OAD
Osservatorio
Attacchi Digitali
in Italia

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

RAPPORTO 2025 OAD

A CURA DI MARCO R. A. BOZZETTI

In collaborazione con:

AICA · Polizia Postale e delle Comunicazioni · FIDA INFORM · malabo ICT Advisory

Silver Sponsor

QINTESI

Prefazione 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 aiuteranno alla diffusione del presente Rapporto OAD 2025.
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 allo Sponsor Qintesi e alle persone che hanno collaborato in vario modo alla realizzazione del questionario on line e del rapporto finale:

- per AIPSI: Massimo Chirivì, dott.ssa Elena Bernucci
- per Malabo Srl: dott. Andrea Bozzetti
- 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,.

Disclaimer - Dichiarazione di non responsabilità

I grafici ed i testi del presente Rapporto OAD 2025 sono stati elaborati e redatti con la massima accuratezza e correttezza possibile, partendo dalle risposte al questionario online totalmente anonimo e che pertanto non possono essere verificate. La loro affidabilità, dato il numero delle risposte, è significativa come tendenza, ma non sono in alcun modo di responsabilità da parte dell'autore, Marco R. A. Bozzetti, di Malabo Srl, di AIPSI, né di alcun altro Sponsor e Patrocinatore. Tutte le informazioni pubblicate NON costituiscono in alcun modo un servizio di consulenza, né di offerta ai lettori. Marco R. A. Bozzetti, Malabo Srl, AIPSI, gli Sponsor ed i Patrocinatori di **OAD 2025** NON sono e NON potranno essere responsabili di qualsivoglia perdita o danno in cui si possa incorrere in seguito all'affidamento sul contenuto delle analisi e delle indicazioni del presente **Rapporto OAD 2025**.

OAD è un progetto scelto da Repubblica Digitale

Rapporto OAD 2025 pubblicato il 12 ottobre 2025.

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

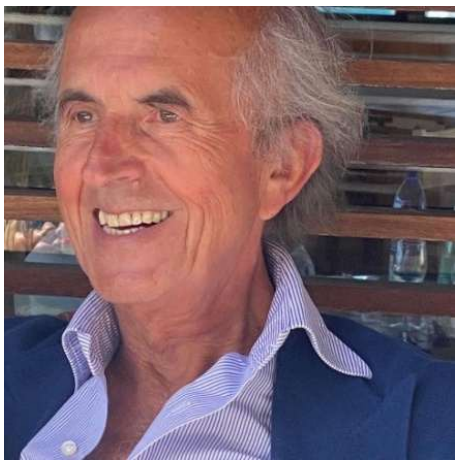
AIPSI c/o Malabo srl Via Savona, 26 20144 Milano - tel. 02 72191512 aipsi@aipsi.org

Malabo Srl Via Savona 26 20144 Milano - tel. 02 72191512 info@malaboadvisoring.it

INDICE Rapporto OAD 2024

PREFAZIONI

PREFAZIONE del dott. Massimo Di Virgilio



Perché un 'osservatorio', in generale, e perché un osservatorio come quello OAD.

Perché in una società in continua e rapida evoluzione, è indispensabile prestare sempre maggiore attenzione a tutto ciò che introduce elementi di cambiamento nella vita delle persone.

La tecnologia, essendo da sempre un poderoso motore di trasformazione della nostra società, merita di essere trattata con molta più cautela e prudenza di quanto si riesca a fare, sottoponendola ad una opportuna e approfondita vigilanza. A maggior ragione oggi, per la capacità che essa ha di agire in forme sempre più articolate, sviluppando la sua azione a largo spettro e con grande rapidità; coinvolgendo masse sterminate, a tutte le latitudini e a tutte le longitudini. Ma non basta, perché essa si insinua anche nel profondo, incidendo nei modi di vivere e di operare delle persone, nelle loro diverse e molteplici vesti di cittadini, lavoratori, docenti, studiosi, studenti, elettori, genitori, lettori e spettatori, nelle loro attività pubbliche e private, influenzando i loro comportamenti, le loro decisioni e le loro relazioni.

Etimologicamente un 'osservatorio' è un luogo o uno strumento, dal quale o con il quale si 'osserva', cioè si custodisce, si guarda attentamente, si tiene d'occhio ciò che accade intorno a noi, nel nostro mondo. È curioso, è invadente, è invasivo, cerca di cogliere gli aspetti più intimi, perché vuole andare alla radice, vuole scoprire, informare, allertare, fornire dei segnali, dare delle indicazioni, suggerire.

È ciò che fa pregevolmente il lavoro dell'ing. Marco Bozzetti (tra i suoi tanti ruoli e titoli, mi piace citare quello di mio predecessore, alcuni anni fa, alla guida di FIDAINFORM, per sottolineare quanto lui abbia inciso nella nostra Federazione, in generale, e in particolare sui temi della Cybersecurity, e quanto per quest'ultima la nostra Federazione sia stata uno dei luoghi di elezione del dibattito sviluppatosi nel nostro Paese nel corso di molti anni) e dei suoi collaboratori; un impegno che merita molta attenzione non solo e non tanto per il grande rigore specialistico e la grande cura con cui viene realizzato ogni anno, qualità che mi permetto di ritenere ormai acclarata, ma anche e, forse soprattutto, per la sollecitazione culturale manageriale, imprenditoriale e professionale che propone a tutti i destinatari. Una platea che dovrà ancor più allargarsi perché, per formare una coscienza critica e autocritica, indispensabile per vivere in un mondo sempre più digitalizzato, non basterà che questa sia conseguita solo dagli addetti ai lavori, cosa peraltro scontata, ma anche da schiere molto ampie di utilizzatori, perché, a maggior ragione in uno scenario globalizzato, per navigare in acque a dir poco insidiose, occorre un grado di consapevolezza che oggi non c'è.

FIDAINFORM e la neonata 'Comunità Collaborative', che annovera già ventidue associazioni, daranno il loro massimo contributo perché la diffusione del Rapporto OAD sia accompagnata da 'azioni collettive', indispensabili per sostenere questa meritoria sfida, ribadendo i complimenti ad AIPSI e formulando l'auspicio che si possa dar vita a un 'patto' e a una 'alleanza' con quante più associazioni possibili, per incrementare il numero dei soggetti coinvolti.

Massimo di Virgilio
Presidente FIDAInform

PREFAZIONE del dott. Ivano Gabrielli

La sicurezza nel dominio cibernetico rappresenta uno degli asset più significativi del sistema Paese per la protezione della dimensione digitale che permea ogni ambito della vita sociale ed economica.

In tale scenario, il Rapporto OAD 2025 – l'indagine annuale sugli attacchi digitali condotta dall'Associazione Italiana Professionisti Sicurezza Informatica (AIPSI) – rappresenta un riferimento autorevole per l'analisi della minaccia informatica e per la valutazione dello stato di salute dei contesti produttivi, pubblici e privati.

Nel corso del 2024, il Servizio Polizia Postale e per la Sicurezza Cibernetica, attraverso il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), ha gestito oltre 12.000 attacchi informatici significativi, emesso più di 59.000 alert di sicurezza e avviato 63 collaborazioni internazionali. Questo impegno è stato esteso e rafforzato dall'operatività delle sue articolazioni territoriali: 18 C.O.S.C. e 82 S.O.S.C., che presidiano il territorio nazionale, garantendo tempestività negli interventi e supporto qualificato alle realtà locali.

L'azione di contrasto ai reati informatici ha coinvolto fenomeni complessi tra i quali phishing, ransomware, frodi BEC, sextortion e diffusione non consensuale di contenuti intimi, con oltre 55.000 eventi segnalati all'autorità giudiziaria. Parallelamente, il Commissariato di PS Online ha svolto un fondamentale ruolo di informazione e assistenza ai cittadini, offrendo contenuti aggiornati, raccogliendo segnalazioni e promuovendo una comunicazione diretta e accessibile.

Queste azioni si sono integrate con un intenso programma di campagne di prevenzione e sensibilizzazione, mirate a diffondere cultura della sicurezza digitale, promuovere pratiche responsabili e rafforzare la consapevolezza dei rischi, in particolare tra giovani, imprese e fasce vulnerabili.

In un contesto cibernetico in rapida evoluzione e con implicazioni sempre più strategiche e geopolitiche, la sinergia tra istituzioni, ricerca e settore privato è fondamentale. Il Rapporto OAD 2025 di AIPSI si conferma quindi un tassello essenziale per orientare le scelte operative e politiche in materia di sicurezza informatica.

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

PREFAZIONE del dott. Antonio Piva

Il Rapporto OAD 2025 offre un quadro aggiornato e puntuale sullo stato della sicurezza informatica in Italia, restituendo una fotografia utile non solo alle aziende e alle organizzazioni, ma anche ai cittadini.
Viviamo in un'epoca in cui la dimensione digitale permea ogni aspetto della nostra vita e pertanto consapevolezza su queste tematiche e sulla cybersecurity in particolare non è più un'opzione, ma un prerequisito essenziale per esercitare una piena cittadinanza.

In questo contesto, l'Osservatorio non si limita a descrivere il presente; ha il merito di tracciare rotte future, indicando a Istituzioni, imprese e individui la direzione da intraprendere per navigare in sicurezza.

Resistere all'insicurezza digitale sistemica, che caratterizza il panorama globale dal 2018, è possibile. Ma richiede una responsabilità individuale diffusa e una chiara comprensione dei rischi, delle minacce e delle strategie di mitigazione da parte di tutti gli attori in gioco. Solo così è possibile valutare rischi, implementare contromisure e gestire gli impatti in modo efficace.

Migliorare le proprie competenze digitali non è solo una strategia per l'occupazione o l'imprenditorialità; è la condizione indispensabile per agire con autonomia e responsabilità. Che si tratti di professionisti, imprenditori o semplici cittadini, investire sulle proprie skill significa non solo accedere in modo consapevole al mondo del lavoro, ma anche mantenere quella “autodeterminazione informativa” che la trasformazione digitale tende a mettere sotto pressione.
Tutto ciò si traduce nella necessità di adottare in modo naturale e continuativo quei comportamenti proattivi che rientrano nella “cyber hygiene”.
Il fattore umano rimane il perno su cui far leva, l'unico elemento in grado di contrastare efficacemente le nuove sfide, dall'IA generativa alla guerra ibrida alle campagne di disinformazione, che sfruttano proprio le vulnerabilità psicologiche e informative.

Avere una chiara mappa degli attacchi e delle buone pratiche, come quella fornita da questo Rapporto, permette a ciascuno di autovalutare la propria postura di sicurezza. È il primo, indispensabile passo per avviare quel percorso di miglioramento continuo che ci permette di proteggere noi stessi, le nostre attività e, in definitiva, la nostra società.

Rafforzare l'anello umano non è solo una priorità: è il comune denominatore di ogni efficace strategia di cybersecurity. È la missione di AICA e deve diventare l'impegno di tutti, per rendere possibile affrontare con maggiore sicurezza le sfide del presente e del futuro"

Antonio Piva
Presidente AICA

1. Sintesi direzionale

L'Osservatorio Attacchi Digitali in Italia, OAD[1]**,** di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica (capitolo italiano della mondiale ISSA), nel 2025 giunge al 18° anno consecutivo di indagini. L'indagine è l'unica in Italia sull'argomento, effettuata con un questionario online via web rigorosamente anonimo per chi lo compila. OAD 2025 è stata effettuata da AIPSI tramite Malabo Srl (la società di Marco R. A. Bozzetti. ideatore e autore di OAD), e in collaborazione con il **Servizio Polizia Postale e per la Sicurezza Cibernetica, AICA** e **FIDAInform**.

Il Rapporto OAD 2025 analizza l'evoluzione degli attacchi digitali **rilevati in Italia nel 2024**, con particolare attenzione agli impatti sui Sistemi Informativi (SI) delle aziende/enti rispondenti, oltre alle misure tecniche ed organizzative di sicurezza digitale adottate dalle aziende/enti rispondenti. Approfondimenti su tre aree di attacco, tra le più critiche attualmente: i siti web, gli ambienti OT, Operational Technology, le applicazioni e i servizi ICT basati su Intelligenza Artificiale.

Contesto e scenario

Il 2024 ha registrato un peggioramento del contesto geopolitico globale (soprattutto in Ucraina e Medio Oriente), con il crescente utilizzo di **guerre informatiche**, **disinformazione** e **attacchi mirati** ai SI di imprese pubbliche e private. Le **tecnologie di Intelligenza Artificiale (IA)** sono state usate sia come strumento che come bersaglio degli attacchi.

Principali evidenze

- Il **71%** dei rispondenti ha subito almeno un attacco digitale intenzionale.
- Le **tipologie di attacco** (che cosa si attacca) **più diffuse,** tra le 16 considerate, includono:
  - Modifiche dannose o non autorizzate a programmi/configurazioni ICT (**29 %**);
  - Uso malevolo o non autorizzato di interi sistemi ICT (**24%**);
  - Attacchi DoS/DDoS (**20%**), spesso collegati a gruppi di attaccanti filo-russi;
  - Attacchi alla supply chain (**15%**), un rischio globale significativo secondo il WEF;
  - Attacchi ai sistemi basati sull'intelligenza artificiale (**8%**).
- Le **tecniche di attacco** (come si attacca) **più diffuse** includono, tra le 8 considerate: attacchi multi-tecnica combinata (**37%**), social engineering (**16%**), malware/ransomware (**10%**).

Focus di OAD 2025 sui seguenti ambienti critici

- **Sistemi Web**: 58% ha subito attacchi; il 64% ha registrato disservizi >2 giorni; vulnerabilità principali legate a software obsoleti e configurazioni errate.

