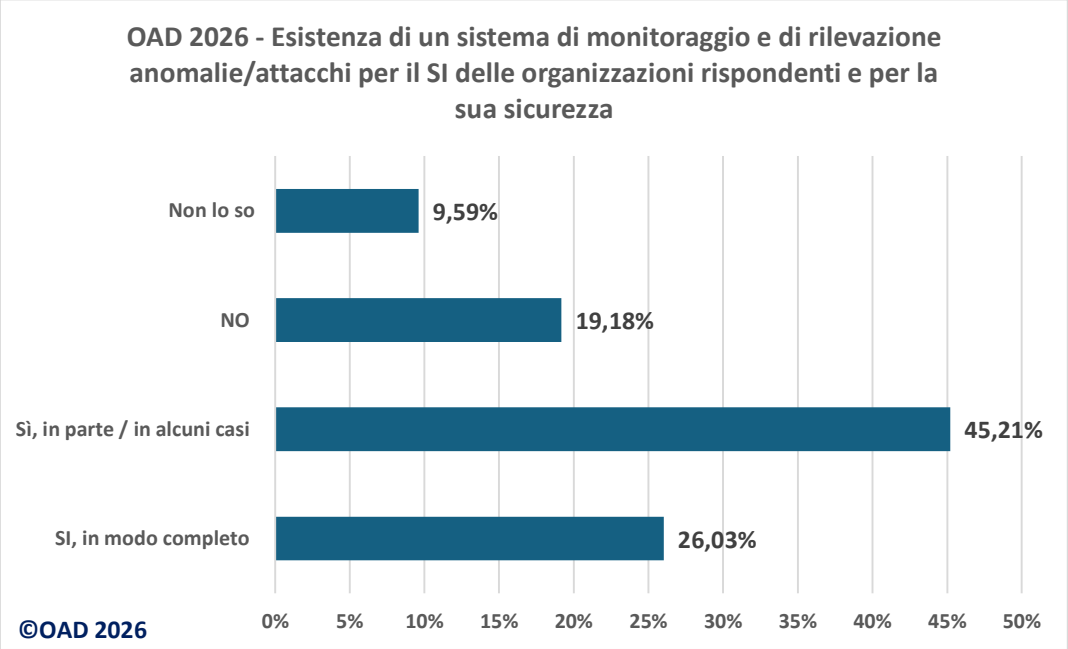


Fig. 7.2.6-1

Per un primo approfondimento su questo argomento si veda "OAD Insight #11 - Il monitoraggio continuo della sicurezza digitale" in https://www.oadweb.it/it/comunita-oad/oad-insight/oad-insight-11-il-monitoraggio-continuo-della-sicurezza-digitale.html

L'archiviazione ed il controllo dei log[21] di sistema e degli utenti sono strumenti importanti per la gestione della sicurezza digitale:

- a livello dei log di sistema per l'analisi del comportamento della risorsa ICT, diagnosticare malfunzionamenti e individuare problemi di sicurezza o intrusioni;
- a livello dei log d'utente per l'analisi del comportamento, l'audit di sicurezza, la conformità a normative e per risalire alle responsabilità in caso di violazioni.

Se opportunamente configurati, tutte le risorse ICT producono log. Occorre archiviarli per un dato periodo e soprattutto gestirli e correlarli tra loro per poter rilavare effettivi problemi. Questa analisi oggigiorno non può

[21] Un file di **log** è un registro cronologico e sequenziale che traccia eventi, operazioni, errori o richieste all'interno di un sistema informatico, di un software o di un dispositivo. I **log di sistema** registrano le attività del sistema operativo, dei server, del kernel, dei driver e dei servizi di rete. I **log d'utente** tracciano le interazioni, i tentativi di autenticazione e le azioni specifiche compiute dai singoli utenti all'interno di un'applicazione, di un sito web o di una rete.

che essere effettuata in maniera automatica, data la loro quantità, ed esistono dei sistemi, come i SIEM, Security Information and Event Management [22], che permettono di farlo.

La domanda su questo tema del questionario OAD 2026 si limitava a chiedere se si conservano e si consultano i log di accesso almeno per la posta elettronica e per i sistemi critici dell'organizzazione, eventualmente anche terziarizzando queste attività ad uno o più fornitori.

Il **70,83%** delle organizzazioni rispondenti lo fa, ma solo il 26,39% lo fa in modo completo, si veda fig. 7.2.6-2.

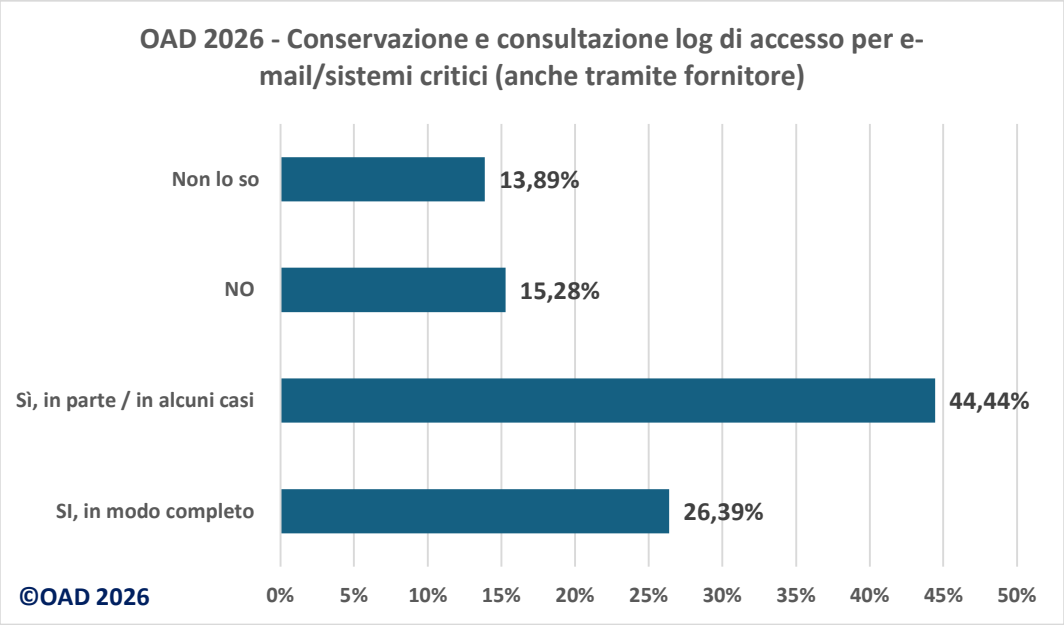


Fig. 7.2.6-2

7.2.7 Gestione vulnerabilità e incidenti

Come si sa, o si dovrebbe sapere, qualsiasi attacco digitale avviene sfruttando delle vulnerabilità tecniche dei sistemi ICT, oppure delle vulnerabilità delle persone o della struttura dell'organizzazione.

La prima domanda del questionario OAD 2026 su questo tema verteva sull'analisi periodica e la gestione delle vulnerabilità tecniche riscontrate nelle risorse ICT del Sistema Informativo dei rispondenti.

La risposta è nella fig. 7.2.7-1: i 2/3 delle organizzazioni analizzano e gestiscono periodicamente le vulnerabilità tecniche, ma solo 1/5 lo fa in modo completo.

Come già indicato in precedenza, la gestione degli incidenti digitali, che possono includere gli attacchi, è uno dei punti chiave nella gestione della sicurezza digitale. In primo luogo, occorre rilevare l'incidente quanto prima possibile, e capire i suoi impatti per qualificarne la gravità, e poi ben sapere cosa fare nell'immediato, ossia nelle prime 24 ore, per minimizzare i danni e gli impatti, e poter quanto prima riattivare/porre in normale funzionamento le risorse ICT coinvolte. Aspetti tecnici si devono integrare con aspetti organizzativi.

Determinante poi saper chi informare e come: certe normative, come ad esempio la NIS2, lo impongono verso sedi istituzionali, ad esempio nel caso NIS2 verso l'ACN.

[22] Si veda "OAD Insight #15 - SIEM: uno strumento di raccolta ed analisi degli eventi in un Sistema Informativo", in https://www.oadweb.it/it/comunita-oad/oad-insight/oad-insight-15-siem.html

Vulnerabilità è la condizione e/o la predisposizione di una persona, un sistema o un organismo a essere ferito, colpito o danneggiato da fattori esterni o interni (fisici, emotivi, sociali o ambientali). Il termine deriva dal latino "vulnus", ferita.

Vulnerabilità tecniche. Sono riscontrabili in ogni prodotto/servizio ICT, di qualsiasi produttore (incluse le comunità che sviluppano sistemi opensource). Le vulnerabilità tecniche individuate sono normalmente registrate nella banca dati mondiale **CVE**, Common Vulnerabilities and Exposures (https://www.cve.org/), con un codice di riferimento, una descrizione e le modalità per eliminarla o ridurre i suoi impatti, se tali modalità esistono e sono state provate. Alla data della pubblicazione del presente Rapporto OAD 2026, sono stati individuate e pubblicate 412.000 vulnerabilità in CVE. Esse sono in continuo aumento: a ottobre 2025 erano 296.000, a settembre 2024 240.830, a settembre 2023 212.202. È bene evidenziare che non tutte le vulnerabilità esistenti sono state individuate e classificate negli elenchi CVE. Quelle non ancora individuate, o sconosciute al produttore o ai responsabili della loro correzione, e per le quali non è ancora disponibile una correzione sono indicate con il termine "**zero-day**": sono le più critiche, perché non prevedono ancora una specifica correzione e, se l'attaccante le conosce, può sfruttarle. Inoltre, per alcune vulnerabilità conosciute, sono occorsi talvolta mesi prima di avere a disposizione una patch/fix correttiva; pertanto, esistono vulnerabilità note ma ancora senza una correzione disponibile.

Occorre distinguere tra vulnerabilità identificate e vulnerabilità effettivamente corrette. La scansione periodica non è sufficiente se non segue una gestione delle priorità e degli interventi di mitigazione.

Vulnerabilità delle persone. In ambito digitale, le vulnerabilità di una persona fanno riferimento al suo "fattore umano", ossia ai suoi punti deboli cognitivi, emotivi, psicologici, comportamentali ed organizzativi.

Le vulnerabilità delle persone rappresentano per il mondo digitale rischi ancora più diffusi e gravi rispetto a quelle tecniche: e sono amplificate dalle vulnerabilità organizzative. Tipiche vulnerabilità personali includono l'incompetenza nell'uso di certi strumenti informatici, poca attenzione e pressapochismo, fretta e urgenza, sudditanza, curiosità, troppa fiducia, mancanza di consapevolezza, disattenzione, stress. Per le vulnerabilità personali lo strumento di contrasto più importante è la formazione continua e la consapevolezza che, nell'uso dei sistemi informativi, occorre comportarsi sempre in maniera attenta ed etica, seguendo le indicazioni che dovrebbero essere state divulgate dall'azienda/ente in termini di policy, linee guida e procedure organizzative.

Vulnerabilità organizzative. Queste vulnerabilità fanno riferimento sia all'interno dell'organizzazione che all'esterno. In ambito interno, esse includono la mancanza di policy e procedure organizzative sull'ICT in generale e sulla sicurezza digitale in particolare, oltre che ruoli e relazioni tra loro non ben definite e sovrapposte, che non consentono una reale separazione di ruoli e di responsabilità. In ambito esterno la mancanza di contratti coi fornitori, consulenti inclusi, con SLA, Service Level Agreement, ben definiti e la mancanza di controlli effettivi.

La fig. 7.2.7-2 mostra che l'87,50% delle organizzazioni rispondenti sanno cosa fare, chi coinvolgere e chi avvertire/informare in caso di incidente digitale.