[1] OAD di AIPSI (Associazione Italiana Professionisti Sicurezza Informatica, Capitolo italiano della mondiale ISSA) costituisce l'unica indagine online in Italia (completamente indipendente e "terza" rispetto ai vari attori in gioco) sugli attacchi digitali intenzionali ai sistemi informativi delle aziende e degli enti pubblici operanti in Italia, e sulle misure tecniche ed organizzative che questi hanno in esercizio. OAD non predefinisce uno specifico bacino di rispondenti, il medesimo negli anni, ma consente a chiunque, interessato e coinvolto nella gestione di un sistema informativo di una azienda/ente, un pieno e libero accesso al questionario online, in maniera totalmente anonima. Dato il numero di risposte raccolte e la loro distribuzione tra aziende ed enti pubblici di varie dimensioni e appartenenti a diversi settori merceologici, l'indagine OAD fornisce preziose indicazioni sul fenomeno degli attacchi digitali intenzionali in Italia e delle misure di sicurezza in essere nei sistemi informativi delle imprese rispondenti. OAD riesce a coinvolgere nell'indagine anche le piccole e piccolissime realtà, che costituiscono in Italia la stragrande maggioranza e che le altre indagini nazionali ed internazionali difficilmente considerano ed analizzano.

- **Sistemi OT, Operational Technology**: colpite il 32% delle organizzazioni con sistemi OT; blocchi >2 giorni nell'85% dei casi.
- **Sistemi IA**: 24% ha rilevato attacchi; principali minacce: **model poisoning** e **gestione impropria degli output**.

Profilo dei rispondenti

- **62%** piccole-medie organizzazioni (fino a 250 dipendenti); settori principali: ICT, manifattura, sanità.
- Ruoli rispondenti: vertici aziendali (26%), CIO (23%), consulenti specializzati (20%).

Livello di sicurezza e terziarizzazione della gestione del SI e della sua sicurezza

- Il 75% considera il proprio SI **essenziale**; il 25% rientra nelle **infrastrutture critiche** (NIS2).
- Il **40%** ha compilato le sezioni opzionale del questionario OAD 2025 sulle misure di sicurezza adottate, ed ha fornito i seguenti principali dati:
    - Utilizzo policy e procedure: 80%
    - Effettuazione analisi dei rischi: 81%
    - Uso Firewall applicativi: 80%
    - Uso Backup e ripristino strutturato: 77%
    - Piano di Disaster Recovery: 70%
- **Terziarizzazione** ampia: gestione totale esterna del SI e/o della sicurezza nel 24–27% dei casi; parziale nel 42–46%.

Conclusioni

Nonostante un buon livello di sicurezza dichiarato, la frequenza e l'impatto degli attacchi digitali restano molto elevati. Il 2024 conferma il permanere di un periodo di **insicurezza digitale sistemica**, iniziato dal 2018, in cui le misure difensive in essere non bastano a prevenire e/o contrastare tutti gli attacchi. Serve un cambio di paradigma: dalla protezione alla **resilienza**.

Raccomandazioni

- Rafforzare la **business continuity** e il **Disaster Recovery** per una effettiva **resilienza** del Sistema Informativo
- Investire in **formazione, automazione della gestione operativa della sicurezza digitale**, e nella **gestione del rischio ICT**.
- Monitorare e adattarsi costantemente all'evoluzione delle minacce, con particolare attenzione a **OT, IA e supply chain**.

1Bis Executive Summary

The 2025 edition of the **OAD**[2], Osservatorio Attacchi Digitali in Italia (**Observatory on Digital Attacks in Italy**), marks the eighteenth consecutive year of research on digital attacks and information system (IS) security in Italy. Once again, the OAD benefits from the collaboration of the Italian Postal and Cyber Police Service, which provided both data and text for Chapter 8 of this Report.

The OAD 2025 online survey covers intentional digital attacks detected throughout 2024. **Results confirm a sustained and serious spread of cyber incidents with significant operational and economic impacts**. The geopolitical instability of 2024—driven by hybrid wars linked to the invasion of Ukraine and the Palestinian conflict—fueled an escalation in cyberwarfare and large-scale disinformation campaigns on social, political, and religious issues. **Artificial Intelligence (AI) was extensively exploited both as an attack vector and as a misinformation tool.**

Chapter 3 outlines the global digital threat landscape, referring to the World Economic Forum and to ENISA (European Union Agency for Cybersecurity) annual Threat Landscape (ETL) reports, as well as to the Italian ACN (National Cybersecurity Agency) and the Postal and Cyber Police Service. The OAD 2025 survey introduced AI as both an attack target and a tool, and provided vertical analyses of cyber attacks to web systems, OT (Operational Technology) systems, and AI-based systems.
Respondents numbered in the hundreds, mainly ICT solution providers (21.4%), followed by manufacturing and construction (14.85%), healthcare and social services (14.41%), and business support services (10.48%). **SMEs represented 62.96% of respondents**, with 22.22% micro-enterprises (<10 employees). OAD remains unique in its consistent inclusion of SMEs (**over 60% every year**).
Respondent roles were mainly owners/executives (26.22%), CIOs (22.56%), and cybersecurity or IT specialists, confirming the ongoing outsourcing trend. Fewer than 10% were CISOs, CSOs, or CTOs.

In 2024, 71.18% of organizations experienced cyberattacks.
Among 16 attack families, the most common were:

- Malicious or unauthorized modifications to ICT programs/configurations (29.26%);
- Unauthorized use of ICT systems (23.58%);
- DoS/DDoS attacks (20%), often linked to pro-Russian hacker groups;
- Supply chain attacks (14.85%), a major global risk per WEF;
- AI-based system attacks (7.86%).

Among eight attack techniques, the most frequent were:

- 37.12% used multiple techniques simultaneously;
- 15.72% involved social engineering and illegal data collection;
- 10.04% employed malicious code, including ransomware.

[2] OAD is provided by AIPSI, the Italian Association of Information Security Professionals, thgat is the Italian Chapter of the global ISSA. OAD is the only online survey in Italy (completely independent and "third-party" with respect to the various stakeholders) on intentional digital attacks on the information systems of companies and public entities operating in Italy, and on the technical and organizational measures they employ. OAD does not predetermine a specific pool of respondents, which remains the same over time, but rather allows anyone interested and involved in managing a company's/institution's IT system full and free access to the online questionnaire, completely anonymously. Given the number of responses collected and their distribution among companies and public entities of various sizes and sectors, the OAD survey provides valuable insights into the phenomenon of intentional digital attacks in Italy and the security measures implemented in the respondent companies' IT systems. OAD also successfully involves small and very small businesses, which constitute the vast majority in Italy and are rarely considered or analyzed by other national and international surveys.

Vertical analysis

- of attacks on web systems revealed:
  - 94.15% use both on-premise and outsourced web systems;
  - 58.4% detected web application attacks, 60.6% of which affected cloud systems;
  - Technical vulnerabilities caused 93.83% of the most severe attacks, often linked to human error (44.44%);
  - Outdated/vulnerable software ranked first (39.51%), followed by misconfiguration (30.86%) and identity/authentication failures (25.93%);
  - 64.29% faced service disruption ≥2 days; 86.5% incurred higher IS costs, and 12.36% had budget-level impacts;
  - Sabotage (44.44%), fraud (40.74%), and extortion (~30%) were the top motives, while hacktivism (21%) and cyberwarfare (16%) showed rising geopolitical influence.

- for OT (Operational Technology) systems
  - used by 40.58% of respondents; 32.1% attacked:
  - Robotic systems were most affected (70%), followed by IoT/IIoT (55.56%);
  - 85% reported downtime >2 days, often spreading to IS applications (30% for 2–3 days);
  - 37% reported significant IS cost increases, 30% company-level budget impacts;
  - Sabotage dominated (93%), followed by vandalism (37%) and extortion (22%).

- for AI-based systems:
  - 41% already use AI applications; 23.8% faced digital attacks;
  - Based on OWASP Top 10 for AI (LLMs and GenAI), “Data and Model Poisoning” (35%) and “Improper Output Handling” (20%) were the main vulnerabilities;
  - Most AI vulnerabilities relate to “prompt” inputs and model training methods—partially regulated by the EU AI Act.

The IT systems (IS) of 87.57% of respondents is managed entirely in Italy; 61.58% operate without a Data Center, typical of SMEs. For 75.14%, the IS is critical to business continuity, and 25.42% provide essential or NIS2-critical services. Full outsourcing applies to 24.29% (IS management) and 27.43% (IS security), while 42–46% adopt partial outsourcing, confirming a strong trend toward managed cybersecurity services.
40% of respondents completed the optional section on digital security measures. Among these, 40.3% declared adequate and 46.8% high levels of IS security, with only 12.9% insufficient and none critical.

Key findings on **IS’s organizational, technical, and control measures** among this 40% sample include:

- Organizational Security Measures:
  - 80% have digital security policies and procedures;
  - 92% use user support tools;
  - 81% conduct digital risk assessments;
  - 52.38% perform audits;
  - 38% hold digital security certifications.

- Technical Security Measures:
  - 67.14% maintain high IS reliability;
  - 85.71% control physical access to ICT premises;
  - 79.1% use UPS systems;
  - 80.8% centrally manage passwords;
  - 57.58% monitor network performance and security;
  - 33.85% adopt secure software development practices;
  - 80% deploy application firewalls (FWA);
  - 84.7% manage corrective maintenance;
  - 43.75% follow backup best practices;
  - 76.56% apply recovery procedures.

- Management and Control Measures:
  - 81.25% have centralized IS control systems;
  - 78.79% manage IT supply chains;
  - 80% conduct vulnerability analyses;
  - 80.6% archive logs (46.27% also manage them);
  - 70% have Disaster Recovery plans; of these, 70% have tested alternatives.

Despite this maturity, cyberattacks remain widespread and impactful, underscoring that even advanced security systems cannot fully prevent digital incidents. OAD 2025 confirms global findings by WEF, ENISA, ACN, and the Italian Postal and Cyber Police Service: **systemic digital insecurity, ongoing since 2018, now defines the global landscape.**

The imperative is no longer full prevention but resilience — strengthening defenses while ensuring business continuity and tested Disaster Recovery capabilities to manage unavoidable insecurity.

2. L'indagine OAD

OAD, Osservatorio Attacchi Digitali in Italia, è l'unica indagine on line via web in Italia sugli attacchi digitali intenzionali ai sistemi informativi di aziende ed enti operanti in Italia, e sulle misure di sicurezza tecniche ed organizzative in essi presenti. L'indagine è rivolta liberamente e in maniera anonima ad aziende/enti di ogni settore merceologico, incluse le Pubbliche Amministrazioni Centrali e Locali, e di ogni dimensione (come numero di dipendenti e fatturato/giro d'affari). Essendo totalmente libero l'accesso ai questionari online su Internet, il campione emerso non ha stretta valenza statistica ma, dato il numero di risposte e la buona distribuzione per dimensioni e per settore merceologico delle aziende/enti di chi risponde, esso fornisce precise ed interessanti indicazioni sul fenomeno degli attacchi digitali in Italia, soprattutto per le piccole e piccolissime organizzazioni, che in Italia sono la stragrande maggioranza (si veda §3.3.2) e che difficilmente sono considerate nelle altre indagini nazionali ed internazionali.

OAD è una iniziativa di AIPSI, operativamente effettuata da **Malabo Srl** sia per la realizzazione del questionario online, sia per l'elaborazione dei dati e la stesura del rapporto finale, e con la preziosa collaborazione **del Servizio Polizia Postale e per la Sicurezza Cibernetica,** di **AICA** e di **FidaInform.**
L'obiettivo primario è di analizzare anno per anno sia il fenomeno degli attacchi digitali intenzionali nella realtà italiana, sia le misure di sicurezza digitale poste in esercizio sui sistemi informativi delle aziende/enti rispondenti al questionario, e di contribuire in tal modo alla formazione "continua" di chi si occupa e di chi deve decidere in merio alla sicurezza digitale. Infatti la compilazione del questionario prima e soprattutto la lettura del rapporto annuale poi contribuiscono alla crescita della cultura sulla sicurezza digitale e ad una maggior consapevolezza in merito, soprattutto verso i decisori "non tecnici", tipicamente figure di vertice dell'organizzazione, che decidono e stabiliscono budget ed interventi per la sicurezza digitale.

Il rapporto finale OAD intende essere un autorevole e indipendente riferimento per aiutare anche le piccole realtà nell'analisi e nella gestione dei rischi informatici, e per fornire un quadro chiaro ed autorevole della sicurezza digitale in Italia in termini sia di attacchi digitali sia di misure tecniche ed organizzative, oltre che dell'attuale quadro legislativo e normativo.

Un quadro contestualizzato nella realtà europea e mondiale, con riferimenti ai rapporti del World Economic Forum e delle Agenzie per la sicurezza digitale, quella europea ENISA e quella italiana ACN.

L'approccio adottato per tutte le indagini OAD consiste nel coinvolgere liberamente e in modo rigorosamente anonimo il maggior numero possibile di rispondenti al questionario online, comprendendo imprese pubbliche e private di ogni settore e dimensione. La diffusione del questionario avviene tramite tutti i canali mediatici di AIPSI, con il supporto delle associazioni patrocinanti. Questo metodo non prevede la definizione di un campione fisso anno dopo anno, ma al termine della raccolta emerge un insieme eterogeneo di rispondenti, provenienti da diversi settori merceologici, incluse le Pubbliche Amministrazioni, e di varie dimensioni in termini di numero di dipendenti.

2.1 L'indagine OAD 2025

OAD 2025 arriva al **18° anno** consecutivo di indagini online via web, ed è focalizzato sugli **attacchi subiti nel 2024** dai Sistemi Informativi (SI) delle aziende/enti rispondenti per:

- gli eventuali **siti e ambienti web, sia locali che terziarizzati;**
- gli eventuali **ambienti OT, Operational Technology**;
- gli eventuali ambienti applicativi **basati su Intelligenza Artificiale (IA)**.

Erano presenti nel questionario online solo due domande sulle altre tipologie di attacco rilevate nel 2024, per poter continuare l'analisi dei trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 al 2024.
Per semplificare il questionario e ridurre il tempo di compilazione, mantenendo comunque rilevanti i contenuti per l'analisi degli attacchi informatici e garantendo continuità con le informazioni raccolte nelle precedenti indagini, sono opzionali le due sezioni relative alle misure di sicurezza adottate. Tuttavia, la compilazione di questa parte è stata consigliata per permettere, al termine del questionario, di ottenere una **macro valutazione** automatica e anonima del **livello di sicurezza del SI** oggetto delle risposte.

Il questionario OAD 2025 è rimasto online da febbraio 2025 a fine agosto 2025: le/i rispondenti sono stati complessivamente **346**, un numero dello stesso ordine di grandezza delle indagini OAD degli anni precedenti: numero che AIPSI auspicava ben maggiore, data la semplificazione del questionario e il coinvolgimento di importanti associazioni patrocinanti, elencate nell'Allegato D di questo rapporto.

La fig. 2.1-1 mostra le copertine di tutti i Rapporti OAD pubblicati. Tutti rapporti annuali pubblicati sono scaricabili gratuitamente, insieme alla documentazione prodotta e/o raccolta di articoli e presentazioni ad essi correlati, dallo specifico sito web www.oadweb.it, che costituisce l'archivio documentale completo di tutte le iniziative negli anni sull'Osservatorio. Si ricorda che, fino al 2015 l'indagine era chiamata OAI, Osservatorio Attacchi Informatici in Italia; dal 2016 è stata chiamata OAD per evidenziare l'integrazione tra informatica e telecomunicazioni (come anche indicato dall'acronimo ICT, Information and Communication Technology, usato in Europa e usato nei Rapporti OAD).

Fig. 2.1-1

OAD 2025 annovera il **patrocinio gratuito** di numerose associazioni, il cui elenco, con una breve descrizione delle loro attività, è nell'Allegato D. Per OAD il ruolo attivo dei Patrocinatori è (o dovrebbe essere) significativo per poter allargare e stimolare il potenziale bacino dei compilatori del questionario via web, tipicamente tramite i loro soci e simpatizzanti. Inoltre, il loro supporto è prezioso per promuovere e diffondere il rapporto finale.

Il presente Rapporto OAD 2025, nel riportare ed analizzare quanto emerge dall'indagine sugli attacchi digitali e sulle misure di sicurezza in essere sui sistemi informativi, utilizza concetti tecnici, riferimenti a standard, framework e normative, pur non avendo la pretesa di essere un manuale sulla sicurezza digitale.
Concetti specifici, tecniche, acronimi, standard e best practice, leggi e normative sono nella maggior parte dei casi brevemente chiariti e referenziati con link nel testo del Rapporto, là dove sono citati per la prima volta.
Per agevolare la comprensione del presente rapporto è richiesta una conoscenza di base di informatica e di sicurezza digitale, e per facilitarne la lettura, è disponibile nell'Allegato B un glossario degli acronimi e dei termini tecnici specialistici usati.

3. Il quadro generale degli attacchi digitali intenzionali

L'indagine OAD fa riferimento al solo contesto italiano, ma per comprendere appieno il fenomeno degli attacchi digitali, che è un fenomeno mondiale, occorre inquadrarlo a livello europeo e mondiale.
L'arco temporale di riferimento di OAD 2025 è **l'intero anno 2024** durante il quale vari elementi hanno dominato e caratterizzato gli aspetti di sicurezza digitale:

- le **crescenti tensioni geopolitiche** tra l'occidente democratico e liberale ed altri stati che non lo sono, aggravate dalla "guerra dei dazi" voluta dall'attuale amministrazione Trump negli USA, che ha creato di fatto una spaccatura nel mondo occidentale liberale, e da varie guerre combattute da tempo sul campo, tra le quali le più critiche e note sono:
  - la guerra in Ucraina causata dall'invasione dell'Ucraina da parte della Federazione Russa a febbraio 2022, ma con un conflitto tra le due nazioni già iniziato nel 2014 con l'invasione della Crimea;
  - la guerra di Gaza, causata dall'attacco terroristico del 7 ottobre 2023 ad Israele da parte di Hamas, organizzazione palestinese islamista fondamentalista, e dalla reazione israeliana;
- il **crescente potere politico di attori che non rappresentano Stati**, quali ad esempio alcune grandissime aziende multinazionali, ed il conseguente declino di potere da parte degli stessi Stati. Questo fenomeno impatta significativamente sulle tensioni geopolitiche del precedente punto;
- la crescente **diffusione di tecnologie emergenti**, in primis quelle relative all'**intelligenza artificiale**, che pur offrendo significative innovazioni, da un lato introducono nuove vulnerabilità e rischi a chi le utilizza, dall'altro sono alla base di nuove tecniche di attacco.

A questi specifici fattori si devono aggiungere quelli "tradizionali", ossia attacchi digitali per ottenere illegali ricavi economici, dalle frodi finanziarie ai furti sui conti corretti bancarie, dai ricatti con ransomware, alla saturazione delle risorse dei sistemi informativi (DoS/DDoS), dai furti di informazioni e di identità digitali al furto "fisico" di dispositivi ICT, quali ad esempio i più avanzati smartphone che hanno un significativo mercato dell'usato.
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 operano sia per le strutture statali, di fatto in logica di guerra digitale (cyber warfare)[3], sia autonomamente per i loro obiettivi criminali, che sono quasi sempre di tipo economico.

Come approfondito nel Capitolo 4, dal 2019-20 si è entrati di fatto nell'**era della insicurezza digitale sistemica** (**systemic cyber insecurity**), ed anche il 2024 conferma questo stato, nel quale le contromisure adottate, pur numerose e costose, non sono sufficienti ed efficaci, e non riescono a contrastare tutti gli attacchi digitali.
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.

3.1 Il quadro a livello internazionale

A livello mondiale Il Global Risk Report[4] del World Economic Forum, WEF, nella sua ultima versione del 2025 evidenzia, si veda fig. 3.1-1, come **lo spionaggio cibernetico e le guerre digitali** siano **tra i primi dieci rischi "globali" a livello mondiale**: a breve termine sono al quinto posto ed a lungo termine sono previste al nono posto.

[3] 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*".
[4] https://www.weforum.org/publications/global-risks-report-2025/

Si noti che nelle precedenti edizioni del rapporto WEF, tra i primi dieci rischi globali, era considerato il rischio **cyber insecurity** che nella presente edizione non c'è più, di fatto sostituito con "lo spionaggio cibernetico e le guerre digitali**".** A giudizio dell'autore tale fatto dipende principalmente dall'acuirsi dell'instabilità geopolitica e dalla polarizzazione di fatto "anti-occidentale".

Fig. 3.1-1 (Fonte: World Economic Forum Global Risks Perception Survey 2024-2025)

Al primo posto, nel breve termine, si colloca la "**misinformation and disinformation**", analogamente alla precedente edizione. 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 sempre al quinto posto in ordine di criticità, così come nella precedente edizione del rapporto WEF. Esse **rimangono un grave pericolo**, soprattutto nell'ambito delle guerre sempre più ibride[5], delle tensioni geopolitiche, delle votazioni. Questo rischio spesso evidenzia anche la polarizzazione sociale[6] come uno dei rischi più gravi (al quarto posto nel breve e all'ottavo nel lungo termine, come evidenziato nella fig. 3.1-1) nello stesso arco di tempo.
Contenuti di scarsa qualità e mancanza di fiducia nelle fonti di informazione continuano a rappresentare una minaccia per la società.

Come mostrato nella fig. 3.1-2, essi hanno legami con gli altri rischi, tecnologici e non, individuati da WEF e rappresentano il rischio tecnologico-digitale a più alta influenza (si vedano le dimensioni del cerchio nella figura rispetto agli altri di colore viola).

[5] 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).
[6] 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.

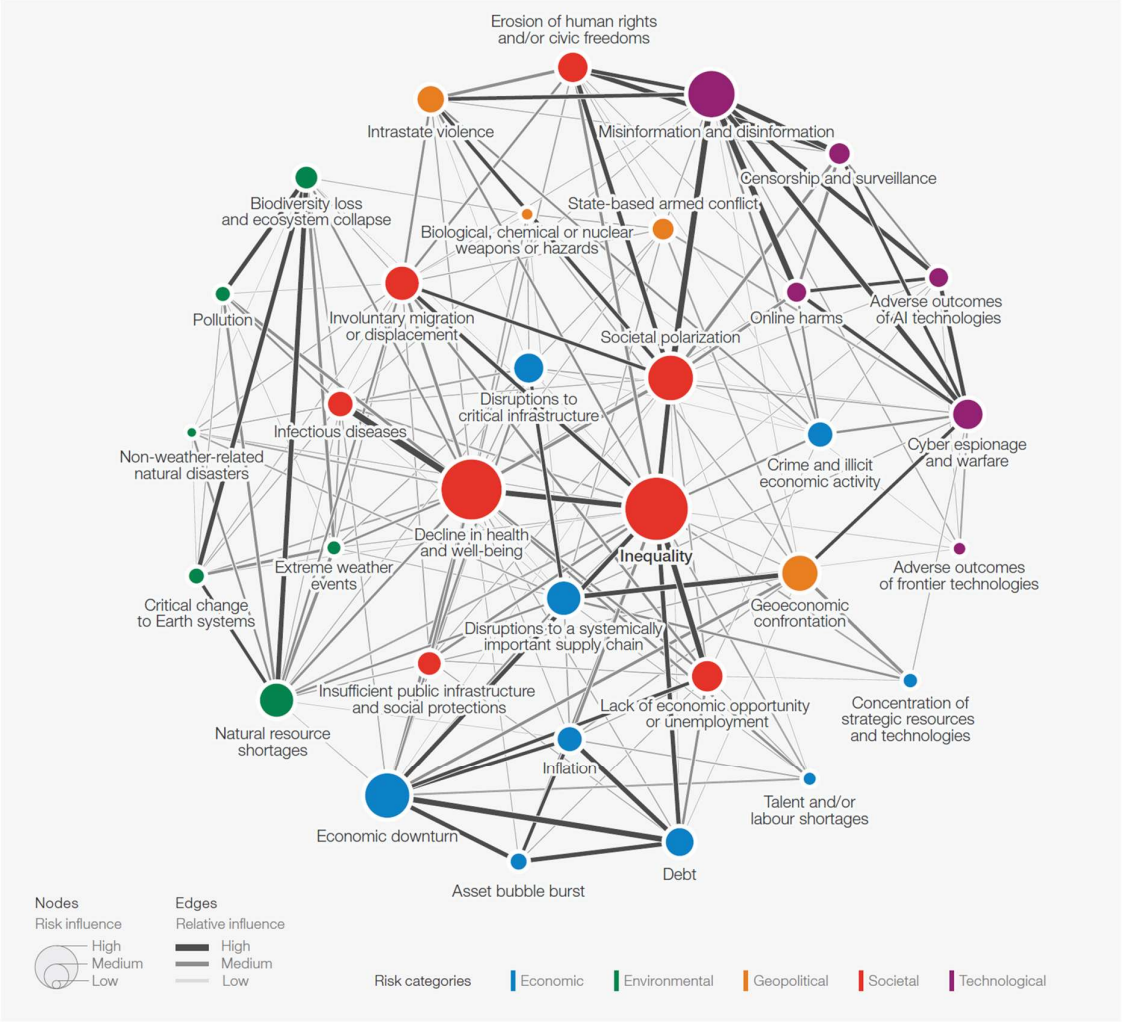


Fig. 3.1-2 (Fonte: World Economic Forum Global Risks Report 2025)

L'aumento di **informazioni false**, causa una voluta **ampia disinformazione** su vari temi, ma con gravi impatti nel quotidiano per le informazioni false, ma credibili, in settori quali l'economia, le leggi, le borse, la tecnologia, le scienze. Informazioni false o scorrette possono indurre individui ed organizzazioni a prendere decisioni sbagliate, con impatti che possono essere estremamente gravi.

L'invasione dell'Ucraina è solo la punta di un ben più grande iceberg di una guerra di fatto tra il mondo occidentale liberale e paesi non occidentali con dittature o democrazie illiberali: molti dei più recenti attacchi digitali rientrano di fatto in questa guerra ibrida da tempo in corso.

Nei secoli scorsi, la disinformazione e le false notizie in tempo di guerra hanno sempre costituito un'arma da parte di ogni belligerante, ma nell'attuale epoca di Internet diffusa a livello mondiale il fenomeno delle "fake news" ha raggiunto livelli estremamente critici, ed è sempre più difficile capire se un'informazione è corretta oppure no.

Tra i rischi tecnologici il Rapporto WEF 2025 considera, oltre alle già evidenziate "**misinformation and disinformation**" e la "**cyber espionage and warfare**", anche:

- Adverse outcomes of AI technologies: le conseguenze negative dei progressi nell'intelligenza artificiale e nelle capacità tecnologiche correlate (inclusa l'intelligenza artificiale generativa) su individui, aziende, ecosistemi e/o economie.
- Adverse outcomes of frontier technologies: i risultati inattesi e negativi di tecnologie di frontiera quali il quantum computing, le biotech, la geoingegneria[7].
- Censorship and surveillance: censura e sorveglianza che osservano in modo ampio e pervasivo un luogo o una persona o una struttura organizzativa per la soppressione di comunicazioni, informazioni e idee, fisicamente o digitalmente, nella misura in cui esse violano in modo significativo i diritti umani e civili (ad esempio, privacy, libertà di parola e libertà di espressione).
- Online harms: i danni online causati dalla erosione della protezione e/o prevalenza di comportamenti dannosi che rappresentano una minaccia digitale sia per le imprese sia per la salute emotiva o mentale e il benessere degli individui.