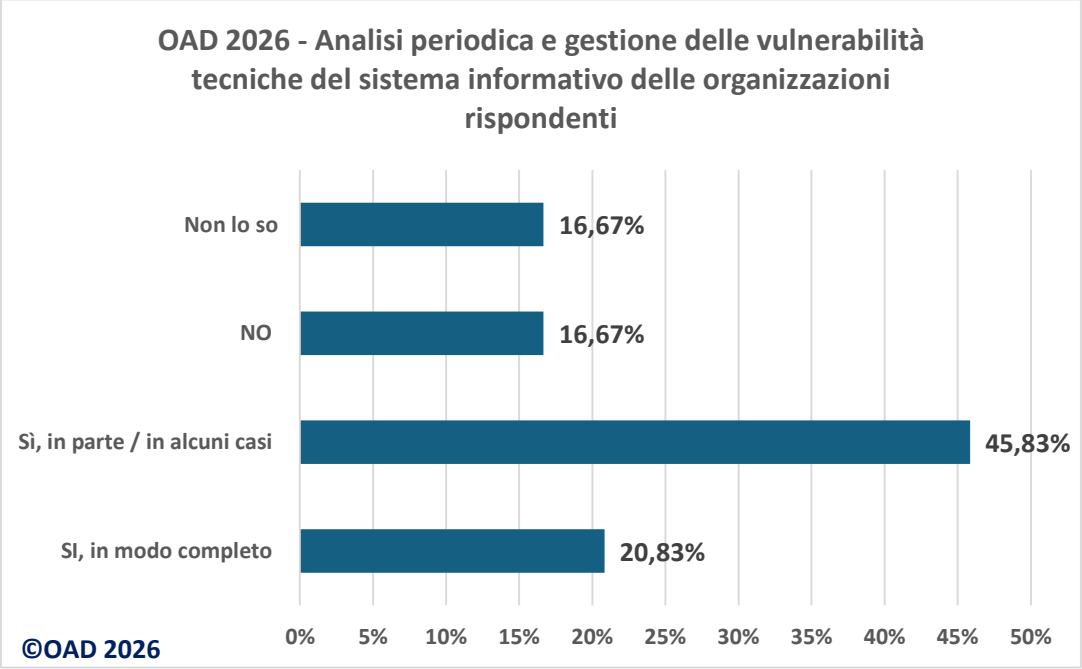


Fig. 7.2.7-1

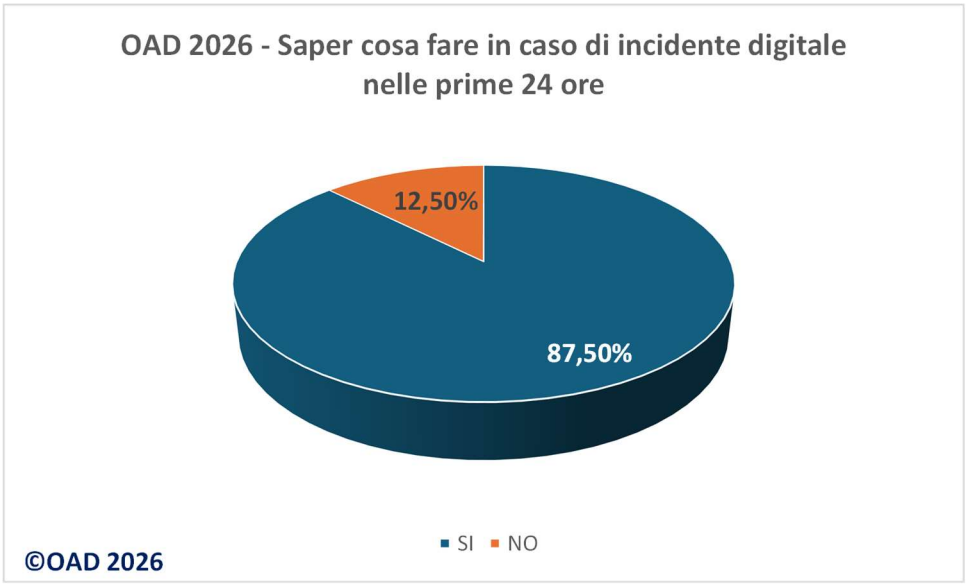


Fig. 7.2.7-2

8. I dati dal Servizio Polizia Postale e per la Sicurezza Cibernetica

OAD riporta in questo capitolo l'intero contributo del "Servizio Polizia Postale e per la Sicurezza Cibernetica[23]", in precedenza chiamato "Polizia Postale e delle Telecomunicazioni", mantenendo il formato grafico con cui è stato fornito, da parte dell'Ispettore **Gaetano Martucci,** dell'Assistente **Luigi Ummaro**, dell'Agente **Valeria Pettirossi**, che l'autore e OAD **ringraziano vivamente** insieme anche al **Direttore** del Servizio Polizia Postale, dott. **Ivano Gabrielli**.

La Polizia Postale da anni collabora con OAD, fornendo significativi dati sulle azioni svolte in Italia nel contrasto agli attacchi digitali e ai crimini informatici, facendo in particolare riferimento alle infrastrutture critiche, al crimine digitale finanziario, al cyber terrorismo, tutti temi che si inquadrano negli attacchi digitali trattati da OAD.

Per quanto riguarda i dati sulla protezione delle infrastrutture critiche e dei servizi essenziali, la Polizia Postale ha una propria struttura, il C.N.A.I.P.I.C., Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche[24], incaricata in via esclusiva della prevenzione e della repressione dei crimini informatici che hanno come obiettivo le infrastrutture ICT critiche ed i servizi ICT essenziali per il funzionamento del sistema paese.

Nella fig. 8-1 sono messe a confronto le informazioni ricevute da OAD negli anni dalla CNAIPIC **sugli attacchi alle infrastrutture critiche e ai servizi essenziali**.

La tabella evidenzia che il numero di attacchi rilevati nel 2025 è **diminuito del 21,71%** rispetto ai valori, molto simili, del 2023 e del 2024, In questa tabella il 2022 costituisce il picco degli attacchi nell'arco temporale considerato, e coincide con il picco di attacchi rilevati nelle indagini OAD, come mostrato nella precedente fig. 4.1-1.

Per il 1° semestre 2026 i dati sugli attacchi, così come quelli sulle persone indagate, sono poco meno della metà di quelli del 2025. Se si confermasse anche nel secondo semestre tale andamento, avremmo un 2026 con valori complessivamente simili o leggermente inferiori rispetto a quelli del 2025.

Il numero di indagati sul numero di attacchi rilevati rimane molto basso, così come negli anni precedenti: è un indicatore della effettiva difficoltà di individuare e attribuire gli attacchi digitali ai relativi autori.

Nella fig.8-2 sono messi a confronto le informazioni ricevute dalla Polizia Postale per il contrasto al **cyber terrorismo**.

Dal 2018 OAD ha avuto informazioni sul controllo dei siti web, dal 2022 si sono aggiunti i dati sugli "Spazi Virtuali con contenuti illeciti rilevati" e su "Spazi oscurati per attività Info-investigative".

Dalla tabella emerge che:

- **i siti web esaminati** dalla Polizia Postale nel 2025 sono diminuiti del 20,57% rispetto al 2024;
- gli **Spazi Virtuali con contenuti illeciti rilevati** nel 2025 sono stati poco più della metà (56,27%) rispetto al 2024;
- gli **spazi virtuali oscurati** nel 2025 sono stati il 77,16% rispetto al 2024, quindi con una riduzione di circa ¼ rispetto all'anno precedente, e costituiscono poco più di ¼ degli Spazi Virtuali con contenuti illeciti rilevati nel 2025.

[23] Il "Servizio Polizia Postale e per la Sicurezza Cibernetica" per brevità viene indicato nel seguito come "Polizia Postale"
[24] https://www.commissariatodips.it/profilo/cnaipic/index.html

La riduzione dei valori rispetto al 2024 evidenzia una minore quantità di spazi monitorati, di contenuti illeciti rilevati e di oscuramenti effettuati. Il dato, tuttavia, non consente da solo di stabilire se tale andamento sia riconducibile a una effettiva diminuzione della presenza online di contenuti connessi all'estremismo e al terrorismo, a una loro migrazione verso canali meno accessibili o ad altri fattori connessi alle modalità di monitoraggio. Rimane pertanto essenziale la continua attività di sorveglianza e di prevenzione svolta dalle strutture competenti.

Non esiste una chiara ed univoca definizione di cyber-terrorismo, e l'autore ha ritenuto opportuno, con questa edizione, soffermarsi sul tema con il seguente approfondimento.

Cyber-terrorismo

Il **cyber terrorismo** può essere definito come l'impiego intenzionale di strumenti e sistemi informatici, oppure l'attacco deliberato a sistemi digitali e infrastrutture da essi controllate, **finalizzato al perseguimento di obiettivi terroristici**, quali intimidire gravemente una popolazione, condizionare o costringere le istituzioni pubbliche o destabilizzare strutture fondamentali della società per finalità politiche, ideologiche o religiose.

Non esiste una definizione universalmente condivisa di cyber terrorismo. È pertanto opportuno distinguere il cyber terrorismo in senso stretto dall'utilizzo delle tecnologie digitali a supporto delle attività terroristiche.

Nel primo caso, definibile anche come **cyber-dependent terrorism**, il cyberspazio costituisce direttamente il mezzo attraverso il quale viene realizzato l'attacco. Possono rientrare in questa fattispecie, qualora siano presenti finalità terroristiche e conseguenze sufficientemente gravi, il sabotaggio di infrastrutture critiche e di servizi essenziali, la compromissione di sistemi industriali e cyber-fisici, l'interruzione prolungata di servizi fondamentali o altre azioni volte a produrre effetti fisici, economici o sociali tali da intimidire la popolazione o esercitare una coercizione nei confronti delle istituzioni.

Nel secondo caso, più propriamente definibile come **utilizzo del cyberspazio per finalità terroristiche** o ***cyber-enabled terrorism***, le tecnologie digitali svolgono invece una funzione di supporto ad attività terroristiche realizzate anche al di fuori del cyberspazio. Rientrano in questa categoria l'attività di propaganda, radicalizzazione e reclutamento, il finanziamento, le comunicazioni tra appartenenti alle organizzazioni, l'acquisizione di informazioni sui potenziali obiettivi, la pianificazione degli attentati e la successiva attività di rivendicazione e amplificazione mediatica.

Elemento fondamentale per qualificare un attacco come cyber terrorismo non è pertanto la sola presenza di una motivazione politica o ideologica, ma la combinazione tra **finalità terroristica, intento di intimidazione o coercizione e gravità degli effetti perseguiti**.

In particolare, il cyber terrorismo non deve essere automaticamente assimilato all'hacktivism. Attacchi DDoS, defacement di siti o altre azioni dimostrative compiute da gruppi politicamente o ideologicamente motivati possono determinare significative conseguenze operative, ma non assumono necessariamente natura terroristica. La qualificazione dipende dalle finalità perseguite, dalla natura dell'organizzazione responsabile e, soprattutto, dalla portata degli effetti prodotti o intenzionalmente ricercati.

La crescente digitalizzazione dei Paesi occidentali e l'interdipendenza tra reti informatiche, infrastrutture critiche e servizi essenziali rendono tuttavia particolarmente rilevante questo tipo di minaccia: un'azione condotta esclusivamente nel dominio digitale può infatti propagare i propri effetti nel mondo fisico, incidendo sul funzionamento di servizi essenziali, sulla sicurezza delle persone e, nei casi più gravi, sulla stabilità economica e sociale.

Per il **crimine digitale finanziario**, dal 2022 la Polizia Postale ha fornito specifiche informazioni sulle "frodi informatiche" e sulle "truffe online", che in precedenza non erano distinte in questo modo ma raggruppate come "financial cyber crime" e per il quale venivano forniti dati sul numero di Transazioni Fraudolente Bloccate, sulle Somme Recuperate in €, sul numero di denunciati e di arrestati (questi due numeri non sono più stati forniti dal 2016).

Dato che le informazioni avute sul "financial cyber crime" non sono confrontabili con le nuove informazioni su frode informatica e truffa on line, OAD ha confrontato, nelle figure seguenti, solo queste ultime, disponibili dal 2022.

È opportuno chiarire la differenza principale tra frode informatica e truffa online, che talvolta sono considerati sinonimi. La differenza sta nell'**oggetto della condotta fraudolenta**: la **truffa online** induce in errore la vittima tramite "artifizi e raggiri" per ottenere un profitto, mentre **la frode informatica** (disciplinata dall'art. 640 ter del Codice penale) consiste nella manipolazione e alterazione di un sistema informatico o telematico, o nell'intervento non autorizzato su dati e programmi al suo interno, per ottenere un ingiusto profitto.

La fig. 8-3 confronta i dati forniti dalla Polizia Postale sulle **frodi informatiche** ed evidenzia:

- un decremento del -7,87 % dei casi trattati tra il 2025 ed il 2024;
- un decremento del -17,77 % delle persone indagate tra il 2025 ed il 2024;
- una riduzione delle somme sottratte con queste frodi del -3,17%.

La fig. 8-4 confronta i dati forniti dalla Polizia Postale sulle **truffe online** ed evidenzia un crescente aumento dei casi trattati, delle persone indagate e delle somme sottratte. In particolare:

- un incremento del 3,83% sul numero di casi trattati tra il 2025 ed il 2024;
- un incremento del 6,12% delle persone indagate tra il 2025 ed il 2024;
- un notevole aumento, del 24,72%, delle somme sottratte con queste truffe;

Nell'arco temporale considerato, 2022-2025, i valori delle truffe online **sono sempre aumentati**.

Comparando le due figure 8-3 e 8-4, emerge innanzitutto una diffusione quantitativamente molto maggiore delle truffe online rispetto alle frodi informatiche. Queste ultime, per le modalità con cui vengono realizzate, possono richiedere maggiori competenze tecniche rispetto alle truffe basate prevalentemente sull'inganno della vittima. Le somme sottratte nell'ambito delle frodi online sono assai inferiori rispetto a quelle delle truffe online: in tutti gli anni considerati, quelle delle truffe hanno un fattore moltiplicativo di più di 3 volte rispetto alle frodi.

⚠ La frase della Polizia Postale "campagne di disinformazione orchestrate con intelligenza artificiale hanno instillato dubbi su verità consolidate, minando la coesione sociale e sollevando interrogativi su come proteggere la democrazia in uno spazio dove il confine tra reale e virtuale si è fatto labile" evidenzia uno dei fenomeni più critici per le democrazie liberali: l'impiego delle tecnologie digitali, e sempre più dell'intelligenza artificiale, nella **produzione e diffusione sistematica di disinformazione** in grado di incidere sulla fiducia nelle istituzioni e sulla coesione sociale. Si tratta pertanto di un ambito che richiede una costante attività di prevenzione, individuazione e contrasto, come già considerato nel Cap.3.

Il documento della Polizia Postale, riprodotto nelle pagine seguenti, considera anche altri temi, legati ai suoi compiti di prevenzione e repressione del crimine informatico, che esulano dal perimetro dell'indagine OAD, ma che sono assai significativi per comprendere nel suo complesso il fenomeno del crimine informatico:

- **pedopornografia online**: 2876 i siti web messi in black list, e significativo il ruolo dei social net nell'adescamento on line; significativa ed efficace, inoltre, l'azione della Polizia Postale che ha indagato un numero di persone che è circa la metà dei casi trattati; nel corso di vent'anni di attività sono stati arrestati più di 1600 criminali;
- **commissariato di PS online**: primo presidio virtuale di polizia in Europa, da quasi vent'anni è il portale informativo e lo strumento di assistenza e di denuncia di attacchi e crimini informatici. Nel 2025 più di 5 milioni di consultazioni e sono state gestite 125.887 pratiche
- **reati contro la persona**: includono i furti di identità digitale, campagne denigratorie, estorsioni a sfondo sessuale, e così via. Nel 2025, 1.315 persone indagate nei confronti di quasi 10.000 casi trattati.