Per quanto riguarda il quadro dei **rischi causati dalle tecnologie ICT**, il Rapporto WEF evidenzia:

- Il crescente utilizzo di piattaforme digitali e il crescente volume di contenuti generati dall'intelligenza artificiale (per brevità nel seguito IA o AI) che stanno rendendo la disinformazione e la mala informazione sempre più diffuse, onnipresenti e divisive in campo sociale e geopolitico.
- I pregiudizi algoritmici potrebbero diventare più comuni a causa della polarizzazione politica e sociale e della disinformazione e la mala informazione ad essa associate.
- Una digitalizzazione più approfondita può semplificare la sorveglianza per governi, aziende e attori delle minacce, e questo diventa un rischio maggiore man mano che le società si polarizzano ulteriormente.

Nel lungo termine il Rapporto WEF evidenzia le tre aree di rischio più gravi, **inquinamento**, **biotecnologie** e **super invecchiamento** di alcune società, che, senza adeguate soluzioni, costituiranno punti di non ritorno per l'intera terra.

La fig. 3.1.3 mostra nel lungo termine (10 anni) i principali rischi per area geografica.

I rischi tecnologici (fondo viola), che includono quelli dell'ICT, nel complesso l'indagine WEF stima che si riducano, soprattutto rispetto a quelli dell'ambiente (fondo verde). Il rischio tecnologico più diffuso per area geografica sarà "**misinformation and disinformation**", che rimane l'unico rischio tecnologico per l'**Europa.** Da evidenziare come in **Nord America**, non sia previsto alcun rischio tecnologico.

[7] La geoingegneria, chiamata anche ingegneria climatica, è l'insieme delle tecniche e delle proposte che mirano a intervenire su larga scala sul clima terrestre per contrastare gli effetti del riscaldamento globale.

Fig. 3.1-3 (Fonte: World Economic Forum Global Risks Report 2025)

Il Rapporto WEF individua quattro "**forze strutturali**", che costituiscono lo sfondo (backdrop) ed il contesto di base dei rischi globali che si manifesteranno nel prossimo decennio e oltre:

- l'**accelerazione tecnologica**: nei prossimi 10 anni forte innovazioni tecnologiche con tutti i relativi rischi tecnici e sociali;
- i **cambiamenti geostrategici**: oltre alla forte instabilità, si assiste da un lato ad una concentrazione di potere, dall'altro alla perdita di autorevolezza e di reale controllo da parte di istituzioni multilaterali quali ad esempio l'ONU;
- il **cambiamento climatico**: strettamente correlato all'inquinamento, ancora crescente come trend, ha forti impatti sulla salute e sugli eco-sistemi a livello mondiale;
- la **biforcazione demografica**: mentre alcune società sono "super invecchiate", con più del 20% della popolazione sopra i 65 anni, altre sono largamente "giovanili", con alte percentuali di persone sotto i 18 anni.

World Economic Forum ha anche pubblicato, a gennaio 2025, il documento "*Global Cybersecurity Outlook 2025",* che evidenzia **la forte crescita della complessità della sicurezza digitale**, causata dai principali elementi evidenziati nella fig. 3.1-4.

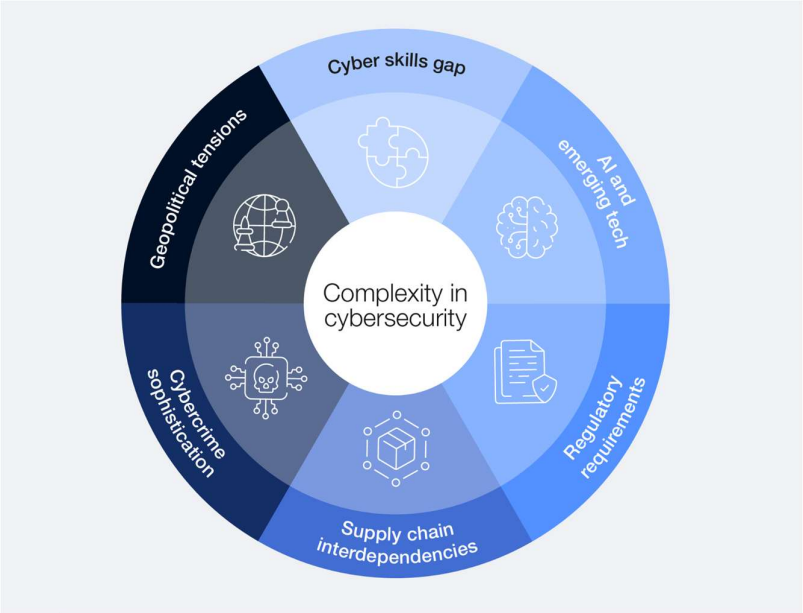


Fig. 3.1-4 (Fonte: WEF Global Cybersecurity Outlook 2025)

La figura considera, oltre alle tensioni geopolitiche e alle nuove tecnologie, in primis l'AI, già discusse nel paragrafo precedente, i seguenti aspetti:

- il cyber skill gap;
- la sofisticazione del cybercrime e dei relativi attacchi;
- l'interdipendenza della supply chain informatica ed i relativi attacchi;
- le varie richieste delle norme sulla sicurezza digitale a livello nazionale ed internazionale.

La **resilienza digitale** è l'obiettivo primario per ogni organizzazione, ed il rapporto evidenzia come le piccole organizzazioni hanno crescenti difficoltà a realizzarla, mentre le grandi sono vicine ad ottenere un adeguato livello, se non l'hanno già raggiunto, di effettiva resilienza anche grazie all'obbligo di adeguarsi alle varie norme sulla sicurezza digitale (per l'Europa NIS2, CER, DORA, etc., si veda fig. 3.2-1)
I tipi principali tipi di attacchi a livello mondiale evidenziati nel rapporto vedono al primo posto, come diffusione, i **ransomware**, anche per la crescente disponibilità di Ransomware as a Service (RaaS), ed è interessante considerare le differenti opinioni tra CEO e CISO sulla gravità dell'impatto, anche da un punto di vista organizzativo, dei principali rischi digitali, mostrati nella fig. 3.1-5. Le maggiori differenze tra il CEO ed il CISO riguardano soprattutto le frodi cyber e la disinformazione, ed il ransomware preoccupa molto di più il CISO.

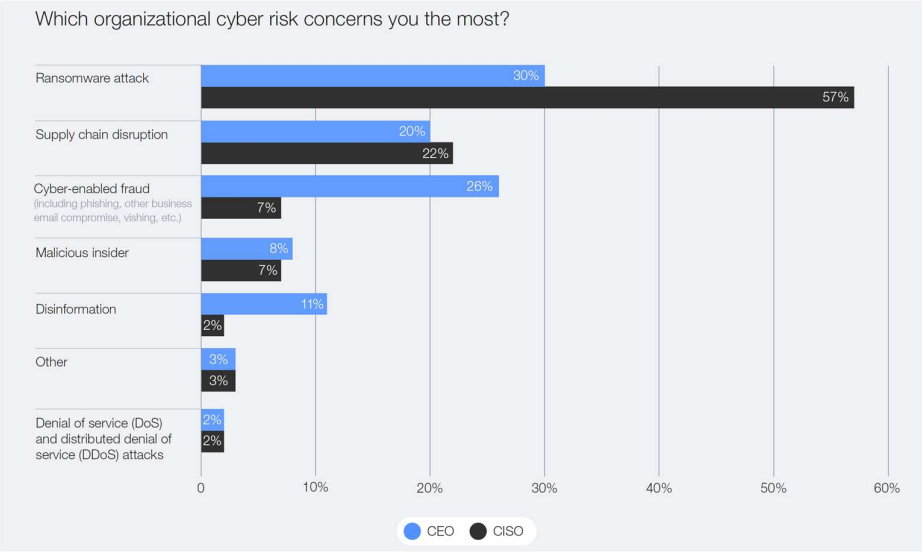


Fig. 3.1-5 (Fonte: WEF Global Cybersecurity Outlook 2025)

Un'importante analisi del rapporto WEF sulla cybersecurity riguarda l'AI. **Gli strumenti di GenAI[8] stanno rimodellando il panorama della criminalità informatica**, consentendo ai criminali di perfezionare i propri metodi e automatizzare e personalizzare le proprie tecniche di attacco, sempre più sofisticate e, soprattutto, efficaci. Come evidenziato in fig. 3.1-6, il 47% delle organizzazioni indica come principale preoccupazione per la GenAI il **progresso delle capacità avversarie**, ossia dei criminali informatici che sfruttano l'efficienza dell'AI per automatizzare e personalizzare le comunicazioni ingannevoli.
Data l'attuale importanza dell'AI sia come strumento di difesa che di attacco in ambito sicurezza digitale, il questionario online OAD 2025 ha voluto approfondire sugli attacchi ai sistemi di AI, basandosi sulle "top ten" vulnerabilità individuate da OWASP: il paragrafo di analisi è §4.4.

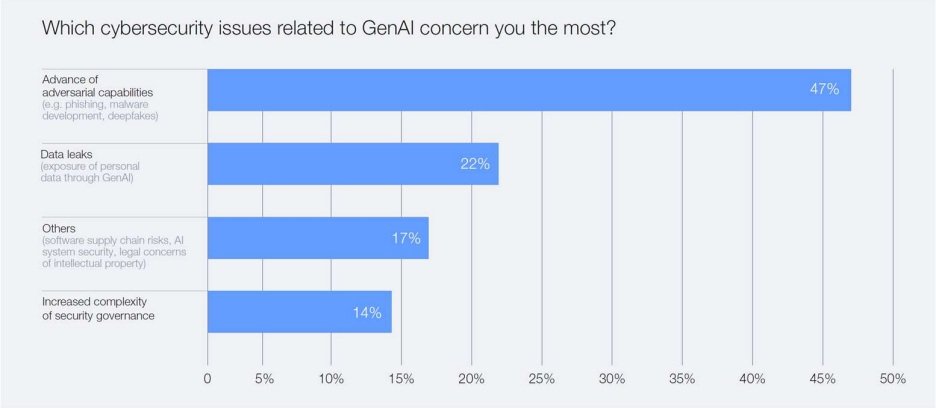


Fig. 3.1-6 (Fonte: WEF Global Cybersecurity Outlook 2025)

[8] **GenAI** è l'AI generativa: una branca dell'intelligenza artificiale che si concentra sulla creazione di nuovi contenuti originali, come testo, immagini, musica, audio e video. Questi sistemi utilizzano modelli di base, addestrati su grandi quantità di dati, per apprendere schemi e strutture complesse, e poi generare nuovi contenuti simili a quelli con cui sono stati addestrati.

Cybercrime e cyber warfare sono sovente correlati ed è difficile individuare e classificare un attacco digitale come una azione di cyber warfare, rispetto ad un "normale" attacco, oppure all'azione di un terrorista o di un attivista (hacktivist). Chi attacca il più delle volte cerca di mascherare il suo attacco, affiancandolo spesso con varie "fake news" fuorvianti. Un attacco digitale potrebbe far parte di una cyber warfare quando ha un certo livello di sofisticazione, che richiede competenze e risorse che un "normale" hacker difficilmente potrebbe avere, ed è ben chiaro l'obiettivo target dell'attacco ed il momento ed il contesto in cui l'attacco viene portato. La diffusione mondiale di Internet da un lato e le guerre ed i crimini digitali dall'altro hanno creato lo **spazio "cyber"**, che si affianca a quelli di terra, mare, cielo e spazio, e che costituisce una ulteriore area strategica e geopolitica, nella quale si confrontano e si contendono non solo nazioni ma anche vari gruppi di terroristi, di attivisti, di aziende.

3.1.1 I principali attacchi digitali a livello mondiale nel 2024

L'elenco è solo un esempio dei più importanti attacchi digitali di cui si ha conoscenza, e l'elenco non è certo esaustivo.

Gennaio 2024

- Sofisticato attacco alla piattaforma di cripto valute Orbit Chain (in particolare Ether, Dai, Tether, e USD Coin), probabilmente effettuato da un gruppo sponsorizzato dalla Korea del Nord: gravissima la perdita istantanea di 86 Milioni di US $, quasi 3/4 dell'intero bilancio.
- Attacco ransomware a Schneider Electric, con una una violazione dei dati di 1,5 TB
- Attacco ransomware LoanDepot, un importante istituto di credito ipotecario, che ha provocato il furto di informazioni di 16,5 milioni di clienti ed il blocco dei servizi.
- Attacco alle reti energetiche di Germania, Polonia e Austria: il malware ShadowGrid ha paralizzato le reti di distribuzione di energia elettrica di questi paesi, lasciando senza corrente per giorni e mettendo a rischio infrastrutture critiche, come ospedali e trasporti. L'attacco, probabilmente commissionato dalla Russia, ha causato danni per miliardi di €.

Febbraio 2024

- Attacco a Change Healthcare, uno dei principali elaboratori di richieste di risarcimento medico negli Stati Uniti, da parte del gruppo ransomware ALPHV/BlackCat, che ha causato notevoli interruzioni nei servizi sanitari a livello nazionale, con l'interruzione dei pagamenti elettronici e dell'elaborazione delle richieste di rimborso delle spese mediche, coinvolgendo oltre 100 milioni di utenti. Questo è considerato uno dei più gravi attacchi digitale del 2024, sia per i danni diretti ed indiretti per i disservizi, ma anche per il pagamento di 22 milioni di US $ di riscatto.

Marzo 2024

- Vulnerabilità Zero-Day nei prodotti di Ivanti che sono state sfruttate per attacchi massivi. L'azienda fin dai primi del 2024 aveva confermato l'esistenza di due vulnerabilità zero-day nei suoi prodotti Connect Secure e Policy Secure gateways, identificate come CVE-2023-46805, un "authentication bypass", e come CVE-2024-21887, un "command injection flaw". Queste vulnerabilità sono state sfruttate dal gruppo cinese UNC5221 fin da gennaio 2024 per distribuire malware personalizzati, tra cui web shell e raccoglitori di credenziali, a livello mondiale. Nonostante il rilascio di patch e nuove release da parte Ivanti, vari gruppi di crackers hanno ampliato gli attacchi massivi, che hanno portato alla compromissione di oltre 1.700 dispositivi VPN ICS tramite la web shell GIFTEDVISITOR. Lo sfruttamento si è intensificato con la scoperta di ulteriori vulnerabilità sui prodotti Ivanti, come CVE-2024-21893, una falla di falsificazione delle richieste lato server, e CVE-2024-21888, un problema di escalation dei privilegi. La Cybersecurity and Infrastructure Security Agency (CISA) statunitensi ordinò

alle agenzie federali di disconnettere le appliance Ivanti interessate fino alla loro completa messa in sicurezza.
- Violazione e furto di dati alla Cisco, confermati dall'azienda.
- Un bug del kernel di Windows (CVE-2024-21338) è stato sfruttato come zero-day per attacchi massivi ai sistemi Windows.

Aprile 2024

- Attacco ransomware a Hoya Corporation, multinazionale tecnologica e medicale giapponese leader mondiale in lenti ottiche e a contatto, lenti intraoculari, endoscopi, componenti per dispositivi a semiconduttore e schermi. L'attacco ha bloccato la gestione ordini e la produzioni e gli attaccanti, Hunters International ransomware, hanno richiesto un riscatto di 10 milioni di US $.

Maggio 2024

- Attacco a Snowflake, che gestisce una piattaforma cloud, con esfiltrazione di dati di centinai di clienti, tra i quali AT&T, Ticketmaster, e Santander Bank. Un gruppo di cracker associati al gruppo Scattered Spider hanno sfruttato le credenziali compromesse di un account di un dipendente di Snowflake. Gli attaccanti hanno chiesto un riscatto tra i 300.000 e i 5 milioni di US $ alle principali società cui hanno rubato i dati
- Attacco al Ministero della Difesa del Regno Unito con una grave violazione dei dati di circa 270.000 attuali ed ex militari britannici tramite la compromissione di un sistema di elaborazione delle buste paga gestito da un appaltatore. Questo sistema conteneva informazioni personali, tra cui nomi, coordinate bancarie e, in alcuni casi, indirizzi di residenza. Non si hanno informazioni ufficiali, ma si ritiene che l'attacco sia stato effettuato dalla Cina.
- Attacco ransomware paralizzante ad Ascension, il principale sistema sanitario statunitense ha subito un attacco nel maggio 2024. L'attacco ha reso inaccessibile il sistema di cartelle cliniche elettroniche (EHR) MyChart. Questo ha causato il blocco di vari servizi informatici, costringendo gli operatori sanitari a fare affidamento sulla documentazione manuale, ritardando e interrompendo gravemente l'assistenza ai pazienti critici.
- Attacco all'australiana MediSecure, importante fornitore di servizi di prescrizione elettronica, con il furto di informazioni personali e sanitarie di circa 12,9 milioni di persone. I dati compromessi includevano nomi, date di nascita, indirizzi, numeri di telefono, numeri Medicare, dettagli delle prescrizioni e motivazioni per l'assunzione dei farmaci. Questa violazione è una delle più grandi e più gravi nella storia australiana.

Giugno 2024

- Attacco ransomware (MedCrypt) al Servizio Sanitario Nazionale del Regno Unito (NHS), che ha criptato i dati di milioni di pazienti, bloccando i sistemi di prenotazione e ritardando interventi chirurgici critici. E' stato richiesto un riscatto di 20 Milioni in Bitcoin, rifiutato dal governo UK.
- Attacco ransomware a Synnovis, il fornitore di servizi di patologia del Servizio Sanitario Nazionale del Regno Unito (NHS da parte della Qilin Ransomware Gang. Grave impatto sui servizi sanitatari: trasfusioni di sangue, risultati di test, operazioni relative a trattamenti contro il cancro e persino parti cesarei hanno dovuto essere riprogrammati. Oltre 1.100 procedure elettive e più di 2.000 visite ambulatoriali nei principali ospedali di Londra sono state rinviate. Gli aggressori di lingua russa hanno rubato e divulgato 400 GB di dati sensibili e hanno tentato di estorcere denaro a Synnovis, presumibilmente con un riscatto di 50 milioni di dollari

Luglio 2024

- Evento interruzione CrowdStrike-Microsoft (più probabilmente un errore involontario che un attacco intenzionale): un aggiornamento difettoso del software Falcon Sensor di CrowdStrike ha causato

disagi diffusi per gli utenti Microsoft Windows a livello globale. Circa 8,5 milioni di sistemi sono andati in crash in tutto il mondo, con l'apparizione dalla "schermata blu di errore": questo evento ha avuto un impatto grave su vari settori critici, tra cui aviazione, banche, ospedali, grande distribuzione, emittenti televisive, produzione.

- Attacco alla piattaforma di cripto valute indiana WazirX da parte del gruppo Lazarus per la Corea del Nord, che ha causato il furto di 235 milioni di US $.

Agosto 2024

- Attacco a **Binance**, una delle principali piattaforme di scambio di criptovalute, sfruttando vulnerabilità nei protocolli di autenticazione. Sono stati rubati oltre 600 milioni di dollari in criptovalute, che l'azienda ha dovuto rimborsare, e l'attacco ha inoltre causato panico tra gli investitori e una perdita di valore di numerose criptovalute.

Settembre 2024

- Inizio della campagna di cyber-spionaggio da parte della cinese Salt Typhoo, che ha preso di mira diversi fornitori di telecomunicazioni statunitensi, inclusi AT&T, Verizon, T-Mobile, e Lumen Technologies, e che ha visto a dicembre 2024 il suo apice. Questi attacchi hanno consentito a di accedere a dati sensibili, come metadati di chiamate e messaggi di testo, informazioni di geolocalizzazione e, in alcuni casi, registrazioni audio di conversazioni telefoniche. Tra i soggetti interessati figurano, in particolare, personaggi di alto profilo, tra cui figure politiche come Donald Trump e J.D. Vance.
- Sofisticato attacco all'azienda dei trasporti londinese, Transport for London (TfL), che ha causato una grave interruzione dei servizi, e soprattutto ha riguardato i passeggeri diversamente abili che si affidavano al servizio Dial-A-Ride di TfL. L'attacco avrebbe compromesso i dati personali di circa 5.000 clienti, inclusi indirizzi di residenza e dati bancari. ciò ha causato significative interruzioni operative e perdite finanziarie per circa 30 milioni di sterline.

Ottobre 2024

- Attacco malware al sistema di trasporti di Tokyo che ha colpito i sistemi di bigliettazione e di gestione dei treni, causando una paralisi di più di tre giorni.

Novembre 2024

- Attacco ransomware a Blue Yonder Group, Inc. , società americana che fornisce soluzioni/servizi per la gestione delle supply chain , e che opera come filiale indipendente della holding Panasonic Corporation. L'attacco ransomware compiuto dal gruppo Termite Ransomware, ha causato il furto di 680 gigabyte di dati da Blue Yonder, tra cui database, indirizzi e-mail e oltre 200.000 documenti assicurativi.

Dicembre 2024

- Attacco ransomware (Black Basta) al Gruppo BT, British Telecom, che ha causato il furto di 500 GB di dati, inclusi quelli finanziari, organizzativi, NDA, documenti personali e confidenziali, oltre alla la messa offline di numerosi server, in particolare quelli della divisione BT Conferencing.
- Nuovo attacco alla Cisco, in particolare all'ambiente per sviluppatori DevHub[9], da parte del gruppo IntelBroker, con il furto di 4.5 Tb di dati.

[9] Centro risorse Cisco per sviluppatori che fornisce strumenti, codice e documentazione per la creazione e l'integrazione di applicazioni con le tecnologie Cisco.

3.2 Il quadro a livello Unione Europea

Quanto indicato nel precedente paragrafo per la sicurezza digitale, si riflette 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 "The report on the state of cybersecurity in the Union"**,** di dicembre 2024, '"ENISA Threat Landscape (ETL) 2024", "Foresight Cybersecurity Threats for 2030 – UPDATE", aggiornato e pubblicato a marzo 2024, "ENISA NIS360 2024", analisi per settore della maturità e delle criticità nell'adozione della normativa NIS2 pubblicato a febbraio 2025, "ENISA Threat Landscape: Finance Sector", pubblicato a febbraio 2025, "Space Threat Landscape", pubblicato a marzo 2025.

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 numerose normative emanate dall'UE; le principali normative europee sono elencate nella fig. 3.2-1.

Normativa	Riferimento UE	Obiettivi norma	Link alla normativa
GDPR, General Data Protection Regulation)	2016/2019	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
DMA, Digital Markets Act	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
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
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
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

Fig. 3.2-1

ENISA fornisce la situazione sugli attacchi digitali rilevati nei paesi EU nei Rapporti ETL 2024 e 2025. Occorre considerare entrambi i rapporti ETL in quanto il primo fa riferimento al periodo luglio 2023 – giugno 2024, il secondo da luglio 2024 a giugno 2025: l'intero anno 2024 è a cavallo tra i due rapporti.
Le segnalazioni degli attacchi considerati nei rapporti ETL di ENISA provengono da segnalazioni dirette ad ENISA e dalle segnalazione fornite alle varie Agenzie per la cybersecurity nazionali, per l'Italia da ACN. Sono quindi segnalazioni di attacchi gravi, fornite da chi li subisce in accordo con le varie normative UE e nazionali, in primis NIS/NIS 2.

La fig. 3.2-2a e 3.2-2b mostrano la tipologia di attacchi rilevati nei paesi dell'UE rispettivamente dai due rapporti ENISA ETL 2024 e 2025.

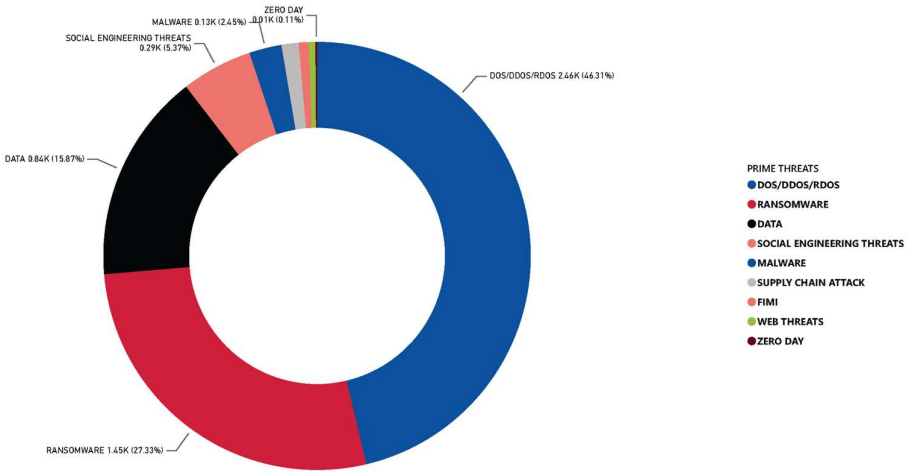


Fig. 3.2-2a (Fonte: ENISA ETL 2024)

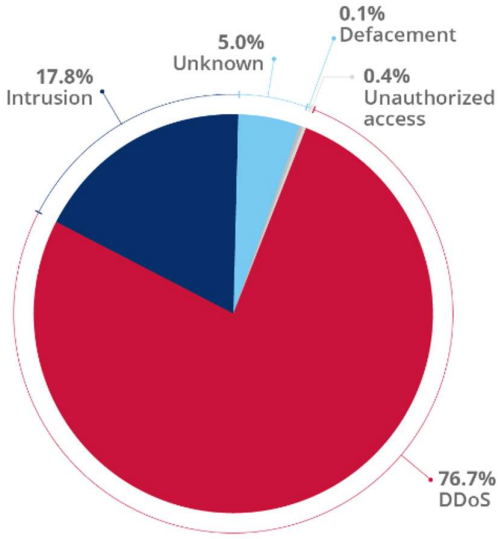


Fig. 3.2-2b (Fonte: ENISA ETL 2025)

L'ultimo rapporto ETL 2025 ha, sugli attacchi digitali, analisi e grafici diversi rispetto all'edizione precedente, come è anche immediatamente visibile dalle due figure a e b sopra riportate.
Entrambe le figure mostrano che **gli attacchi Dos/DDoS** sono stati i più diffusi attacchi digitali e rimangono la principale minaccia per i paesi dell'UE, seguiti dai **ransomware**. Tra i rischi di questo tipo ENISA include i **RDoS,** Ransom Denial of Service, dove gli attaccanti ricattano minacciando un attacco DoS/DDoS.
Gli attacchi DDoS sono effettuati prevalentemente da gruppi di hacktivisti e da gruppi legati a stati (che ENISA definisce "State-nexus actors"[10]). I gruppi di sola criminalità informatica contribuiscono in misura marginale ai DDoS, e quasi sempre con obiettivi all'estorsione, tipicamente DDoS con richiesta di riscatto.

[10] ENISA utilizza le seguenti tipologie di attaccanti:

- **State-nexus actors**: dipendono direttamente o indirettamente da strutture governativi e/o militari, dispongono di grandi risorse sia economiche, che tecniche e di personali, e sono i principali attori operanti nelle guerre digitali.

Nella fig. 3.2-2b gli attacchi indicati come "intrusion" includono attività dei criminali informatici, seguite da gruppi di intrusione allineati allo stato, che in genere perseguono la persistenza. Gli hacktivisti compaiono solo marginalmente nei casi di intrusione.
I **defacement**, tipicamente la deturpazione della home page di un sito web, sono stati quasi esclusivamente associati agli hacktivisti, sottolineando il loro ruolo di tattica simbolica per ottenere visibilità e protesta, piuttosto che di metodo di intrusione continua.