⚠ Tutti i dati forniti dalla Polizia Postale, unitamente alle considerazioni contenute nel contributo riportato nelle pagine seguenti e pienamente condivise dall'autore, confermano la rilevanza e la pervasività della criminalità cyber in Italia. Assume particolare significato la persistenza degli attacchi rivolti anche a infrastrutture critiche e servizi essenziali, ossia a sistemi che, per rilevanza e potenziale impatto, dovrebbero essere caratterizzati da elevati livelli di protezione. Nel loro complesso, tali evidenze contribuiscono a confermare la valutazione, già sviluppata nei precedenti capitoli del Rapporto OAD, di una condizione di **insicurezza digitale sistemica** che continua a caratterizzare il Sistema-Paese tra il 2020 e il 2026.

Protezione strutture critiche/essenziali	1° semestre 2026	1 gen - 31 dic 2025	1 gen - 31 dic 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Attacchi rilevati (*)	4032**	9440**	12.058 **	12.101 **	13.099	282	509	1181	459	1.032	844
Alert diramati	n.d.	54.554	59.875	77.012	113.420	24.824	83.416	82.484	80.777	31.524	6.721
Indagini avviate	n.d.	n.d.	n.d.	96	110	34	103	155	74	72	70
Persone denunciate/indagate (*)	84**	171**	178 **	224**	334	n.d.	105	117	14	1.316	1.226
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	n.d.	47	63	79	77	17	69	79	108	83	85

Fig. 8-1 (Fonte: elaborazione OAD su dati storici del Servizio Polizia Postale e per la Sicurezza Cibernetica)

Cyber Terrorismo	1° semestre 2026	1 gen -31 dic 2025	1 gen - 31 dic 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018
Spazi web monitorati	n.d.	234.709	295.493	182.209	175.572	11.962	37.081	36.377	36.000
Spazi Virtuali con contenuti illeciti rilevati	n.d.	2.002	4.642	2.037	1.598				
Spazi oscurati per attiv. infoinvestigative	n.d.	541	2.369	2.700	338				

Fig. 8-2 (Fonte: elaborazione OAD su dati storici del Servizio Polizia Postale e per la Sicurezza Cibernetica)

Frodi informatiche	1° semestre 2026	1 gen -31 dic 2025	1 gen - 31 dic 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022
Casi trattati	n.d.	7.925	8.602	10.755	5.908
Persone indagate	n.d.	759	923	927	725
Somme sottratte (€)	n.d.	46.793.621	48.674.917	40.503.616	35.509.160

Fig. 8-3 (Fonte: elaborazione OAD su dati storici del Servizio Polizia Postale e per la Sicurezza Cibernetica)

Truffe online	1° semestre 2026	1 gen -31 dic 2025	1 gen - 31 dic 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022
Casi trattati	n.d.	19.694	18.967	16.637	15.699
Persone indagate	n.d.	3.849	3.627	3.610	3.570
Somme sottratte (€)	n.d.	228.713.334	183.377.101	139.536.457	116.454.550

Fig. 8-4 (Fonte: elaborazione OAD su dati storici del Servizio Polizia Postale e per la sicurezza cibernetica)



Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA
DIREZIONE CENTRALE PER LA POLIZIA SCIENTIFICA E LA SICUREZZA CIBERNETICA
SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA



POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Contributo statistico per l'Osservatorio Attacchi Digitali in Italia

ANNO 2025

e

Primo Semestre 2026

(fonte dati: mattinale Polizia Postale e per la sicurezza cibernetica)

Dati aggiornati al 30 giugno 2026

Roma, 18 settembre 2026

Isp. della Polizia di Stato
Gaetano Martucci

Ass. C. della Polizia di Stato
Luigi Ummaro

Agt. della Polizia di Stato
Valeria Pettirossi

PREMESSA



Il dominio cibernetico non è più riconducibile a un singolo settore. È ormai parte integrante del funzionamento dell'intero sistema economico e sociale e rappresenta una delle principali infrastrutture attraverso cui si sviluppano attività produttive, servizi pubblici e relazioni tra cittadini, imprese e istituzioni. La digitalizzazione, in questo quadro, non costituisce soltanto uno strumento di efficientamento, ma una condizione essenziale per la competitività e lo sviluppo delle economie contemporanee.

La crescente diffusione delle tecnologie digitali pone, tuttavia, nuove sfide per la sicurezza che richiedono un approccio costantemente aggiornato. La sfida non consiste soltanto nell'adottare tecnologie avanzate, a partire dall'intelligenza artificiale, ma soprattutto nel garantire la sicurezza dell'ambiente digitale nel quale tali tecnologie vengono sviluppate e utilizzate.

Il 2026 rappresenta, sotto il profilo normativo, un passaggio particolarmente significativo. L'attuazione dell'*AI Act* europeo, accompagnata dai recenti interventi normativi adottati nel nostro ordinamento, segna una nuova fase nella governance dell'intelligenza artificiale, nella quale innovazione, sicurezza e responsabilità devono procedere insieme.

L'intelligenza artificiale può infatti rafforzare le capacità di prevenzione e contrasto delle minacce informatiche, ma gli stessi strumenti possono essere utilizzati dagli autori di reato per rendere più efficaci e difficili da individuare le proprie attività. I modelli generativi, ad esempio, possono essere impiegati in modo distorto per elaborare schemi di frode complessi o generare contenuti artefatti, rendendo necessaria un'evoluzione parallela degli strumenti di contrasto.

Di fronte a questa evoluzione, le Forze di polizia devono poter disporre di strumenti tecnologici adeguati alla complessità della minaccia. Sistemi capaci di individuare tempestivamente anomalie e comportamenti illeciti possono rappresentare un importante supporto all'attività investigativa, purché il loro impiego avvenga nel pieno rispetto delle garanzie previste dall'ordinamento.

La tecnologia, d'altra parte, non sostituisce l'attività dell'operatore. La componente umana rimane centrale nella definizione delle metodologie, nell'addestramento dei sistemi, nella valutazione dei risultati e nelle decisioni investigative. È un principio coerente con l'approccio antropocentrico posto alla base della disciplina europea e nazionale dell'intelligenza artificiale.

In tale scenario, la missione della Polizia di Stato si estende naturalmente anche allo spazio cibernetico. Nell'anno in cui ricorre il 174° Anniversario della sua fondazione, il principio dell'"Esserci Sempre" trova una nuova dimensione anche nella rete: prevenire, intervenire e assistere significa oggi essere presenti anche nei luoghi virtuali nei quali si sviluppano nuove forme di criminalità e di vulnerabilità.

La sicurezza informatica, pertanto, non può più essere considerata esclusivamente una questione tecnica. È un elemento strategico per assicurare la continuità dei servizi, la tutela delle persone e la stabilità del Sistema-Paese. Al tempo stesso, nessuna tecnologia può essere realmente efficace senza una diffusa cultura della sicurezza digitale, capace di coinvolgere istituzioni, imprese e cittadini.

Il presente documento intende offrire un quadro aggiornato delle principali dinamiche del cybercrime e delle attività di prevenzione e contrasto sviluppate dalla Polizia Postale e per la Sicurezza Cibernetica. Conoscere l'evoluzione della minaccia è infatti il primo passo per poterla affrontare in modo efficace e fare in modo che l'innovazione rimanga una risorsa, anziché trasformarsi in una nuova fonte di rischio.

I dati relativi all'attività operativa del 2025 restituiscono un quadro articolato. Nel corso dell'anno sono stati gestiti 9.440 eventi informatici di rilievo, 967 dei quali hanno riguardato attacchi contro sistemi di servizi pubblici essenziali e infrastrutture critiche.

Il 2025 segna anche il ventennale del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), istituito nel 2005. Nel corso dei suoi vent'anni di attività, il Centro ha consolidato il proprio ruolo nella protezione degli asset strategici del Paese, sviluppando una rete di collaborazione con soggetti pubblici e privati. La cooperazione con i gestori delle infrastrutture e dei servizi essenziali costituisce uno degli strumenti fondamentali per prevenire e affrontare minacce capaci di compromettere la continuità operativa.

Il fenomeno criminale incide in modo significativo anche sulla sfera economica e patrimoniale dei cittadini. Nel 2025 sono state raccolte 27.619 denunce relative a truffe e frodi telematiche. Dati che confermano come la tutela della sicurezza informatica sia

ormai un elemento imprescindibile non solo per le infrastrutture, ma per la serena fruizione dei servizi digitali da parte dei cittadini.

Un ambito distinto è quello della sicurezza dello Stato e del contrasto all'estremismo online. Nel corso delle attività di monitoraggio sono state esaminate 234.709 piattaforme virtuali, con l'oscuramento di 541 spazi illeciti. Si tratta di un'attività che assume rilievo in un ambiente caratterizzato dalla presenza di reti transnazionali, soggetti non statuali e attori operanti anche dall'estero.

La dimensione internazionale del cybercrime rende indispensabile una cooperazione costante tra le autorità investigative dei diversi Paesi. Strumenti quali l'Ordine Europeo di Indagine e le Squadre Investigative Comuni, anche con il supporto di Eurojust ed Europol, consentono di coordinare attività investigative che, per loro stessa natura, non possono essere efficacemente condotte entro i soli confini nazionali.

Tra gli interventi più significativi del 2025 rientrano l'operazione "*Eastwood*", diretta nei confronti del collettivo "*NoName057(16)*", e il sequestro e la chiusura delle piattaforme "*Cracked*" e "*Nulled*", storicamente utilizzate nell'ambito delle attività criminali online.

La cooperazione internazionale incontra tuttavia ancora alcuni ostacoli. Le differenze tra gli ordinamenti nazionali possono rallentare le procedure investigative, soprattutto quando è necessario acquisire prove digitali conservate all'estero o ricostruire movimenti finanziari effettuati attraverso criptovalute. A ciò si aggiunge la crescente disponibilità di strumenti di intelligenza artificiale, che possono essere utilizzati per facilitare diverse forme di criminalità informatica e rendere più rapida l'esecuzione di alcune attività illecite.

Sul piano nazionale, la prevenzione si sviluppa anche attraverso la collaborazione con i gestori delle reti e dei servizi maggiormente esposti e attraverso iniziative con il mondo accademico. In questo ambito, strumenti come la *cyber threat intelligence* e la *cyber deception* contribuiscono a individuare le minacce e a rafforzare la capacità di prevenire attacchi mirati contro infrastrutture e servizi essenziali.

La prevenzione passa, però, anche dalla consapevolezza degli utenti. Nel 2025 le campagne "Una Vita da Social" e "Cuori Connessi" hanno coinvolto 4.335 istituti scolastici e oltre 330.000 studenti. Nello stesso anno, il portale del Commissariato di P.S. Online ha registrato oltre cinque milioni di consultazioni, confermandosi uno strumento importante per informare i cittadini, favorire la prevenzione e facilitare il ricorso alle autorità in caso di necessità.

Questa funzione di prossimità acquista un valore particolare nel 2026, anno in cui ricorre il ventennale del Commissariato di P.S. Online, istituito nel 2006 come primo presidio virtuale di polizia in Europa. In vent'anni, la piattaforma ha accompagnato l'evoluzione della criminalità digitale e delle esigenze dei cittadini, diventando un punto di riferimento per la segnalazione e la gestione dei fenomeni emergenti. Nel solo 2025 sono state gestite 125.887 pratiche.

Il Commissariato svolge oggi una duplice funzione: da un lato rappresenta un importante punto di osservazione sull'evoluzione dei fenomeni criminali online; dall'altro costituisce un presidio di assistenza e intervento nelle situazioni che richiedono una risposta tempestiva, comprese quelle relative alle allerte per intenti suicidari.

Il cybercrime produce conseguenze rilevanti anche sulla sfera personale. Nel 2025 i reati contro la persona hanno dato luogo a 9.768 denunce. Tra i fenomeni più rilevanti rientrano quelli che colpiscono la reputazione, l'identità e la dimensione psicologica delle vittime. L'intelligenza artificiale generativa può rendere particolarmente rapida la produzione di contenuti falsi e deepfake, che possono essere utilizzati per campagne denigratorie, estorsioni a sfondo sessuale e furti di identità.

Nel dettaglio, la Polizia Postale ha trattato oltre 3.400 casi di sostituzione di persona, più di 2.300 episodi di diffamazione online e oltre 1.200 fascicoli relativi a sextortion. Si tratta di dati che confermano la necessità di affiancare all'attività investigativa e repressiva una concreta capacità di sostegno alle vittime, soprattutto nei casi in cui il danno prodotto dalla condotta criminale si estende alla sfera personale e psicologica.

La tutela dei minori resta una priorità. Nel 2026 ricorrono i vent'anni di attività del Centro Nazionale per il Contrasto della Pedopornografia Online (CNCPO), istituito per contrastare uno dei fenomeni criminali più gravi presenti nel web.

L'evoluzione delle modalità di comunicazione, l'utilizzo di reti anonime e la crescente diffusione della crittografia hanno reso più complessa l'attività investigativa. Per questo motivo, nel tempo, l'azione del Centro si è orientata sempre più verso l'individuazione dei soggetti che operano ai livelli superiori delle reti criminali e verso l'interruzione delle strutture che rendono possibile la produzione e la diffusione di materiale pedopornografico.

Nel corso dei vent'anni di attività sono stati arrestati oltre 1.600 soggetti. La Black List continua, inoltre, a svolgere una funzione preventiva attraverso l'inibizione dei siti illeciti: al 31 dicembre 2025 nella black list erano presenti 2.876 siti.

Nel complesso, i 52.590 fascicoli investigativi gestiti nel 2025, insieme agli elementi emersi nei primi mesi del 2026, delineano alcune priorità precise per il prossimo futuro: mantenere aggiornato il quadro normativo, investire nella formazione specialistica del personale, sviluppare strumenti tecnologici adeguati e rafforzare la cooperazione internazionale.

L'obiettivo rimane quello di rendere lo spazio digitale un ambiente sempre più sicuro e affidabile, nel quale cittadini, imprese e istituzioni possano continuare a utilizzare le opportunità offerte dalla tecnologia in una cornice di affidabilità e protezione.

La Polizia Postale e per la Sicurezza Cibernetica è chiamata, in questo processo, a adeguare costantemente strumenti e metodologie di intervento. La sicurezza digitale, tuttavia, non può essere affidata esclusivamente all'azione delle istituzioni. La trasformazione digitale richiede una responsabilità condivisa, nella quale alle capacità investigative e preventive delle Forze di polizia si affianchino comportamenti consapevoli da parte di cittadini, imprese e organizzazioni.

È dall'integrazione di queste componenti — istituzioni, tecnologia e responsabilità individuale — che può nascere una maggiore capacità del Paese di prevenire, affrontare e superare le minacce del cyberspazio.

Il Settore Analisi e Pianificazione Strategica
del Servizio Polizia Postale e per la sicurezza cibernetica
Ispettore Gaetano Martucci
Assistente Capo Luigi Ummaro

Agente Valeria Pettirossi

CENTRO NAZIONALE ANTICRIMINE INFORMATICO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE (C.N.A.I.P.I.C.) – COMPUTER CRIME

	1 gen – 31 dic 2025
Attacchi rilevati totali (*)	9.440
Alert diramati	50.445
Persone indagate (*)	171
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	47
Attacchi solo I.C. – OSE – PAL	***967***
Persone indagate solo I.C. – OSE – PAL	***49***

* Target: Infrastrutture Critiche (I.C.), Operatori Servizi Essenziali (OSE), Pubbliche Amministrazioni Locali (PAL), Aziende, Privati
** Dati aggregati C.N.A.I.P.I.C. e Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.).

-=oOOo=-

CENTRO NAZIONALE PER IL CONTRASTO DELLA PEDOPORNOGRAFIA ON-LINE (C.N.C.P.O.)

	1 gen – 31 dic 2025
Casi trattati pedopornografia e adescamento online	2.623
Persone indagate	1.309
Perquisizioni	1.039
Monitoraggi rete	16.609
Siti presenti in black list al 31/12/2025	2.876

-=oOOo=-

IL COMMISSARIATO DI P.S. ONLINE

	1 gen – 31 dic 2025
Segnalazioni	100.443
Informazioni	25.444
Visite	5.199.902
Accessi	75.830.724
Alert Diramati	28
Interventi finalizzati alla prevenzione di intenti suicidari	346

-=oOOo=-

PREVENZIONE CYBERTERRORISMO

Eversione Internazionale Estremismo religioso e politico *Eversione nazionale estrema destra, area antagonista, attività in circostanze di emergenza*	**1 gen – 31 dic 2025**
Spazi web monitorati	234.709
Spazi Virtuali con contenuti illeciti rilevati	2.002
Spazi oscurati per attiv. infoinvestigative	541

-=oOOo=-

LE FRODI INFORMATICHE

	1 gen – 31 dic 2025
Casi trattati	7.925
Persone indagate	759
Somme sottratte	46.793.621 €

-=oOOo=-

LE TRUFFE ONLINE

	1 gen – 31 dic 2025
Casi trattati	19.694
Persone indagate	3.849
Somme sottratte	228.713.334 €

=oOOo=-

REATI CONTRO LA PERSONA

	1 gen – 31 dic 2025
Casi trattati	9.768
Persone indagate	1.315

DATI STATISTICI PUBBLICABILI - PRIMO SEMESTRE 2026 (1° gen - 30 giu 2026)
(Dati Dossier Viminale 2026)[25]

- **Attacchi rilevati a danno di infrastrutture critiche:** 4.082 (corrispondente a un calo del 16,9% rispetto ai 4.911 attacchi del primo semestre 2025).
- **Indagati per attacchi alle infrastrutture critiche:** 84 indagati (in aumento del 71% rispetto al medesimo periodo del 2025).
- **Cyberterrorismo:** 89 eventi rilevati (con un decremento del 23,3% rispetto ai 116 del primo semestre 2025).

[25]https://www.interno.gov.it/sites/default/files/2026-08/dossier_viminale_2026.pdf

ALLEGATI

ALLEGATO A - Aspetti metodologici dell'indagine OAD 2026

L'indagine OAD 2026, come le precedenti, è indirizzata da un lato all'analisi totalmente anonima degli **attacchi digitali intenzionali** ai sistemi informativi (SI) delle aziende/enti rispondenti operanti in Italia (non agli incidenti ai SI causati da malfunzionamenti hardware e software, da errato/maldestro uso dei sistemi ICT da parte degli utenti e degli operatori, o da fenomeni accidentali esterni); dall'altro la rilevazione ed analisi, sempre in maniera anonima, delle **principali caratteristiche dei SI dei rispondenti**, e delle loro **misure di sicurezza**, sia tecniche che organizzative.

Per il questionario online sono da considerarsi gli attacchi che sono stati effettivamente rilevati, e non è necessario che essi abbiano creato danni ed impatti negativi al SI attaccato, ovvero che l'attacco non abbia avuto il successo sperato dall'attaccante.

L'attacco contro un SI va a buon fine quando si intende violato, con una attività non autorizzata, almeno uno dei requisiti della sicurezza ICT, intesa come la "protezione dei requisiti di integrità, disponibilità e confidenzialità" delle informazioni trattate, ossia acquisite, comunicate, archiviate e processate.

OAD costituisce una indagine indipendente online in Italia sugli attacchi digitali intenzionali ai sistemi informativi delle aziende e degli enti pubblici operanti in Italia. OAD non predefinisce uno specifico bacino di rispondenti, il medesimo negli anni, ma consente a chiunque, interessato e coinvolto nella gestione di un SI di una azienda/ente, un pieno e libero accesso al questionario online, in maniera totalmente anonima.

L'indagine OAD non ha pertanto valore strettamente statistico e non pretende di rappresentare quantitativamente l'intera realtà nazionale. Il numero e l'eterogeneità delle aziende e degli enti rispondenti consentono tuttavia di individuare fenomeni ricorrenti, situazioni critiche e tendenze utili alla comprensione dell'evoluzione degli attacchi digitali e delle misure di sicurezza adottate in Italia.

Il questionario è rigorosamente **anonimo**: non viene richiesta alcuna informazione personale e/o identificativa del compilatore e della sua azienda/ente, non viene rilevato e tanto meno registrato il suo indirizzo IP, sulla banca dati delle risposte non viene specificata la data di compilazione.

Tutti i dati forniti vengono usati solo a fini di analisi complessiva e per la produzione di grafici e tabelle di sintesi.

Il livello di dettaglio sulle caratteristiche tecniche dei sistemi ICT non consente in alcun modo di poter risalire alla azienda/ente rispondente.

L'autore garantisce la totale riservatezza sulle risposte raccolte.

Per limitare la possibilità di compilazioni multiple da parte dello stesso rispondente, il questionario utilizza una specifica funzionalità di LimeSurvey che, tramite cookie del browser, impedisce di norma una seconda compilazione dallo stesso browser dopo il completamento della prima. Tale meccanismo costituisce una misura di prevenzione, ma non garantisce l'impossibilità assoluta di compilazioni ripetute.

Per acquisire il maggior numero possibile di rispondenti, OAD, AICA, FIDAInform ed i Patrocinatori coinvolti invitano a compilare il questionario i potenziali rispondenti, tramite posta elettronica, social network e con specifiche pagine o messaggi sui loro siti web. Ulteriori inviti alla compilazione del questionario sono inoltre effettuati nell'ambito di eventi sull'ICT e sulla sicurezza digitale tenuti dall'autore, da AICA e da FidaInform.

Quando termina il periodo previsto per la compilazione del questionario, OAD elabora ed analizza i dati raccolti tramite fogli elettronici, e sulla base di tali elaborazioni viene redatto il rapporto finale, che viene pubblicato sul sito di OAD per poter essere scaricato gratuitamente da tutti gli interessati.

L'elaborazione dei dati raccolti inizia con l'eliminazione di quelli palesemente errati o che non hanno senso.

Il calcolo statistico per la creazione dei grafici differisce a seconda che le **risposte siano multiple** (l'utente può selezionare più risposte per la stessa domanda) **oppure no**, e se la domanda, con relative risposte, è un dettaglio rispetto ad una precedente risposta.

Per le risposte multiple ad una data domanda, il denominatore nel calcolo della percentuale è dato dal numero di rispondenti complessivo per quella domanda o insieme di domande, non per la sommatoria delle risposte avute: la somma finale delle percentuali di ogni singola risposta può essere pertanto superiore o inferiore al 100%.

Per le risposte singole ad una data domanda, il denominatore nel calcolo della percentuale è dato dalla somma dei rispondenti: la somma finale delle percentuali di ogni singola risposta è e deve essere 100%.

In alcuni casi le domande fanno riferimento ad una specifica risposta di una domanda precedente: per queste il valore al denominatore per il calcolo della percentuale è dato dal numero dei rispondenti che hanno selezionato la specifica risposta cui fa poi riferimento la successiva sotto domanda.

La correlazione tra i dati forniti da domande diverse del questionario è effettuata tramite pivot del foglio elettronico contenente tutte i record delle risposte, e da questi fogli pivot vengono rielaborati i dati estratti e creati i relativi grafici.

A.1 La tassonomia degli attacchi digitali per OAD 2026

Le 15 tipologie di attacco considerate sono le seguenti, e fanno riferimento, a grandi linee, a che cosa si attacca:

1. Distruzione e/o compromissione FISICA di dispositivi ICT FISSI o di loro parti
2. Furto dispositivi FISSI ICT o di loro parti
3. Furto di dispositivi ICT MOBILI di proprietà dell'azienda/ente e in uso presso i suoi dipendenti/collaboratori
4. Furto INFORMAZIONI da singoli specifici sistemi FISSI ICT (PC, server, storage system, etc.) del Sistema Informativo, anche terziarizzati/in cloud
5. Furto INFORMAZIONI relative all'azienda/ente da sistemi MOBILI (palmari, smartphone, tablet, ecc.) sia di proprietà dell'azienda/ente sia dell'utente finale che li usa in logica BYOD
6. Attacchi ALL'IDENTIFICAZIONE, AUTENTICAZIONE E CONTROLLO ACCESSI degli utenti finali e privilegiati
7. Attacchi alle RETI locali e geografiche, fisse e wireless, inclusi i collegamenti ad Internet, e ai DNS
8. Attacco e/o uso non autorizzato di SISTEMI IT NEL LORO COMPLESSO (dal PC agli host fisici e virtuali). anche terziarizzati o in cloud
9. MODIFICHE malevoli e/o non autorizzate ai PROGRAMMI APPLICATIVI e alle loro configurazioni, del Sistema Informativo anche terziarizzate e in cloud
10. MODIFICHE malevoli e/o non autorizzate alle INFORMAZIONI trattate dalle applicazioni del Sistema Informativo, anche quelle terziarizzate/in cloud
11. SATURAZIONE (DoS, DDoS) risorse digitali del Sistema Informativo, anche quelle terziarizzate/in cloud
12. Attacchi ai propri sistemi/servizi digitali in CLOUD o comunque TERZIARIZZATI presso Fornitori terzi

13. Attacchi a dispositivi dei sistemi OT, OPERATIONAL TECHNOLOGY, ivi inclusi i sistemi IoT/IIoT, i sistemi per l'automazione industriale (SCADA, DCS, PLC, strumenti di diagnosi medica informatizzati, ecc.) e la robotica
14. Attacchi alla "SUPPLY CHAIN" causati da vulnerabilità di fornitori e/o clienti interconnessi
15. Attacchi a sistemi/servizi/applicativi basati su Intelligenza Artificiale.

Due ulteriori domande erano poste in aggiunta a queste 15:

- Nel corso dell'intero 2025/primo quadrimestre 2026 **non è stato rilevato alcun attacco digitale** intenzionale al Sistema Informativo
- Nel corso dell'intero 2025/primo quadrimestre 2026 il Sistema Informativo ha subito attacchi digitali la cui tipologia non è stata individuata

Quest'ultima domanda consente una risposta a chi ha rilevato attacchi al proprio SI ma non è in grado di associarli ad una o più delle 15 tipologie indicate.

La classificazione degli attacchi in OAD distingue il **che cosa** si attacca dal **come**. Spesso, anche nei più autorevoli rapporti internazionali, la distinzione tra che cosa viene attaccato e quali tecniche si usano per effettuare tale attacco non sempre è chiara, anche perché talvolta il nome usato per individuare l'attacco rappresenta anche la tecnica di attacco. Si è cercato di distinguere il più chiaramente possibile il target dell'attacco, ossia che cosa si attacca, dalle tecniche usate (sovente una loro combinazione), queste ultime raggruppate in 8 voci, descritte nel prossimo paragrafo.

A.1.1 Le classi di tecniche di attacco considerate (come si attacca)

Facendo riferimento principalmente alle tassonomie sviluppate da CERT[26] e da Sandia[27], si sono categorizzate le tecniche di attacco sotto riportate per poter descrivere e richiedere nel questionario OAD 2026 quali sono (o quali si pensa possano essere state) le tecniche usate dall'attaccante per portare l'attacco rilevato.

È opportuno sottolineare e ricordare che la fantasia degli attaccanti rende l'argomento piuttosto fluido e soggetto a rapida evoluzione e, a causa di ciò, variabile e dinamico anche nella nomenclatura. Il presente rapporto non può illustrare e spiegare l'ampio argomento interdisciplinare della sicurezza digitale, e per chi volesse approfondire tale argomento si rimanda alle numerose pubblicazioni disponibili.

L'elenco delle "famiglie" di tecniche di attacco considerate:

- Attacco fisico
- Raccolta malevola e non autorizzata di informazioni
- Script e programmi maligni
- Agenti autonomi
- Toolkit
- Botnet e simili
- Utilizzo di strumenti e tecniche di Intelligenza Artificiale
- Utilizzo di due o più tecniche di attacco.