Le principali vulnerabilità/rischi sfruttate per gli attacchi rilevati da ENISA sono rappresentate nella fig. 3.2-3. Il grafico mostra che i **dispositivi mobili** sono ancora la superficie di attacco primaria, perché spesso non protetti o con protezioni troppo leggere, ad esempio il pin per accedervi. Seguono le **minacce web**, dato il persistente, se non crescente, utilizzo di servizi e applicazioni online. Il mondo **OT,** Operational Technology, è la terza area di vulnerabilità/rischi sfruttati, e riflette la crescente esposizione dei sistemi OT che sono sempre più connessi con il sistema informativo (integrazione IT/OT, si veda anche §4.3 e §7.3) e sovente, non avendo le idonee misure di sicurezza, rappresentano un punto di ingresso per gli attacchi al sistema informativo cui sono collegati. **La supply chain è** diventata, a sua volta, negli ultimi anni un punto di ingresso per gli attacchi al sistema informativo oggetto dell'attacco, sfruttando percorsi indiretti attraverso fornitori, clienti e dipendenze che non hanno sufficienti livelli di sicurezza digitale.

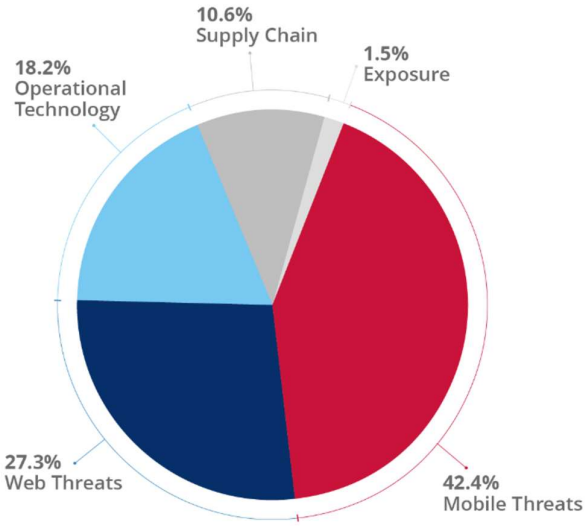


Fig. 3.2-3 (Fonte: ENISA ETL 2025)

- **Cybercriminali** e **hacker-for-hire:** sono gruppi di criminali o singole persone che effettuano attacchi digitali per illeciti guadagni, che provengono principalmente dalle vendita di risorse ICT rubate, in primis da informazioni, e da ricatti ad aziende/enti a seguito di attacchi DDoS e di malware; nell'ambito di questo gruppo ENISA individua gli hacker a noleggio, che effettuano, dietro pagamento, attacchi digitali per conto terzi.
- **PSOA, Private Sector Offensive Actors:** sono organizzazioni private o singole persone con alte competenze nella sicurezza digitale in grado di individuare vulnerabilità "zero day" e/o realizzare strumenti di attacco digitale e di venderli; non sono cybercriminali, in quanto le loro attività non sono illegali, ma sovente forniscono i loro strumenti ai cybercriminali e agli hacktivisti.
- **Hacktivisti:** sono singole persone o gruppi animati da forti motivazioni, ed utilizzano l'hacking per farsi conoscere e perorare qualche causa, con l'obiettivo di provocare qualche forma di cambiamento politico o sociale. Gli hacktivisti sono talvolta sfruttati anche da attori con legami con Stati per operazioni di influenza o altre forme di campagne di intrusione.

La fig. 3.2-4b, da ENISA ETL 2025, mostra la ripartizione percentuale delle **motivazioni**[11] per gli attacchi rilevati, ed evidenzia come la motivazione **ideologica** sia predominante, rispetto alla motivazione **finanziaria** che, soprattutto in Italia, è stata sempre considerata come la principale, se non l'esclusiva, molla degli attacchi digitali: un **79,4%** contro un **13,4%.**
Nel precedente rapporto ENISA RTL 2024 l'**ideologia** era la motivazione principale ma "solo" (rispetto al 79,4%) nel **43%** degli attacchi considerati, e quella **finanziaria** raggiungeva il **40%,** come mostrato nella fig. 3.2-4a.

Risulta quindi significativo, e preoccupante, come l'aspetto ideologico influisca sempre più sugli attacchi digitali ai paesi dell'UE a causa non solo delle crescenti tensioni geopolitiche, e delle conseguenti guerre digitali, ma anche della sempre più grave mala informazione/disinformazione ed ignoranza delle persone dell'UE, soprattutto giovani, nei riguardi dei vari temi direttamente o indirettamente impattanti sulla geopolitica.

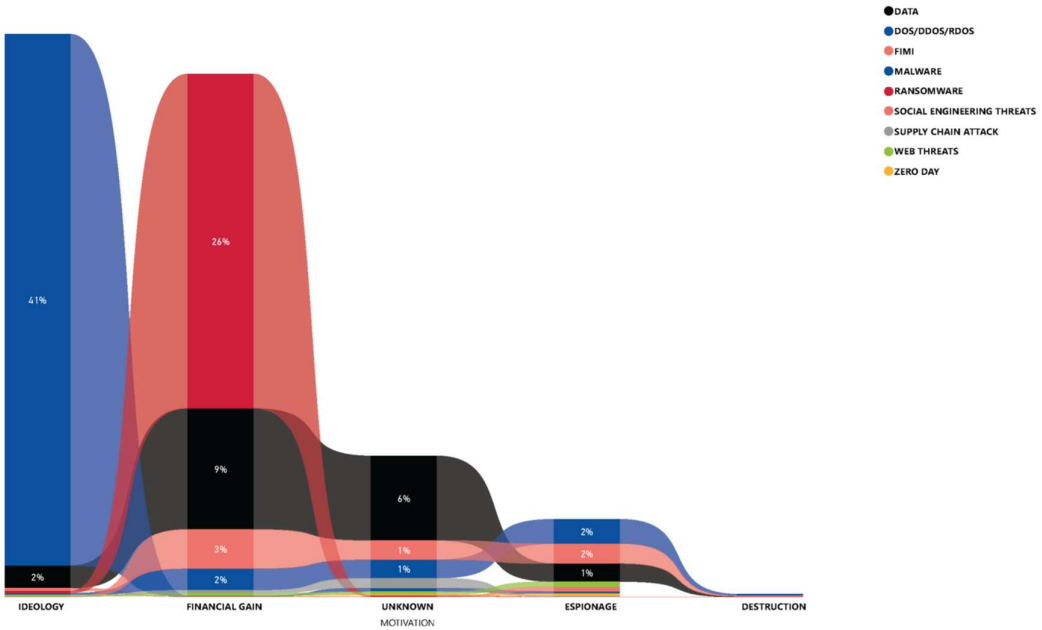


Fig. 3.2-4a (Fonte: ENISA ETL 2024)

[11] ENISA fa riferimento alle seguenti principali motivazioni per gli attacchi e gli attaccanti:

- **Guadagno finanziario**: qualsiasi azione finanziariamente rilevante (condotta principalmente da gruppi di criminalità informatica);
- **Spionaggio**: acquisizione di informazioni su proprietà intellettuale, dati sensibili, dati classificati (condotta principalmente da gruppi sponsorizzati da Stati);
- **Distruzione**: qualsiasi azione distruttiva per ambienti ICT che potrebbe avere conseguenze irreversibili;
- **Ideologico**: qualsiasi azione supportata da un'ideologia (come l'hacktivismo).

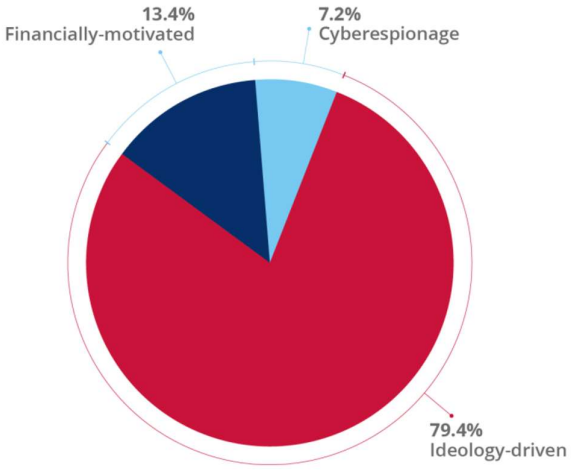


Fig. 3.2-4b (Fonte: ENISA ETL 2025)

I principali **gruppi di attaccanti** che hanno attuato nel 2024 gli attacchi rilevati da ENISA, e che in gran parte tutt'ora operano in ambito europeo**,** sono riportati nella fig. 3.2-5.
Al primo posto percentualmente un "**unknown**", con un **34%** . Per più di 1/3 degli attacchi digitali rilevati da ENISA, il gruppo di attacco e le modalità dell'attacco sono ignote. Il primo e più attivo gruppo di attaccanti riconosciuto, con un **30,46%** è **NoName057(16)**, un gruppo filorusso attivo da marzo 2022, l'anno dell'invasione dell'Ucraina. Ha rivendicato su Telegram la responsabilità di migliaia di attacchi cibernetici contro agenzie governative, media e aziende private dell'Ucraina e di paesi che stanno aiutando l'Ucraina contro l'invasione russa. Effettua prevalentemente attacchi DDoS, ed ha creato lo strumento DDoSIA per realizzare attacchi DDoS, messo a disposizione, inizialmente su GitHub[12], a chi voglia effettuare questo tipo di attacchi sugli obiettivi informatici, il target, indicati dal gruppo stesso, e con ricompensa in criptovalute. NoName057(16) è stato oggetto di una indagine, chiamata Eastwood[13], della Polizia Postale italiana con Europol che ha portato a denunce e alla chiusura di centinaia di server che costituivano l'infrastruttura ICT per gli attacchi DDoS.
Al terzo posto, con **5,43%**, **C10p**, un gruppo cyber-criminale filo e di lingua russa, noto per gli attacchi basati su malware e su "multilevel extortion" con i ransomware (ricatta più volte l'attaccato, prima per eliminare il ransomware e far funzionare il sistema infetto, poi per non vendere i dati estratti illegalmente, e così via). Al quarto posto, con **5,1%**, il gruppo **LockBit**, cyber-criminali russi specializzati negli attacchi ransomware, non totalmente eliminato dalla operazione Cronos[14] delle forze di polizia internazionali.

[12] GitHub è un servizio di hosting per progetti software, di proprietà della società GitHub Inc., controllata da Microsoft.
[13] https://www.commissariatodips.it/notizie/articolo/operazione-eastwood-nei-confronti-del-gruppo-hacker-filorusso-noname/
[14] L'Operazione Cronos è stata una grande operazione internazionale del febbraio 2024, guidata dalla National Crime Agency (NCA) del Regno Unito con il coordinamento di Europol, che ha permesso di smantellare l'infrastruttura del gruppo ransomware LockBit.

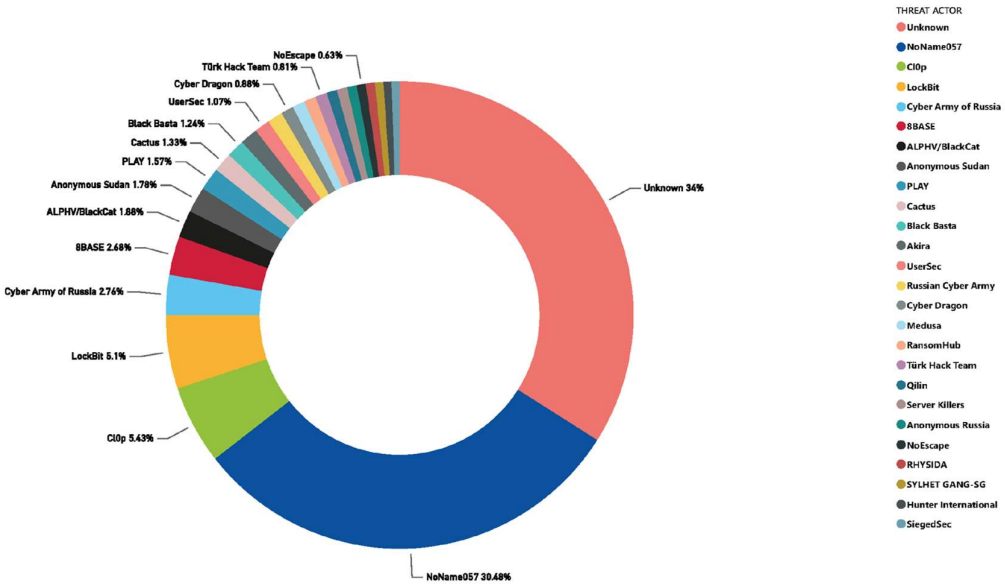


Fig. 3.2-5 (Fonte: ENISA ETL 2024)

ENISA ETL 2025 sottolinea che, nel corso degli ultimi anni:

- i **confini** tra hacktivismo, criminalità informatica e attività legate allo Stato sono sempre più sfumati;
- gli strumenti degli hacktivisti e gli ecosistemi criminali si intersecano sempre di più. L'emergere di FunkSec alla fine del 2024 ha portato con sé il ransomware FunkLocker, che fonde messaggi politici con estorsioni finanziarie, sottolineando quanto rapidamente un branding ideologico possa trasformarsi in monetizzazione.

Dai dati dei rapporti ETL 2024 e 2025 emergono in estrema sintesi i seguenti elementi.

- **Ransomware al centro** delle attività criminali, con operazioni sempre più decentralizzate e aggressive, favorite da modelli **as-a-service** e dalla professionalizzazione dell'ecosistema criminale.
- I **gruppi sponsorizzati da stati** intensificano il cyberspionaggio verso settori strategici dell'UE (telecomunicazioni, logistica, manifattura), usando tecniche sofisticate (compromissione supply chain, malware furtivi[15], driver firmati[16]).
- **Hacktivismo in crescita**, rappresentando l'80% degli incidenti, prevalentemente tramite attacchi DDoS a basso impatto ma ideologicamente motivati.
- Aumentata **esposizione sistemica dell'UE**, con pubbliche amministrazioni (38%) e trasporti (soprattutto marittimo e logistico) come target primari di ransomware e cyberspionaggio.