Si noti come in questa edizione OAD ha inserito **l'IA come insieme specifico di tecniche di attacco.**

[26] Per CERT/CC si veda https://www.sei.cmu.edu/about/divisions/cert/index.cfm
[27] https://www.sandia.gov/

A.1.1.1 Attacco di tipo fisico

Nell'ambito degli attacchi intenzionali che OAD tratta, quelli di tipo fisico ai sistemi ICT richiedono la presenza fisica di uno o più attaccanti che:

- rompono e/o sconnettono i sistemi ICT ed i servizi a loro supporto (alimentazione elettrica, condizionamento aria, allarmi antintrusione, allarmi antincendio, etc.): l'attacco può essere distruttivo se uno o più dispositivi, o loro parti, vengono fracassate. Può essere non distruttivo se non viene rotto nulla ma vengono sconnessi e/o riconnessi in maniera sbagliata i vari dispositivi: ad esempio sconnessione e/o scambio delle porte degli switch di rete, sconnessioni o taglio dei cavi di connessione, etc.
- rubano dispostivi ICT o loro parti, dagli smartphone ai laptop, dagli hard disk alle chiavette USB, sia per il loro valore sul mercato sia per i dati contenuti.
- tramite chiavette USB, scaricano i file del sistema ICT attaccato connettendole manualmente alle porte USB non disabilitate/protette presenti nel sistema ICT.

L'attacco fisico è considerato sia come tipologia d'attacco, in quanto viene attaccato l'hardware dei dispostivi ICT o di loro parti (il che cosa viene attaccato), sia come tecnica d'attacco, perché scassare o rubare i dispositivi ICT è una tecnica per manomettere, anche gravemente, il funzionamento dell'intero sistema informativo o di sue parti, oltre che sottrarre e/o distruggere le informazioni contenute in tali dispositivi sia asportando gli hard disk sia copiando file con chiavette USB.

A.1.1.2 Raccolta/diffusione malevola e non autorizzata di informazioni

Per attaccare un sistema ICT sono utili, in taluni casi indispensabili, informazioni sia dirette sulla sua posizione, sul suo funzionamento, sulla sua configurazione, sulle misure di sicurezza di cui dispone, sugli account degli utenti, sia indirette, come i nomi dei suoi utenti e dei suoi gestori, indirizzi fisici e digitali, numeri di telefono, contatti anche via rete con dipendenti potenzialmente infedeli o ingenui etc. Innumerevoli le tecniche per carpire, direttamente o indirettamente, le informazioni che servono per attuare un attacco digitale. Alcune sono "fisiche", come la personale interazione con le persone che usano o gestiscono un dispositivo o le applicazioni del SI, come l'acquisizione di informazioni da carte e stampe nei cestini dei rifiuti, come la richiesta di informazioni in maniera subdola sia "de visu" sia per telefono (anche questo è social engineering). Altre tecniche per raccogliere informazioni sono informatiche ed includono, ad esempio, phishing, pharming, hoax, scam, data entry in server trappola, scannerizzazioni e ricerche in Internet, etc.

Si sta inoltre assistendo in maniera crescente alla diffusione, soprattutto via Internet, di informazioni false (le così dette fake news) e/o malevoli atte a far compiere all'inconsapevole destinatario operazioni di ausilio all'attuazione dell'attacco. I canali

A.1.1.3 Script e programmi maligni

Gli **script** sono semplici programmi software scritti in un linguaggio interpretato facile da utilizzare, senza interfaccia grafica, che svolgono funzioni molto specifiche ed accessorie, ed in grado di interfacciarsi con altri programmi più complessi per svolgere operazioni più sofisticate. Gli script sono sovente usati per personalizzare la configurazione automatica di un sistema ICT, per rendere più dinamica una pagina web, per fornire comandi ad un sistema operativo (tipico dei così detti "script shell") e a data base, per personalizzare e rendere "smart" documenti Microsoft Office, Libre Office, o analoghi. Esempi di linguaggi di scripting includono Bash, AppleScript, JavaScript, Perl, Python, PHP, VBScript.

Programmi in script sono usati per attacchi digitali, e quelli più semplici richiedono un intervento umano per farli giungere sul sistema bersaglio (ad esempio l'apertura di un allegato in posta elettronica o lo sfruttamento di un buffer overflow presente in una applicazione); quelli più sofisticati sono in grado di attaccare senza bisogno di interventi di persone. Gli script maligni possono essere utilizzati per realizzare diverse tipologie di attacco, tra cui il Cross-Site Scripting (XSS) [28],, gli attacchi drive-by[29], e quelli basati sull'esecuzione di codice fileless[30]

Con linguaggi più sofisticati, come C, C++, C#, Java, si possono realizzare programmi d'attacco più complessi e più dannosi, chiamati genericamente **malware** o **codici maligni**. Essi sono caratterizzati da un qualche meccanismo con il quale riescono a raggiungere il bersaglio, e sono classificati con specifici nomi, e da un "payload", una parte che esegue l'azione di attacco.

La classificazione per funzioni e capacità dei malware include Trojan Horse, ransomware, spyware, adware (si rimanda al Glossario in Allegato B per una sintetica spiegazione di questi termini). Occorre sottolineare che la sofisticazione oggi raggiunta da molti codici maligni rende difficile una esatta classificazione, dato che essi sono in grado di svolgere diverse funzioni anche alternative tra loro, il così detto polimorfismo.

Nella categoria "script e programmi maligni" è stata inclusa anche quella dei così detti "command", ossia di comandi al sistema operativo o al DBMS che quando vengono eseguiti possono avere gravi conseguenze per il sistema attaccato. Si tratta di comandi malformati che controlli inadeguati consentono di mandare in esecuzione, comandi che altrimenti non sarebbero stati autorizzati. Il comando può modificare i diritti di accesso al sistema, consentire di interrogare, modificare, distruggere informazioni. Come caso tipico di esempio, l'attaccante ha attivato una sessione Telnet con il bersaglio o, nel caso di "SQL injection", scritto alcuni caratteri in un form web. Un esempio di comando ad un data base è il XSS.

A.1.1.4 Agenti autonomi

Sono programmi maligni capaci di replicarsi e diffondersi in rete su altri sistemi autonomamente, come i **virus** ed i **worm**. Per la loro basilare caratteristica di potersi diffondere sui sistemi in rete in maniera autonoma, vengono considerati una categoria, o sottocategoria, a parte rispetto ai malware.

A.1.1.5 Toolkit

Come dice il nome, sono una "cassetta degli attrezzi" di strumenti informatici che aiutano a compiere l'attacco: trovano le informazioni necessarie e le vulnerabilità presenti nel sistema target, e tali informazioni possono essere usate per sviluppare codici maligni. Molti di questi strumenti sono normalmente usati per il monitoraggio ed il controllo delle misure di sicurezza, e per l'hacking etico, ad esempio analisi di vulnerabilità e penetration test. In linea generale i toolkit possono essere classificati per le loro funzionalità, e quindi per il loro utilizzo, che dipende in base alla fase dell'attacco o del test.

Alcuni toolkit sono specifici per determinati linguaggi ed ambienti, altri più generali. Sono da evidenziare due categorie di toolkit: i rootkit ed i meta exploit tool. I primi derivano il nome dal termine "root", radice, che nei sistemi Unix è il livello a cui si ottengono i massimi livelli amministrativi: i rootkit sono quindi strumenti per acquisire i diritti di "root", i più alti per un utente privilegiato. Con il tempo e negli ambienti Microsoft Windows è prevalso un altro significato: uno strumento che nasconde la presenza di malware. Tipicamente il rootkit guadagna i diritti di amministratore usando vulnerabilità note o carpendo informazioni via social engineering, e poi modifica il sistema operativo in modo da nascondere la sua presenza e quella di altro

[28] XSS, Cross-site scripting: vengono iniettati script dannosi in siti web attendibili, che possono modificare le pagine web e che vengono poi eseguiti nel browser della vittima.
[29] Sfruttano vulnerabilità del browser per scaricare ed eseguire codice maligno non appena l'utente visita un sito web infetto.
[30] Eseguono codice dannoso direttamente nella memoria RAM senza scriverlo su disco, rendendo più difficile il rilevamento da parte degli antivirus tradizionali.

malware che ad esempio può installare backdoor, keylogger o strumenti che bloccano o eludono i meccanismi di controllo delle licenze, di protezione delle copie e più in generale i meccanismi di sicurezza digitale.

Gli exploit sono attacchi ad una risorsa ICT basandosi sulle sue vulnerabilità ed il termine "meta exploit" indica strumenti software che facilitano l'individuazione di vulnerabilità e la verifica di come sfruttarle per attuare attacchi, anche con l'aiuto di basi di conoscenza contenenti centinaia di exploit.

A.1.1.6 Botnet e simili

Strumenti distribuiti controllati centralmente da un Command & Control, spesso indicato con C&C o 2C, il più delle volte anonimo e che continua a spostarsi da un server all'altro (a livello mondiale, e in tempi brevi) per non farsi identificare. Gli agenti distribuiti sono codici maligni, talvolta virus, e sono chiamati bot, droni, zombi. Dopo essere stati installati all'insaputa dell'utente e/o del gestore del sistema involontariamente ospite, restano dormienti fino a quando il C&C ordina loro di attivarsi. Gli attacchi DDoS si basano su botnet con innumerevoli sistemi che contengono gli agenti, che al comando del C&C inondano di traffico il sistema ICT bersaglio, saturando le sue connessioni ad Internet.

A.1.1.7 Utilizzo di strumenti e tecniche di Intelligenza Artificiale

L'Intelligenza Artificiale (IA) viene utilizzata per gli attacchi informatici principalmente per automatizzare e potenziare attività come il phishing e il social engineering tramite la creazione di contenuti fraudolenti più convincenti e personalizzati. Gli attaccanti usano l'IA per analizzare grandi quantità di dati al fine di identificare e sfruttare vulnerabilità, per creare malware più efficaci e per automatizzare le operazioni di attacco, rendendo più difficile il rilevamento. L'IA viene anche usata per generare deepfake e manipolare dati, creando disinformazione e minacce più sofisticate.

A.1.1.8 Utilizzo di due o più tecniche di attacco

I moderni e più temibili attacchi digitali utilizzano più di una tecnica di attacco, anche contemporaneamente: ad esempio sono in grado di analizzare le vulnerabilità di un sistema ICT, e di attaccarlo con la tecnica più idonea, e in parallelo attivare virus, inondare di agent gli altri sistemi, e mantenere il controllo di tutto questo trame un C&C di cui al precedente paragrafo. Questa categoria include tipicamente gli attacchi APT, Advanced Persistent Threat: sono attacchi persistenti, che possono durare nel tempo, soprattutto nella fase preparatoria e di individuazione delle vulnerabilità da sfruttare (persistent), e che utilizzano innovazioni tecnologiche (advanced).

Attacchi APT sono realizzati ed usati prevalentemente da organizzazioni con grandi capacità e risorse, in taluni casi anche da stati.

A.2 La macro-valutazione qualitativa del livello di sicurezza digitale del sistema informatico oggetto delle risposte al questionario

Con l'obiettivo di meglio e più fortemente motivare un potenziale rispondente a compilare il questionario online di OAD 2026, è stata fornita, in tempo reale a chi completa la compilazione, una macro-valutazione qualitativa del livello di sicurezza digitale del sistema informativo oggetto delle sue risposte, rispetto alle esigenze di sicurezza dell'azienda/ente per la quale si risponde.

La macro-valutazione è stata realizzata assegnando degli opportuni "pesi" numerici a tutte le opzioni di risposta previste nel questionario, rispetto alle domande relative:

- alle generali caratteristiche del sistema informativo (**A**);
- all'importanza e alla necessità del sistema informativo e della sua sicurezza, per le attività ed il business dell'azienda/ente rispondente (**B**);
- alle misure di sicurezza digitale, tecniche ed organizzative, in essere nel sistema informativo e selezionate scegliendo le varie opzioni di risposta predefinite presenti per ogni misura (**S**).

Nel procedere nella compilazione del questionario, il sistema LImeSurvey, opportunamente configurato e predisposto, somma i pesi delle risposte relative alle domande inerenti A, B ed S.

Calcola poi un Indice di Sicurezza Digitale numerico (IDS) dato dalla formula seguente:

$$\text{Indice Sicurezza Digitale} = \sum Si \,/\, (\sum Ai + \sum Bi)$$

Il numero IDS calcolato viene posizionato in una scala di valori numerici che caratterizzano le seguenti valutazioni qualitative del livello di sicurezza digitale: **elevato (IDS>0,80), idoneo (IDS > 0,5 e IDS <= 0,80)**, **insufficiente (IDS > 0,25 e IDS <= 0,5)**, **molto critico (IDS <= 0,25)**.

Queste valutazioni appaiono online alla fine del completamento del questionario, inclusa la parte opzionale sulle misure di sicurezza digitale, cui segue, anche stampabile, l'elenco delle risposte fornite che evidenziano la mancanza o l'insufficienza di misure di sicurezza digitale e che hanno portato alla specifica valutazione del livello di sicurezza.

La macro-valutazione ha natura indicativa e non costituisce un audit, una certificazione o una valutazione completa del livello di sicurezza digitale dell'organizzazione.

ALLEGATO B - Mini Glossario essenziale

Il presente glossario, volutamente sintetico, raccoglie i principali termini e acronimi ICT e di cybersecurity utili alla lettura del Rapporto OAD 2026. Non intende pertanto costituire un repertorio esaustivo. Per una copertura più ampia e aggiornata si rinvia anche al Glossario dell'ACN-CSIRT: https://www.acn.gov.it/portale/csirt-italia/glossario.

Account	Insieme delle informazioni usate per identificare e autenticare un utente di un sistema informativo.
ACN	Agenzia per la Cybersicurezza Nazionale.
Adware	Codice che si installa automaticamente nel computer, come un virus o lo spyware, ma in genere si limita a visualizzare una serie di pubblicità mentre si è connessi a Internet. L'adware può rallentare sensibilmente il computer e nonostante costringa l'utente a chiudere tutte le finestre pop-up visualizzate, non rappresenta una vera minaccia per i dati, a meno che non nasconda un codice maligno.
AI / IA	Artificial Intelligence / Intelligenza Artificiale: insieme di tecniche e sistemi capaci di svolgere compiti tipicamente associati all'intelligenza umana.
APT	Advanced Persistent Threat: attore o campagna di attacco sofisticata, mirata e persistente nel tempo, generalmente caratterizzata da più tecniche e fasi operative.
Attacco massivo	Attacco rivolto a una grande quantità di obiettivi simili; phishing e ransomware ne sono esempi tipici.
Attacco mirato	Attacco rivolto a uno specifico obiettivo o gruppo di obiettivi, con tecniche adattate al bersaglio.
Backdoor	Meccanismo nascosto che consente di accedere a un programma o sistema aggirando le normali procedure di accesso.
Backup	Copia di dati, configurazioni o altri elementi necessari al recupero delle informazioni e, quando previsto, al ripristino dei sistemi.
BC / Business Continuity	Business Continuity: capacità di un'organizzazione di continuare a erogare prodotti e servizi essenziali durante e dopo un'interruzione.
Botnet	Insieme di sistemi compromessi e controllati da remoto, spesso utilizzati per attacchi distribuiti come i DDoS.
BYOD	Bring Your Own Device: utilizzo per attività lavorative di dispositivi personali degli utenti.
C&C	Command & Control: infrastruttura usata per comandare e coordinare sistemi compromessi, ad esempio una botnet.
CAaaS	Cyber Attack as a Service: fornitura di capacità o strumenti di attacco come servizio.
CER	Critical Entities Resilience: Direttiva UE 2022/2557, recepita in Italia dal D.Lgs. 134/2024, sulla resilienza dei soggetti critici.
CERT	Computer Emergency Response Team.
CIO	Chief Information Officer: figura responsabile della direzione e della gestione strategica dei sistemi informativi di un'organizzazione.
CISO	Chief Information Security Officer: responsabile della sicurezza digitale dell'organizzazione.

ClickFix	Tecnica di ingegneria sociale che induce l'utente a eseguire comandi malevoli, presentandoli come la soluzione a un problema tecnico o una verifica.
Cloud computing	Erogazione tramite rete di risorse e servizi informatici, quali capacità di calcolo, archiviazione e applicazioni, gestiti in proprio o da fornitori esterni.
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, nell'ambito della Polizia Postale e per la Sicurezza Cibernetica.
CSIRT	Computer Security Incident Response Team; in Italia opera nell'ambito dell'ACN.
CVE	Common Vulnerabilities and Exposures: sistema di identificazione e catalogazione pubblica delle vulnerabilità note.
CVSS	Common Vulnerability Scoring System: metrica per valutare la gravità di una vulnerabilità.
Cyber resilience / Resilienza digitale	Capacità di prepararsi, resistere, rispondere e ripristinare le attività essenziali a seguito di incidenti o interruzioni digitali.
Cyber warfare	Impiego di operazioni nello spazio cibernetico nell'ambito di conflitti o attività ostili tra Stati e altri attori.
Dark web	Parte del web accessibile tramite specifici software o configurazioni e non indicizzata dai normali motori di ricerca.
Data breach	Violazione della sicurezza dei dati che comporta distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati; nel contesto GDPR il termine si riferisce alla violazione di dati personali.
DCS	Distributed Control System: sistema di controllo distribuito impiegato in ambito industriale e OT.
DDoS / DoS	Distributed Denial of Service / Denial of Service: attacco che mira a rendere indisponibili sistemi o servizi sovraccaricandoli o esaurendone le risorse.
Deepfake	Contenuto audio, video o immagine sintetico o manipolato, spesso tramite IA, che può simulare realisticamente persone o eventi.
DLP	Data Loss Prevention: tecniche e sistemi per prevenire perdita, sottrazione o diffusione non autorizzata di dati.
DMARC	Domain-based Message Authentication, Reporting and Conformance: standard per contrastare lo spoofing e migliorare l'autenticazione delle e-mail.
DORA	Digital Operational Resilience Act: Regolamento UE 2022/2554 sulla resilienza operativa digitale del settore finanziario.
DR / Disaster Recovery	Disaster Recovery: insieme di processi, risorse e procedure per ripristinare sistemi e servizi ICT dopo un incidente grave o un'interruzione.
EDR	Endpoint Detection and Response: soluzione per rilevare, analizzare e contrastare attività malevole sugli endpoint.
Endpoint	Dispositivo terminale collegato a una rete o a un sistema informativo, come ad esempio PC, server, smartphone o tablet.
ENISA	European Union Agency for Cybersecurity.
Escalation	Procedura per coinvolgere livelli successivi di responsabilità o competenza nella gestione di incidenti, emergenze o problemi non risolti.

Evento cyber / Incidente cyber	Evento cyber: circostanza rilevante per la sicurezza che viene osservata o segnalata; incidente cyber: evento con conseguenze effettive sulla sicurezza o sul funzionamento dei sistemi, secondo i criteri della fonte che lo classifica.
Exploit	Codice o tecnica che sfrutta una vulnerabilità di una risorsa ICT.
Fix	Traducibile in "riparazione", è la specifica soluzione tecnica a un singolo difetto del codice software, che può anche essere inserita in una patch.
FW	Firewall: sistema che controlla e filtra il traffico di rete in base a regole definite.
GDPR	General Data Protection Regulation: Regolamento UE 2016/679 sulla protezione dei dati personali.
GenAI	Intelligenza artificiale generativa: sistemi di AI capaci di creare nuovi contenuti, come testi, immagini, audio o video.
Hacktivism	Uso di tecniche informatiche offensive con finalità politiche, ideologiche o sociali.
Hoax	In italiano "bufala" o burla, indica la segnalazione di falsi virus; rientra tra le tecniche di social engineering.
IAM	Identity & Access Management: processi e tecnologie per gestire identità digitali e diritti di accesso.
ICS	Industrial Control System: sistema di controllo industriale, tipico degli ambienti OT.
ICT	Information and Communication Technology: tecnologie dell'informazione e della comunicazione.
IDS	Intrusion Detection System: sistema per individuare tentativi di intrusione o attività anomale. Nel Rapporto, l'acronimo IDS è usato anche per l'Indice di Sicurezza Digitale, quando espressamente indicato.
IIoT	Industrial Internet of Things: dispositivi e sistemi IoT utilizzati in ambito industriale.
Incident response	Processi e attività per identificare, analizzare, contenere e gestire un incidente di sicurezza digitale.
Info stealer	Malware progettato per sottrarre informazioni, ad esempio credenziali e dati dell'utente.
IoT	Internet of Things: insieme di dispositivi connessi in rete in grado di raccogliere, scambiare o elaborare dati.
IPS	Intrusion Prevention System: sistema che rileva e blocca tentativi di intrusione o traffico malevolo.
KEV	Known Exploited Vulnerabilities: catalogo delle vulnerabilità note e sfruttate attivamente, gestito dalla CISA statunitense.
LLM	Large Language Model: modello di Intelligenza Artificiale addestrato su grandi quantità di dati testuali per elaborare e generare linguaggio.
Log	Registrazione cronologica di attività, eventi e operazioni effettuate da utenti, applicazioni, dispositivi o sistemi.
MaaS	Malware as a Service: disponibilità di malware e relativi servizi secondo modelli "as a service".
Malicious insider	Soggetto interno all'organizzazione che usa legittimi privilegi o accessi per compiere azioni dannose.

Malware	Termine generale per indicare software progettato con finalità malevole.
MFA	Multi-Factor Authentication: autenticazione che richiede due o più fattori distinti.
MSS / MSSP	Managed Security Service / Managed Security Service Provider: servizio gestito di sicurezza e relativo fornitore.
N-day	Vulnerabilità già nota pubblicamente, anche quando non è stata ancora corretta in tutti i sistemi interessati.
NIS2	Direttiva UE 2022/2555 sulla sicurezza delle reti e dei sistemi informativi, recepita in Italia dal D.Lgs. 138/2024.
NIST	National Institute of Standards and Technology, organismo statunitense che pubblica standard e linee guida anche in materia di cybersecurity.
NVD	National Vulnerability Database: banca dati statunitense sulle vulnerabilità, gestita dal NIST.
OT	Operational Technology: tecnologie hardware e software usate per controllare e monitorare processi e sistemi fisici.
PAM	Privileged Access Management: strumenti e processi per governare gli accessi privilegiati.
Patch / Patching	Patch: aggiornamento software destinato a correggere difetti o vulnerabilità; patching: attività di pianificazione, applicazione e verifica di tali aggiornamenti.
PhaaS	Phishing-as-a-Service: modello di fornitura di kit, infrastrutture e servizi che facilitano la realizzazione di campagne di phishing.
Pharming	Attacco digitale per carpire informazioni riservate di un utente basato sulla manipolazione dei server DNS o dei registri del sistema operativo del PC dell'utente.
Phishing	Attacco di social engineering, tipicamente via e-mail, finalizzato a sottrarre credenziali o altre informazioni riservate.
PLC	Programmable Logic Controller: controllore logico programmabile usato per l'automazione di macchine e processi industriali.
Ransomware	Malware che cifra o blocca dati e sistemi, spesso accompagnando l'attacco con richieste di riscatto e minacce di divulgazione dei dati sottratti.
RDoS	Ransom Denial of Service: ricatto basato sulla minaccia di un attacco DoS/DDoS.
Rootkit	Insieme di strumenti o componenti software utilizzati per nascondere attività malevole e mantenere accessi privilegiati su un sistema compromesso.
RPO	Recovery Point Objective: quantità massima di dati, misurata in tempo, di cui si accetta potenzialmente la perdita dopo un'interruzione.
RTO	Recovery Time Objective: tempo obiettivo entro cui ripristinare un servizio o un sistema dopo un'interruzione.
SCADA	Supervisory Control And Data Acquisition: sistemi per il controllo e il monitoraggio di processi in ambito OT.
SCAM	Tentativo di truffa via posta elettronica. A fronte di un millantato forte guadagno o forte vincita ad una lotteria, si chiede di versare un anticipo o pagare una tassa.
SI	Sistema Informativo: insieme di persone, processi, informazioni, applicazioni e risorse ICT che supportano le attività di un'organizzazione.

SIEM	Security Information and Event Management: sistemi che raccolgono e correlano eventi e log di sicurezza.
SLA	Service Level Agreement: accordo contrattuale che definisce i livelli di servizio attesi, inclusi quando previsti tempi di risposta e di ripristino.
Smishing	Phishing effettuato tramite SMS o altri messaggi di testo.
SOAR	Security Orchestration, Automation and Response: tecnologie per automatizzare e integrare attività e processi di sicurezza.
SOC	Security Operation Centre: struttura dedicata al monitoraggio e alla gestione operativa della sicurezza.
Social Engineering	Tecniche che sfruttano il comportamento umano per ottenere informazioni, credenziali o accessi non autorizzati.
Spear phishing	Letteralmente significa "pesca con la fiocina". E' un attacco di phishing sofisticato e orientato ad una singola persona o gruppo di persone.
Spyware	Codice maligno che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete, etc.) senza il suo consenso, utilizzandole poi per trarne profitto, solitamente attraverso l'invio di pubblicità mirata.
Spoofing	Falsificazione dell'identità o dell'origine di una comunicazione, ad esempio dell'indirizzo mittente di un'e-mail.
SQL injection	Tecnica di attacco che sfrutta vulnerabilità applicative per inserire comandi SQL malevoli verso un database.
Supply chain digitale	Catena di fornitura di prodotti, componenti e servizi ICT; le dipendenze tra fornitori e clienti possono propagare effetti di un incidente.
Targeted Attack	Attacco mirato verso uno specifico soggetto o sistema, spesso condotto con tecniche multiple e persistenti.
Trojan Horse	Codice malevolo che si presenta come legittimo o è nascosto in un software, eseguendo azioni non note o non desiderate dall'utente.
UEBA	User and Entity Behavioral Analytics: analisi del comportamento di utenti ed entità per individuare anomalie e possibili minacce.
Virus	Tipologia di malware capace, una volta attivato, di danneggiare documenti e file eseguibili. Il virus è caratterizzato dalla presenza di istruzioni che ne consentono la replicazione e la conseguente diffusione, che avviene durante il trasferimento del file infetto da un computer a un altro. Si differenzia dal worm, che è in grado di propagarsi autonomamente mediante diffusione dentro reti di computer o tramite e-mail.
Vishing	Attacco di social engineering tramite chiamate telefoniche o comunicazioni vocali.
VPN	Virtual Private Network: rete virtuale protetta che consente comunicazioni sicure attraverso una rete pubblica.
Vulnerability assessment	Attività di individuazione, analisi e valutazione delle vulnerabilità di sistemi, applicazioni o infrastrutture.
WAF	Web Application Firewall: firewall applicativo che analizza e filtra il traffico HTTP/HTTPS diretto alle applicazioni web.

Watering Hole	Attacco mirato che compromette siti web abitualmente visitati dal bersaglio per colpirlo indirettamente.
Wiper	Malware distruttivo progettato per cancellare o rendere inutilizzabili dati e sistemi.
Worm	Malware capace di propagarsi automaticamente tra sistemi, spesso sfruttando reti e vulnerabilità.
XSS	Cross-Site Scripting: tecnica di attacco che permette l'iniezione e l'esecuzione di script non autorizzati nel browser di altri utenti tramite applicazioni web vulnerabili.
Zero Trust	Modello di sicurezza che non attribuisce fiducia implicita a utenti, dispositivi o sistemi e richiede verifiche continue.
Zero-day	Vulnerabilità sconosciuta al produttore o priva di correzione disponibile al momento del suo sfruttamento; il termine può riferirsi anche all'attacco che la sfrutta.