[15] I malware furtivi (o stealth malware) sono software dannosi progettati per operare senza essere rilevati dagli utenti o dai sistemi di sicurezza, come gli antivirus, per rubare dati, spiare attività, accedere a sistemi o estorcere denaro. La loro caratteristica principale è la capacità di nascondersi.

[16] I driver firmati sono file software di dispositivo, come quelli per una stampante o una scheda grafica, che sono stati verificati da un'entità di terze parti fidata tramite una firma digitale. Questa firma garantisce che il driver provenga da un editore legittimo, che non sia stato manomesso e che sia compatibile con il sistema operativo, fornendo un livello di sicurezza che impedisce l'installazione di software dannoso o potenzialmente dannoso. Anche se firmati, alcuni driver sono vulnerabili e consentono agli attaccanti di disabilitare o aggirare le soluzioni di sicurezza, con conseguente compromissione del sistema ICT che utilizzi tali driver. Alcuni attacchi, tipicamente via malware, hanno sfruttato anche driver firmati non vulnerabili.

- **Phishing** rimane il principale vettore d'intrusione (60%), evoluto grazie a piattaforme phishing-as-a-service, accessibili anche ad attori non specializzati.
- **Abuso di dipendenze digitali** in crescita: repository open source, estensioni browser e fornitori di servizi sotto attacco, aumentando il rischio sistemico.
- **Sfruttamento rapido delle vulnerabilità** (21,3% degli accessi iniziali), che evidenzia l'urgenza di una gestione tempestiva delle patch e di un'adeguata igiene informatica.
- **AI come fattore abilitante**: oltre l'80% del phishing globale è ora supportato da tecniche AI (modelli jailbroken[17], media sintetici[18], avvelenamento modelli[19]), aumentando precisione e impatto delle campagne.
- Il panorama evolve verso **campagne convergenti, continue e diversificate**, meno incidenti isolati ma più pressione sistemica e persistente, che mina la resilienza complessiva.

Nel Rapporto ENISA "Foresight Cybersecurity Threats for 2030 – UPDATE" sono elencati i 10 principali rischi più provabili entro il 2030, ripresi nella fig. 3.2-6 in ordine della loro probabilità di occorrenza e della gravità del loro impatto. Rischi che ritroviamo come base degli attcchi rilevati da ENISA e analizzati nelle precedenti pagine.

1. **Compromissione della Supply Chain informatizzata**
2. **Carenza di competenze**
3. **Errore umano e sistemi legacy sfruttati all'interno di ecosistemi cyber-fisici**
4. **Sfruttamento di sistemi non patchati e obsoleti all'interno dell'ecosistema tecnologico attaccato**
5. **Aumento dell'autoritarismo nella sorveglianza digitale / perdita della privacy**
6. **Fornitori di servizi ICT transfrontalieri come singolo punto di errore**
7. **Campagne avanzate di disinformazione / operazioni di influenza**
8. **Aumento di minacce ibride avanzate**
9. **Abuso di Intelligenza Artificiale**
10. **Impatto fisico di effetti/disastri naturali/ambientali su infrastrutture digitali critiche**

Fig. 3.2-6 (Fonte: ENISA Foresight Cybersecurity Threats for 2030 – UPDATE)

Al primo posto i rischi di attacchi alla supply chain informatica, ed al secondo la carenza di competenze, tema assai gravi soprattutto in Italia, come approfondito in §3.4.2; da questo deriva anche, ma non solo, il rischio di errore umano che si posiziona al terzo posto, e che si aggrava in ambiti OT, come descritto in §4.3, dove la security si intreccia con la safety, soprattutto quando i sistemi OT hanno bisogno di intervento umano (sistemi cyber-fisici). Anche questo tema è stato trattato dall'indagine OAD 2025, si veda &4.3 e §7.3. Al quarto posto il problema dei sistemi ICT non aggiornati e obsoleti, che possono così mantenere vecchie ma gravi vulnerabilità facilmente individuabili e sfruttabili dagli attaccanti. Sebbene alcune minacce come "Compromissione delle dipendenze software nella supply chain" e "Campagne avanzate di disinformazione/operazioni di influenza" abbiano registrato un leggero calo della loro rilevanza percepita fino al 2030, continuano a rappresentare rischi significativi. "Ascesa dell'autoritarismo nella sorveglianza digitale/Perdita della privacy" mostra un leggero calo di impatto e probabilità. D'altro canto, le prospettive a lungo termine di minacce come "Carenza di competenze" e "Fornitori di servizi ICT transfrontalieri come singolo punto di errore" si sono in qualche modo intensificate nella percezione degli esperti. "Abuso dell'IA" e "Attacchi informatici che interrompono/amplificano l'IA" hanno acquisito maggiore probabilità, il che non sorprende, data l'ampia copertura delle applicazioni di IA emergenti su larga scala e le considerazioni sull'uso

[17] Un'AI "jailbroken" è un'intelligenza artificiale in cui sono state aggirate le restrizioni di sicurezza imposte dagli sviluppatori, solitamente attraverso l'uso di specifici "prompt" o comandi ingannevoli, per farla agire in modi che normalmente non le sarebbero permessi, ad esempio generando contenuti inappropriati o aggirando le sue linee guida etiche.

[18] I media sintetici sono qualsiasi tipo di video, immagini, oggetti virtuali, suoni o parole prodotti dall'intelligenza artificiale (o con l'aiuto di essa).

[19] In ambito AI, l'avvelenamento dei dati, chiamato in inglese "data poisoning", si verifica quando dati di addestramento compromessi deviano il comportamento dell'AI.

etico dei modelli di IA appena rilasciati, nonché di quelli emergenti. L'argomento è stato trattato nell'indagine OAD 2025, si veda §4.4.

3.2.1 Gli attacchi digitali in ambito finanziario nell'Unione Europea

ENISA ha pubblicato il rapporto "ENISA Threat Landscape: Finance Sector" verticale sul settore finanziario. Questo Rapporto considera gli attacchi digitali più significativi occorsi in questo settore nell'UE tra gennaio 2023 e giugno 2024.
La fig. 3.2.1-1 mostra le principali minacce digitali rilevate nel settore finanziario europeo da gennaio 2023 a giugno 2024.

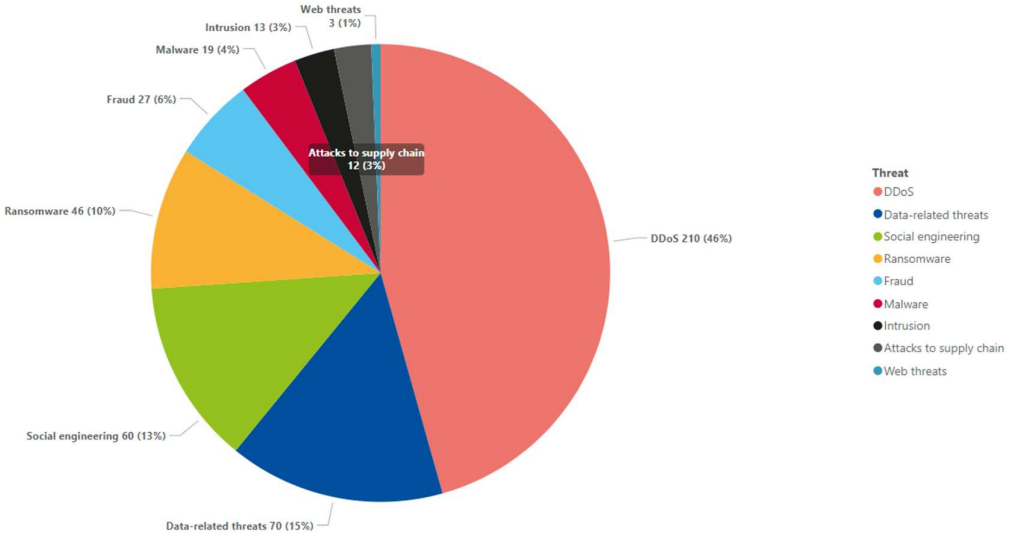


Fig. 3.2.1-1

I principali risultati emersi da questa indagine sono riportati nei seguenti punti.

- Le **banche europee** sono state le più frequentemente prese di mira, con una percentuale del **46%**. Seguono le agenzie governative e le **organizzazioni del settore pubblico nel settore finanziario** (**13%**). I **singoli individui** (**10%**) sono stati attirati e truffati da campagne di social engineering con un tema rilevante per la finanza.
- Il settore finanziario ha registrato **picchi di attività DDoS** legati a eventi geopolitici, in particolare all'invasione russa dell'Ucraina. Gli hacktivisti hanno spesso preso di mira **istituti di credito europei** (**58%** degli attacchi) e **siti web governativi relativi alla finanza** (**21%**), causando interruzioni operative e sollevando preoccupazioni in materia di sicurezza informatica.
- Gli **istituti finanziari** hanno spesso subito perdite significative a causa di attacchi digitali quali frodi, ransomware e violazioni dei dati. Queste perdite sono state aggravate dai costi associati alle azioni di ripristino, spese legali e sanzioni normative.
    - **Violazioni e fughe di dati** sono problematiche critiche per gli istituti di credito europei (**39%**), che sono stati i principali obiettivi nell'ambito finanziario, con danni anche alla reputazione.
    - Le **campagne di ingegneria sociale** (social engineering), tra cui phishing, smishing e vishing, sono state le tattiche prevalenti utilizzate dagli attaccanti. Questi incidenti miravano a rubare

informazioni sensibili e commettere frodi finanziarie, colpendo **privati (38%)** e **istituti di credito (36%).**

- Le **frodi** hanno rappresentato il **6%** degli attacchi complessivi, colpendo principalmente **privati (40%)** e **istituti di credito (35%)**. Sebbene i casi segnalati sembrino bassi, la sottostima e le conseguenze secondarie di altri attacchi informatici suggeriscono un problema più ampio. La criminalità informatica legata alle criptovalute ha visto un aumento di furti, truffe e riciclaggio illecito.
- Gli attacchi **ransomware** hanno preso di mira principalmente entità finanziarie meno mature, come **fornitori di servizi (29%)** e **compagnie assicurative (17%)**, con conseguenze che includono perdite finanziarie (38%), esposizione dei dati (35%) e interruzione delle attività operative (20%).

- Il **malware**, pur avendo in figura una percentuale bassa, prende di mira un gran numero di individui, principalmente i clienti degli istituti di credito. Esempi di tali trojan bancari includono:
  - Anatsa, usato in campagne rivolte alla Repubblica Ceca;
  - Mispadu rivolto a utenti in Italia, Polonia e Svezia;
  - Godfather rivolto ad applicazioni bancarie dell'UE;
  - Medusa (TangleBot) rivolto a Spagna, Turchia, Italia e Francia;
  - Hydra rivolto a telefoni Android in Polonia;
  - Copybara utilizzato in campagne fraudolente rivolte a Regno Unito, Spagna e Italia;
  - SpyNote rivolto a diversi clienti di banche europee; e
  - Bizarro rivolto a clienti di banche in tutta Europa.
- Il panorama delle minacce e degli attacchi sui **dispositivi mobili** è rimasto dinamico e complesso, con **malware mobile** sempre più sofisticato. Trojan bancari e spyware hanno rappresentato minacce significative, consentendo il furto di dispositivi e attività fraudolente. I principali colpiti sono stati **gli istituti di credito (36%)** e **i privati (24%).**
- Gli **attacchi ai fornitori**, principalmente violazioni dei dati e ransomware, hanno comportato **l'esposizione e la vendita di dati sensibili (63%)**, **interruzioni operative (26%)** e **perdite finanziarie (11%).**

3.2.2 Gli attacchi digitali in ambito spaziale

Il rapporto ENISA "Space Threat Landscape", pubblicato a marzo 2025, evidenzia la crescente importanza delle considerazioni sulla sicurezza digitale per l'industria spaziale, con particolare attenzione ai satelliti commerciali. Negli anni i si sono verificati diversi significativi attacchi digitali rivolti all'industria spaziale, compresi i sistemi satellitari su larga scala. Inoltre, il crescente corpus di quadri normativi dell'UE che regolamentano la sicurezza delle reti e delle informazioni, nonché la resilienza dei settori critici e importanti, riconosce **il settore spaziale tra le entità essenziali**, sottoponendolo quindi a rigorosi requisiti di sicurezza informatica che saranno applicabili a partire da gennaio 2025.

Nonostante l'enorme crescita del settore spaziale negli ultimi anni, sembra mancare una base di dati consolidata sugli incidenti di sicurezza informatica verificatisi in questo periodo.
La mancanza di analisi e controllo delle infrastrutture e degli oggetti spaziali è al 11° posto nelle previsioni ENISA al 2030, aggiornate a marzo 2024.

Nel presente Rapporto OAD 2025 non si intende entrare nel complesso mondo dei satelliti (per questo si rimanda al rapporto ENISA), che vede, come sintetizzato dalla fig. 3.2.2-1, tre principali segmenti: quello delle attività nello spazio, quella delle attività a terra, quello delle risorse umane che vi operano.