ALLEGATO C - Principali fonti e riferimenti

C.1 Dall'OCI all'OAI e a OAD: un po' di storia della sicurezza digitale in Italia

- FTI, Forum per la Tecnologia dell'Informazione: "Osservatorio sulla criminalità informatica – Rapporto 1997" in collaborazione SPACE dell'Università Bocconi, Franco Angeli.
- M. R. A. Bozzetti, P. Pozzi (a cura di): "Cyberwar o sicurezza? Secondo Osservatorio Criminalità ICT", 2000, Franco Angeli.
- M. R. A. Bozzetti, R. Massotti, P. Pozzi (a cura di): "Crimine virtuale, minaccia reale", 2004, Franco Angeli
- M. R. A. Bozzetti, F. Zambon: "Sicurezza Digitale – una guida per governare un sistema informatico sicuro", giugno 2013, Soiel International, ISBN 9788890890109
- I vari Rapporti annuali OAI e OAD: https://www.oadweb.it/it/main-it/rapporti-e-relativi-convegni.html
- Marco R. A. Bozzetti: "Attacchi digitali e misure di sicurezza: l'indagine OAD di AIPSI", SecSolution Magazine n.34, p. 75-78, Agosto 2024: https://www.secsolution.com/notizia.asp?id=18956&c=0
- Marco R. A. Bozzetti: "Come evolvono gli attacchi cyber in Italia: le indagini OAD di AIPSI", Agenda Digitale 360, 1° agosto 2024: https://www.agendadigitale.eu/sicurezza/evoluzione-degli-attacchi-digitali-in-italia-lanalisi-delle-indagini-oad-di-aipsi/
- Yvette Agostini, Marco R. A. Bozzetti: "Il fattore umano nella sicurezza digitale", pubblicato su Linea EDP, 31 luglio 2025: https://www.lineaedp.it/featured/il-fattore-umano-nella-sicurezza-digitale/
- Marco R. A. Bozzetti: Rubrica settimanale "OAD Insight", pubblicata da luglio 2026: https://www.oadweb.it/it/comunita-oad/oad-insight.html

C.2 Le principali fonti sugli attacchi, i rischi ICT e le vulnerabilità ICT

L' elenco, in ordine alfabetico, non ha alcuna pretesa di essere esaustivo e completo: le fonti citate sono quelle indipendenti da fornitori e considerate più autorevoli a livello mondiale, europeo e nazionale.

- ACN, Agenzia Cybersicurezza Nazionale: https://www.acn.gov.it/
- AGID, Agenzia per l'Italia Digitale: https://www.agid.gov.it/
- CISA, Cybersecurity Infrastructure Security Agency, è l'Agenzia statunitense per la sicurezza informatica e delle infrastrutture (analoga all'ACN italiana): https://www.cisa.gov/
- CSIRT, Computer Security Incident Response Team – Italia: https://csirt.gov.it/
- CVE, Common Vulnerabilities and Exposures, è un elenco aggiornato di tutte le vulnerabilità note pubblicamente, identificate da un numero univoco: https://www.cve.org/
- Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri: https://innovazione.gov.it/
- ENISA, European Union Agency for Network and Information Security: http://www.enisa.europa.eu/
- First, Forum for Incident Response and Security Team, fornisce aggiornate informazioni su attacchi e vulnerabilità, classificandole in base al CVSS, Common Vulnerability Scoring System: http://www.first.org/
- Internet Crime Complaint Center (IC3) è una partnership tra FBI (Federal Bureau of Investigation), il National White Collar Crime Center (NW3C) e il Bureau of Justice Assistance (BJA), e fornisce, oltre alla possibilità di denunciare negli US attacchi digitali, informazioni sugli attacchi stessi e sui trend in atto per i crimini digitali: https://www.ic3.gov/
- MITRE ATT&CK è una base di conoscenza aggiornata che cataloga i comportamenti, le tattiche, le tecniche e le procedure (TTP) utilizzate dai criminali informatici negli attacchi digitali. Viene usata per analisi dei rischi ICT proattive, per analisi di possibili attacchi o di quelli già occorsi, per simulare attacchi e individuare i migliori strumenti di difesa.
- NVD, National Vulnerability Database, è l'archivio statunitense di informazioni sulla vulnerabilità standardizzate e gestibili in maniera automatizzata con il protocollo SPAC: https://nvd.nist.gov/
- OECD, Organisation for Economic Co-operation and Development, produce rapporti sui rischi e gli attacchi digitali che impattano sull'economia delle nazioni in Europa: http://www.oecd.org/sti/ieconomy/security.htm
- OWASP, Open Web Application Security Project, progetto open source per la sicurezza delle applicazioni web, fornisce vari rapporti e linee guida sul tema, tra cui, periodicamente, le "top ten", le vulnerabilità ed i rischi più critici per le applicazioni web: https://www.owasp.org/
- Sistema di informazione per la sicurezza della Repubblica Italiana, insieme di organi e autorità che hanno il compito di assicurare le attività di informazione per la sicurezza, allo scopo di salvaguardare la Repubblica da ogni pericolo e minaccia proveniente sia dall'interno sia dall'esterno del Paese, inclusa la sicurezza digitale: http://www.sicurezzanazionale.gov.it/
- World Economic Forum, realizza un annuale rapporto sui rischi globali, che includono anche i rischi ICT e le cyberwar: https://www.weforum.org/

ALLEGATO D - Il profilo dell'autore Marco R. A. Bozzetti

Marco Rodolfo Alessandro Bozzetti



Ingegnere Elettronico laureato al Politecnico di Milano, ha maturato una lunga ed ampia esperienza nell'ICT e nella consulenza direzionale.

È stato fondatore e CEO di **Malabo S.r.l.**, dal 2001 al 2026, specializzata in progetti di innovazione, sicurezza digitale e strategie ICT per aziende ed enti pubblici.

Questa attività professionale è ora nell'ambito del suo **Studio MRAB**, di cui è titolare, e che per ora fa ancora riferimento al sito web https://www.malaboadvisoring.it/.

Precedenti esperienze professionali

- **ENI (1995–2000)** – Primo **CIO,** Chief Information Officer dell'intero Gruppo. Ha guidato una delle più grandi razionalizzazioni e terziarizzazioni dei sistemi informativi ENI avvenute in Europa.
- **Arthur Andersen MC e GEA/GEALAB** – Consulente senior per progetti complessi in ambito ICT.
- **Olivetti e Italtel** – Ruoli con responsabilità crescenti in ambito tecnico e manageriale.
- **Fondatore o partner** di varie aziende del settore ICT: Abiemme, CA.SI, ClickICT, Ibimaint System Engineering, System Engineering.

Iniziative e Progetti di Rilievo

- Ideatore e coordinatore scientifico di **EITO** (European Information Technology Observatory) per SMAU e le principali fiere ICT europee (anni '90 - 2003).
- Ideatore e realizzatore di **OAD**, Osservatorio Attacchi Digitali in Italia, attivo dal 2009 (oadweb.it).

Competenze Chiave

- **Governance ICT**: ITIL, COBIT, ISO, NIST
- **Sicurezza digitale**: Risk assessment, BIA, Business Continuity, Disaster Recovery
- **Strategia ICT & Innovazione**: digital transformation
- **Valutazione e sviluppo competenze ICT**
- **Compliance** normative europee ed italiane (GDPR, NIS2, CER, DORA, etc.)

Formazione & Docenze

- Formatore senior in ambito tecnico e manageriale (in aula e online) per aziende, enti formativi e master universitari.
- Argomenti trattati: protocolli OSI/TCP-IP, architetture ICT, SOA, microservizi cloud, sicurezza digitale, governance e management ICT, compliance ICT, ruoli-competenze-certificazioni ICT, NIS2.
- Tutti i corsi includono casi reali tratti dall'esperienza diretta di M. R. A. Bozzetti.

Incarichi Associativi e Istituzionali

- **Presidente Onorario** (Past President) di **AIPSI**
- **Tesoriere** (Past President e Past Vicepresidente) di **FIDAInform**
- **Revisore dei conti** e socio (Past President e Past Vicepresidente) del **ClubTI Milano**
- **Coordinatore** del gruppo di lavoro **GL09 CT 526 UNINFO** su "Profili di ruolo professionale manageriali operanti nell'ICT"
- **Commissario d'Esame AICA** per certificazioni **eCFPlus (EN 16234 – UNI 11506)**

Certificazioni

- **ITIL v3**
- **EUCIP Professional Certificate – Security Specialist**

Pubblicazioni

- Oltre **260 pubblicazioni**, tra cui **50 libri e rapporti internazionali**.

ALLEGATO E - Collaborazioni istituzionali

E.1 AICA

https://www.aicanet.it/



Associazione Italiana per l'Informatica e il Calcolo Automatico, è l'associazione italiana senza scopo di lucro di cultori e professionisti ICT per lo sviluppo e la diffusione delle conoscenze e della cultura digitale. Numerose le sue iniziative, tra le principali ha realizzato a livello europeo l'ECDL (ora ICDL) e l'eCF (UNI EN 16234-1:2016): per quest'ultimo è accreditata Accredia come ente certificatore. Quest'ultima attività, orientata ai professionisti ICT, ha portato AICA a sviluppare un insieme di iniziative per questo specifico settore, basato prevalentemente su corsi di formazione e relative certificazioni, in parte "proprietarie di AICA", in parte accreditate Accredia. Attualmente le iniziative in questo settore includono:

- **e-CFplus:** il servizio AICA rivolto ai professionisti ICT, che include servizi di *Autovalutazione* e di *Certificazione* (accreditata Accredia) che fanno riferimento all'e-Competence Framework versione 4.0 recepito nella norma UNI EN 16234-1:2020, con riferimento ai profili di ruolo professionali descritti nella UNI 11621-2:2021 (e sue successive parti) ed ai criteri di valutazione descritti nella norma UNI 11506:2021.
- EUCIP **IT Specialist**: certificazione (accreditata Accredia) orientata agli Amministratori di Sistema, garantisce una solida base di conoscenze ed abilità pratiche per la gestione dell'infrastruttura IT di piccole organizzazioni, imprese o uffici decentrati di un grande ente.
- EUCIP **IT Administrator**: certificazione (accreditata Accredia) orientata ai responsabili dell'infrastruttura ICT di piccole-medie aziende o degli uffici decentrati di una grande organizzazione.
- **EPM,** European Project Management: certificazione AICA per i Project Manager di qualsiasi settore, basata su EPM, che fa riferimento allo standard UNI 11648:2016.
- **Protezione Dati Personali** -GDPR, Privacy e Sicurezza: certificazione AICA per la verifica delle competenze in ambito di privacy e di protezione dei dati tramite l'applicazione del GDPR, normativa fondamentale per garantire la corretta gestione dei dati personali e la conformità alle norme.
- **Informatica Giuridica**: certificazione AICA per la verifica delle competenze e delle abilità acquisite riguardanti l'informatica giuridica e tutte le implicazioni legali e formali inerenti all'utilizzo della tecnologia ICT.
- **EQDL**-concetti e conoscenze di base sulla qualità: certificazione AICA, attuata in accordo con AICQ, delle conoscenze di base sulla Qualità, aggiornata all'ultima versione della norma UNI EN ISO 9001.
- **e4job**: certificazione AICA (accreditata Accredia) delle competenze di base informatiche per i vari ruoli professionali non ICT, coerente con e-CF e nel rispetto della norma ISO 17024:2012 e della legge italiana 4/2013.
- **NIS2 Cert**: percorso formativo AICA con relativa certificazione per l'addetto e il responsabile NIS2.
- **Quantum Cert**: percorso formativo AICA con relativa certificazione per comprendere i principi della computazione quantistica, conoscere le tecnologie attuali, fornendo una base solida per chi desidera inserirsi nel mondo del quantum computing.

E.2 FIDAInform

http://www.fidainform.it/

Federazione Nazionale delle Associazioni Professionali di Information Management: è la federazione a livello nazionale di alcune associazioni no-profit di professionisti operanti nell'ambito ICT. Si propone come "nodo" attivo del Sistema-Paese per lo sviluppo del settore delle tecnologie dell'informazione e della comunicazione (ICT), promuovendo la professionalità dei Soci. FIDAInform ha creato Comunità Cooperative, un gruppo di altre associazioni di persone non operanti ma utenti in ambito ICT, grazie alle quali estende il bacino di interlocutori e di competenze, e che ha coinvolto in alcuni suoi progetti. Attualmente i progetti di FIDAInform o ai quali collabora sono:

- La collaborazione ed il supporto alle iniziative OAD 2026
- Il coordinamento con le associazioni socie e l'attuazione di iniziative di **mentorship gratuite** per singoli professionisti, giovani e no, PMI e startup.
- Il progetto "Autonomia Digitale", per l'analisi e la produzione di un innovativo documento-proposta sul tema, sempre più caldo e critico, dell'indipendenza e della sovranità digitale in Italia, inquadrando il tema nell'ambito dell'Unione Europea. L'aspetto innovativo è dato soprattutto dall'analisi del livello di autonomia digitale, in ottica Italia/UE, dei principali prodotti e servizi ICT europei rispetto a quelli più diffusi e conosciuti a livello mondiale.
- Da marzo 2025 FidaInform si è associato a UNINFO per le attività del Comitato Tecnico (CT) 526 APNR - Attività Professionali Non Regolamentate ICT. In particolare, ha iniziato a partecipare attivamente con 3 suoi esperti al Gruppo di Lavoro (GL) 09 "Profili di ruolo professionale manageriali operanti nell'ICT". Tale partecipazione rientra nella strategia FIDAInform di fornire contributi concreti per la crescita professionale di chi si occupa di ICT.

E.3 Servizio Polizia Postale e per la Sicurezza Cibernetica



Il Servizio polizia postale e per la sicurezza cibernetica provvede alla direzione e al coordinamento delle attività di competenza della Specialità polizia postale e delle comunicazioni della Polizia di Stato, e svolge le funzioni di Organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni stabilite dalla legge. Il Servizio dispone di 18 Centri Operativi per la Sicurezza Cibernetica, attivi nei principali capoluoghi di regione, e di 82 Sezioni Operative per la Sicurezza Cibernetica, presenti nelle province. Il Servizio si articola in cinque Divisioni, di cui si evidenziano le principali attività.

- **Prima Divisione:** si occupa della formazione e la pianificazione strategica delle risorse umane; sviluppa campagne di prevenzione e di educazione alla legalità online; assicura la gestione dell'archivio del servizio e le attività del Commissariato di PS online.
- **Seconda Divisione:** svolge attività di prevenzione e di contrasto degli illeciti online in tema di protezione dei minori, assicurando le attività di prevenzione e di contrasto dei fenomeni di cyberbullismo, di istigazione alle condotte autolesioniste, delle dipendenze on line dei minori, nonché di ogni altra forma di aggressione online nei confronti dei minori stessi; assicura la gestione del Centro Nazionale di Contrasto alla Pedopornografia Online (C.N.C.P.O.); attraverso l'Unità di Analisi del Crimine Informatico (U.A.c.I.) cura l'analisi di tutti i reati e fenomeni di competenza.
- **Terza Divisione**: svolge le attività per la prevenzione e il contrasto degli attacchi informatici in relazione ai danni delle infrastrutture critiche attraverso il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.C.); per la prevenzione ed il contrasto alle minacce eversivo-terroristiche in rete, mantenendo rapporti con i collaterali organi esteri di polizia e con gli enti della cooperazione internazionale, assolvendo altresì alle funzioni del Punto di contatto nazionale; svolge attività di ricerca e di sviluppo di soluzioni tecnologiche avanzate per il supporto tecnico-operativo alle attività istituzionali, con particolare riferimento alle attività di analisi forense.
- **Quarta Divisione**: assicura il coordinamento delle attività informative e investigative per la prevenzione e il contrasto dei fenomeni di criminalità informatica, caratterizzati dall'utilizzo di particolari tecniche di hacking, tecnologie software e hardware per acquisire, riprodurre e utilizzare fraudolentemente "identità digitali", codici di utilizzo di servizi bancari online o di carte di pagamento nelle transazioni elettroniche o che implichino la contraffazione o l'illecito utilizzo dei mezzi di pagamento elettronici.
- **Quinta Divisione:** cura la gestione dell'infrastruttura tecnologica del Servizio, nonché la custodia del materiale informatico assegnato; garantisce il supporto tecnico-operativo; assicura supporto in materia di sistemi di intelligenza artificiale per la sicurezza cibernetica; cura i rapporti con gli interlocutori di riferimento, pubblici e privati, attivi nel campo della ricerca e dell'innovazione scientifica.

ALLEGATO F - Profilo Partner

Gruppo Qintesi



www.qintesi.com

Il Gruppo Qintesi – con un organico di oltre 400 dipendenti – è una *Tech-Company* che eroga servizi di *management consulting* e *system integration*. Contribuisce ad accrescere il valore e migliorare la competitività dei clienti supportandoli nei processi di digitalizzazione ed innovazione, attraverso una *value proposition* basata su soluzioni applicative SAP, Google, Kyriba, SAP Fioneer e Anaplan, implementate con l'utilizzo di metodologie certificate ed il costante riferimento alle *best practices* di settore.

Il gruppo Qintesi è **Gold Partner SAP** con la qualifica di "Service Partner", "Build Partner" e "Sell Partner" ed ha ottenuto differenti riconoscimenti da parte di SAP.

Qintesi opera su tutto il territorio con sedi a Milano, Roma, Bergamo, Venezia, Mantova e Brescia oltre ad intervenire abitualmente in contesti internazionali. I mercati di riferimento sono i financial services, in particolare il mondo assicurativo; engineering & construction, manufacturing, services & utilities, consumer products, fashion, transportation.
Il Network copre in maniera sinergica molteplici aree funzionali, declinando ciascuna soluzione in base alle specificità di settore che contraddistinguono i differenti business. Oltre a coprire l'infrastruttura IT (con annessi servizi di manutenzione, project e process management), ha solide competenze in particolare in area finance & treasury, controlling, compliance & risk, sourcing & procurement e manufacturing.

Il Gruppo Qintesi ha ottenuto le seguenti certificazioni:

- **ISO 9001:2015** per "Progettazione, sviluppo e messa in opera di soluzioni informatiche in ambito gestionale, amministrativo e finanziario", dal 2016, una delle prime realtà del proprio settore di riferimento ad aver ottenuto questa certificazione;
- **ISO/IEC 27001:2013** per **"**Gestione della sicurezza delle informazioni per la fornitura di servizi di configurazione di soluzioni informatiche pacchettizzate a supporto dei processi operativi, direzionali e strategici**",** dal 2022**.**
- **UNI/PdR 125:2022** per la "Parità di genere", ottenuta nel 2023, che attesta l'impegno di Qintesi nel supportare l'empowerment femminile all'interno dei percorsi di crescita aziendale, lo sviluppo di una leadership equa ed il contrasto di stereotipi, divari, penalizzazioni e disparità a tutti i livelli.

Qintesi ha anche ottenuto importanti riconoscimenti, quali:

- Rating della Legalità, attribuito da AGCM, Autorità Garante della Concorrenza e del Mercato, per gli alti standard di qualità di Qintesi e l'attenzione posta sui principi etici nei comportamenti aziendali;
- Campione della Crescita 2025, attribuito da uno studio sulle aziende più dinamiche in Italia, condotto dall'Istituto Tedesco di Qualità (ITQF)e da "La Repubblica Affari&Finanza";
- Eccellenza dell'anno – Innovazione e sostenibilità applicativi IT integrati, attribuito a dicembre 2022 da Le Fonti Awards.

Qintesi ha realizzato alcuni tra i primi progetti a livello europeo di migrazione a SAP S/4HANA su piattaforma Google Cloud Platform; è attiva, inoltre, in importanti progetti di digital transformation basati sulla piattaforma Google.

Qintesi ha avviato una partnership con **Kyriba**, società leader nelle soluzioni di tesoreria e finanza in cloud, che offre funzionalità essenziali per la gestione della cassa e del rischio, i pagamenti e le soluzioni di capitale circolante.
Qintesi ha stretto una partnership con SAP **Fioneer**, leader globale nelle soluzioni software per l'industria dei servizi finanziari al fine di fornire alle istituzioni finanziarie soluzioni all'avanguardia e supportarle nell'implementazione di progetti complessi.
Qintesi ha stretto una partnership anche con **Anaplan**, piattaforma leader di pianificazione e analisi degli scenari progettata per ottimizzare il processo decisionale nel complesso ambiente aziendale odierno, consentendo alle imprese di superare la concorrenza e il mercato.

Inoltre, Qintesi è tra i primi partner **Planon** in Italia, rafforzando il suo ruolo di innovatore nell'ecosistema SAP e aprendo nuove opportunità di crescita anche a livello internazionale. Da Gennaio 2026 la soluzione Planon è diventata SAP solution extension, per le soluzioni relative al Real Estate e Facility Management, andando a colmare i processi non coperti da SAP Real Estate Flexible e SAP Plant Maintenance.

Nell'ambito della consulenza direzionale comprende la Service Line dedicata "Management & Consulting", per offrire al mercato servizi professionali idonei a supportare le imprese nei loro percorsi di crescita, portando competenze manageriali ed efficaci strumenti operativi in ottica "best practice" di settore.

Con riferimento a tematiche attuali per le imprese, come i processi di *Governance, Risk & Compliance*, anche in ottica di *business continuity*, Qintesi si propone come un player specializzato su questi contenuti che richiedono un mix di competenze funzionali e normative relative ai processi di *Compliance* e *Risk Management*, insieme a competenze tecnologiche legate alla *Cyber Security* e alla *Data Governance*.

La roadmap progettuale di Qintesi sul tema Cyber Security prevede un approccio integrato metodologico-applicativo a supporto di concrete necessità di sicurezza digitale perseguite dai propri Clienti, con l'obiettivo di rispondere alle più attuali richieste in tema di sicurezza e protezione del patrimonio informativo aziendale.



ALLEGATO G - Profili Patrocinatori

A.I.S.I.S.

Associazione Italiana Sistemi Informativi in Sanità, raggruppa i professionisti ICT nelle aziende sanitarie italiane pubbliche o private, e favorisce la crescita dell'attenzione sulle problematiche connesse all'utilizzo dell'ICT in sanità come leva strategica di cambiamento.

https://www.aisis.it/

AITASIT

AITASIT è un'associazione scientifica apartitica, apolitica e senza scopi di lucro che riunisce i tecnici sanitari di radiologia medica specialisti nella gestione dei sistemi informativi in diagnostica per immagini.

http://www.aitasit.org/

ANIPA

Associazione Nazionale Informatici Pubblici e Aziendali, costituita nel 1991 in ambito del Ministero del Tesoro, di Grazia e Giustizia, dei Beni Culturali e dei Lavori Pubblici, si è poi estesa a tutte le altre Pubbliche Amministrazioni Centrali e Locali, al Para Stato, alle scuole e ai privati. Obiettivi principali includono il riconoscimento e la valorizzazione dei ruoli informatici e la formazione continua.

https://www.anipa.it/

ANORC

ANORC si esprime in due associazioni no profit, ANORC Mercato, rappresentativa del mondo aziendale, e ANORC Professioni, punto di riferimento per i professionisti. ANORC Mercato e ANORC Professioni sono due associazioni impegnate nel campo della digitalizzazione e della protezione del patrimonio informativo e documentale in ambito pubblico e privato, promuovendo il dialogo istituzionale, la formazione e l'aggiornamento professionale, l'organizzazione di eventi, nonché lo sviluppo di attività informative e di comunicazione del settore.

https://anorc.eu/

Club Dirigenti Tecnologie dell'Informazione di Roma

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT dell'area romana-laziale, che si propone di contribuire allo sviluppo sociale, economico e industriale del Paese tramite la promozione dell'uso delle tecnologie dell'informazione. Aderisce a FIDAInform.

https://www.cdti.org/

Confassociazioni digital

E' la confederazione delle associazioni professionali operanti nel digitale/ICT, che fa parte della più generale Confassociazioni. Obiettivo primario è la crescita delle associazioni professionali ed il loro dialogo con le istituzioni e le altre parti sociali, per la crescita e lo sviluppo del Paese in termini di innovazione, creatività e qualità nelle prestazioni fornite al cittadino/consumatore.

https://www.confassociazioni.eu/

CSIG

Il Centro Studi Informatica Giuridica di Ivrea-Torino è un'associazione interdisciplinare indipendente e senza scopo di lucro che si occupa in particolare del diritto applicato alle nuove tecnologie.

http://www.csigivreatorino.it/

OWASP Italy

Capitolo italiano della mondiale OWASP® Foundation, associazione impegnata a migliorare la sicurezza del software attraverso progetti software open source guidati dalla comunità, e organizzando conferenze locali e globali.

https://owasp.org/www-chapter-italy/

Digital Security Festival

Digital Security Festival è l'evento nazionale per la divulgazione della cultura e della sicurezza digitale a persone, aziende, scuole e istituzioni. Diverse location, diverse regioni, per un evento diffuso ma unitario.

https://www.digitalsecurityfestival.it/

SESAMO

Associazione Nazionale degli Amministratori di beni immobili, denominata SESAMO (Sindacato Europeo Servizi Amministrazioni Manutenzioni Organizzazioni Condominiali): persegue il costante controllo della qualità ed eticità dei servizi prestati dagli Amministratori associati grazie anche ai corsi di formazione per amministratori e condomini

http://www.sesamoamministratori.it/

ALLEGATO H - Studio MRAB

Lo Studio MRA Bozzetti, fondato e diretto da Marco R. A. Bozzetti, opera nella consulenza direzionale e organizzativa nell'ambito dei sistemi informativi, della sicurezza digitale e della governance ICT.

Lo Studio valorizza la pluridecennale esperienza professionale del suo fondatore, maturata nella direzione di sistemi informativi complessi, nella consulenza, nella formazione e nelle attività associative e di normazione tecnica.

Le principali aree di intervento comprendono:

- **Governo e gestione del Sistema Informativo:** supporto alla definizione di strategie, politiche, processi organizzativi e sistemi di controllo.
- **Sicurezza digitale**: supporto alla governance strategica e alla gestione operativa della sicurezza digitale dell'organizzazione, al suo miglioramento continuo, all'analisi del rischio e delle vulnerabilità e agli aspetti organizzativi, gestionali ed economici.
- **Competenze, ruoli e organizzazione ICT**: valutazione e sviluppo delle competenze, definizione dei ruoli professionali e supporto all'evoluzione dell'organizzazione ICT.
- **Compliance normativa**: supporto nell'analisi e nell'applicazione di requisiti normativi, standard, controlli e sistemi di gestione con una visione integrata dell'organizzazione.
- **Trasformazione digitale**: accompagnamento nei percorsi di evoluzione digitale, mettendo in relazione organizzazione, processi, competenze e tecnologia.
- **Analisi del Valore ICT**: Approcci di analisi del valore applicati all'ICT per supportare valutazioni, priorità e decisioni in termini di efficacia, utilizzo e sostenibilità degli investimenti.
- **Formazione**: Interventi formativi collegati alle aree di competenza, progettati in relazione alle esigenze delle organizzazioni e dei professionisti coinvolti.

Lo Studio MRAB cura inoltre iniziative di ricerca, divulgazione e approfondimento sui temi della sicurezza digitale. Tra queste rientra l'Osservatorio Attacchi Digitali in Italia (OAD), ideato e coordinato da Marco R. A. Bozzetti, che mantiene la propria indipendenza metodologica e scientifica.

Studio MRAB

Via Savona 26 – 20144 Milano
Sito web: https://www.malaboadvisoring.it/

E-mail: mrab@mrab.it

OAD
Osservatorio
Attacchi Digitali
in Italia

Patrocinatori



www.oadweb.it