Si è a conoscenza di attacchi digitali ai sistemi satellitari fin dal 1977, con l'attacco ai sistemi di broadcasting audio ITM, e la fig. 3.2.2-2 mostra la distribuzione dei tipi di attacchi noti ai satelliti.
Il progetto di una banca dati sugli attacchi digitali ai sistemi spaziali è stato lanciato da una rivista specializzata, si veda https://www.spacesecurity.info/en/space-attacks-open-database/

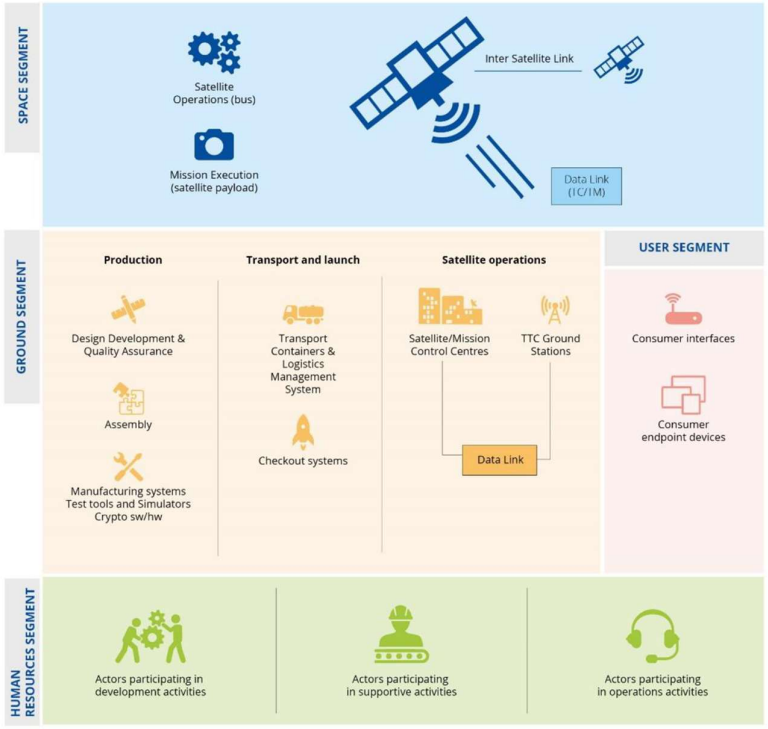


Fig. 3.2.2-1 (Fonte: ENISA Space Threat Landscape)

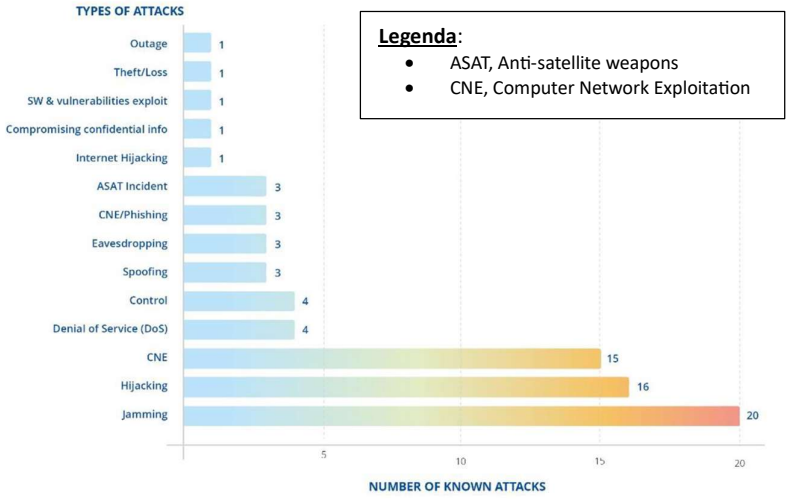


Fig. 3.2.2-2 (Fonte: ENISA Space Threat Landscape)

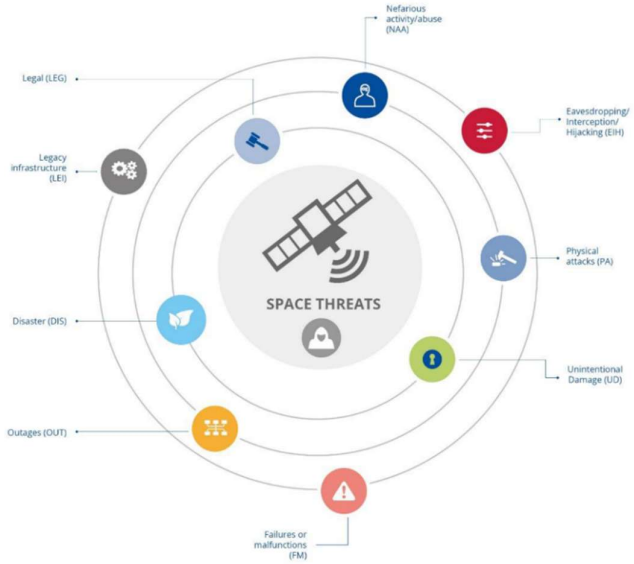


Fig. 3.2.2-3 (Fonte: ENISA Space Threat Landscape)

Fig. 3.2.2-4 (Fonte: ENISA Space Threat Landscape)

Il jamming[20] è stato tra le minacce più frequenti, i cui effetti possono variare dall'interruzione dell'accesso a un satellite all'impatto sui Sistemi Globali di Navigazione Satellitare (GNSS) utilizzati per servizi come il GPS. Seguono l'hijacking [21]e lo sfruttamento delle reti informatiche. Gli attacchi mirati alle funzioni di controllo, così come lo spoofing[22], l'intercettazione e l'impiego di armi anti-satellite (ASAT)[23], sono stati molto meno frequenti.

3.3 Il quadro a livello italiano

Per l'Italia OAD 2025, come nelle precedenti edizioni, fa riferimento ai dati pubblicati da ACN e dal Servizio Polizia Postale e per la Sicurezza Cibernetica (per quest'ultimo argomento **si veda Cap. 8**), oltre ovviamente alla sua indagine online i cui risultati sono **riportati nel Cap. 4**.
Il 2024 è stato per l'Italia un anno significativo per il quadro normativo, con le varie normative europee e con la legge n. 90/2024, su "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" prevalentemente orientato alle PA centrali e locali di medie-grandi dimensioni, incluse le rispettive società in house che forniscono servizi informatici, i servizi di trasporto urbano ed extra urbano, i servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, o di gestione dei rifiuti.
Per le normative europee il recepimento e l'attuazione della Direttiva NIS2, l'entrata in vigore del nuovo Regolamento per il cloud per le PA, l'approvazione del Cyber Resilience Act, del Regolamento eIDAS2 e dell'AI Act**.** Per le principali normative UE si veda fig. 3.2-1.

3.3.1 Gli attacchi digitali rilevati nel 2024 in Italia da ACN

Attraverso il **CSIRT** (Computer Security Incident Response Team) Italia, https://www.acn.gov.it/portale/csirt-italia, **ACN** (Agenzia per la Cybersicurezza Nazionale) ha potuto monitorare l'occorrenza di attacchi digitali soprattutto ai Sistemi Informativi (SI) considerati infrastrutture critiche e/o fornitori di servizi essenziali in Italia: in pratica tutte le organizzazioni previste dalla normativa NIS2[24], ed evidenziate nella fig. 3.3.1-1. Le organizzazioni dei settori elencati nella figura obbligati a seguire la NIS2 sono principalmente operatori di servizi essenziali (OSE), fornitori di servizi digitali (FSD), e Pubbliche Amministrazioni (PA) ed aziende dei settori indicati che superano i limiti di dimensione previsti: 50 dipendenti o un fatturato superiore ai 10 milioni di euro. Le PA considerate per la NIS2 sono, al momento, tutte le PA Centrali (PAC), le Regioni e le Province autonome, le Città metropolitane, i Comuni con popolazione superiore ai 100.000 abitanti, i Comuni capoluogo di Regione e le Aziende sanitarie locali.

[20] Il jamming informatico è un attacco che consiste nell'interferire o bloccare intenzionalmente i segnali wireless di un sistema, solitamente tramite un dispositivo chiamato "jammer". I jammer, o disturbatori, emettono segnali sulla stessa frequenza dei dispositivi bersaglio per sovraccaricarli, diminuire il rapporto segnale-rumore e impedire o degradare la comunicazione wireless, compromettendo sistemi di navigazione, reti cellulari, allarmi di sicurezza e altri dispositivi connessi.
[21] Un "hijacking" è un tipo di attacco informatico in cui un aggressore prende il controllo, o "dirotta", una comunicazione, un dispositivo o un account, reindirizzando la vittima verso risorse dannose o sfruttando sessioni di lavoro per accedere a informazioni riservate. Gli obiettivi possono variare, come generare traffico pubblicitario fraudolento (browser hijacking), rubare i cookie di sessione per accedere a sistemi (session hijacking), o alterare le rotte di Internet per dirottare i flussi di dati (IP hijacking).
[22] Un attacco spoofing è un tipo di frode informatica in cui un aggressore falsifica le proprie informazioni di origine per impersonare un'entità legittima, come un utente, un dispositivo o un servizio. L'obiettivo è ingannare la vittima o il sistema target per ottenere accesso non autorizzato a informazioni, risorse protette o per indurre azioni dannose, come il furto di denaro o dati sensibili.
[23] Le armi anti-satellite (ASAT) informatiche sono sistemi o tecniche che utilizzano l'hacking e la compromissione dei sistemi informatici di un satellite per danneggiarlo, controllarlo o renderlo inattivo senza contatto fisico diretto. A differenza delle ASAT cinetiche che distruggono i satelliti con impatti fisici, queste armi mirano all'elettronica e ai dati del satellite, potendo causare danni permanenti o temporanei attraverso software malevoli, compromissione di dati e attacchi digitali mirati.
[24] La NIS2 è l'entrata in vigore in Italia il 16 ottobre 2024, con il l D.Lgs. n. 138/2024 (c.d. decreto NIS2)

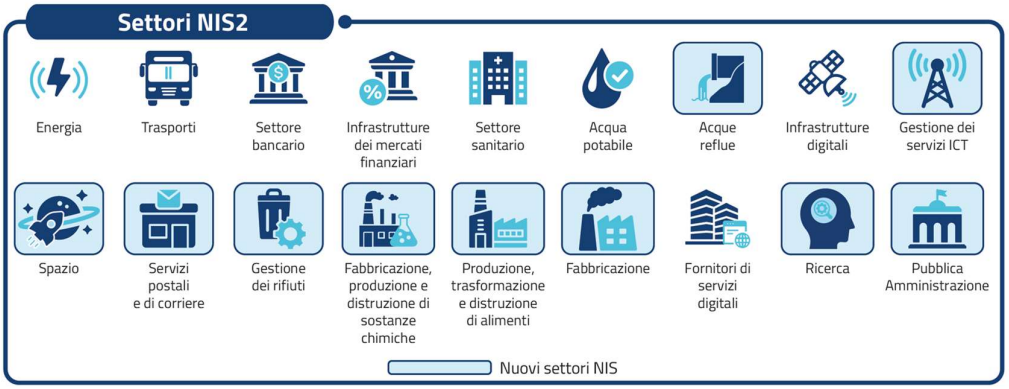
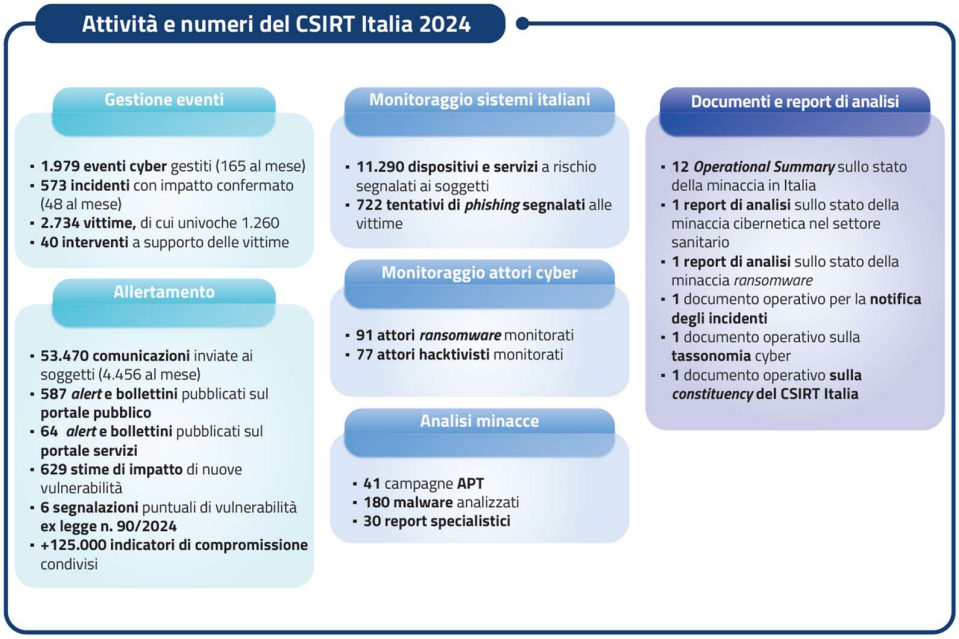


Fig. 3.3.1-1 (Fonte: CSIRT-ACN)

La fig. 3.3.1-2, dal Rapporto ACN 2024 alle Camere, sintetizza i numeri delle principali attività svolte dal CSIRT Italia nel 2024.



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

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

Fig. 3.3.1-2 (Fonte: CSIRT-ACN)

Per una corretta lettura dei dati riportati nella figura, occorre considerare le seguenti definizioni usate da ACN:

- **Case**: un avvenimento d'interesse per il CSIRT Italia, opportunamente approfondito al fine di identificare il possibile impatto e valutare la necessità di azioni di resilienza. I case possono diventare eventi cyber.
- **Evento cyber**: case con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, il CSIRT Italia dirama alert e/o supporta, eventualmente anche in loco, i soggetti colpiti.
- **Incidente**: un evento cyber con impatto su confidenzialità, integrità o disponibilità delle informazioni confermato dalla vittima.

Gli attacchi rilevati nel 2024 da CSIRT-ACN sono caratterizzati prevalentemente da ransomware e DDoS , ma anche dalla diffusione di malware via e-mail e phishing, indirizzati a diverse realtà pubbliche oltre che ad aziende attive nei settori più disparati (primi fra tutti telecomunicazioni, trasporti e servizi finanziari).

Più dettagliatamente la fig. 3.3.1-3 elenca le tipologie dei più importanti attacchi (top 20) rilevati in Italia da CSIRT-ACN nel 2024: il DDoS (Distributed Denial of Service) risulta di gran lungo il più diffuso, soprattutto per le PA e le aziende sanitarie.

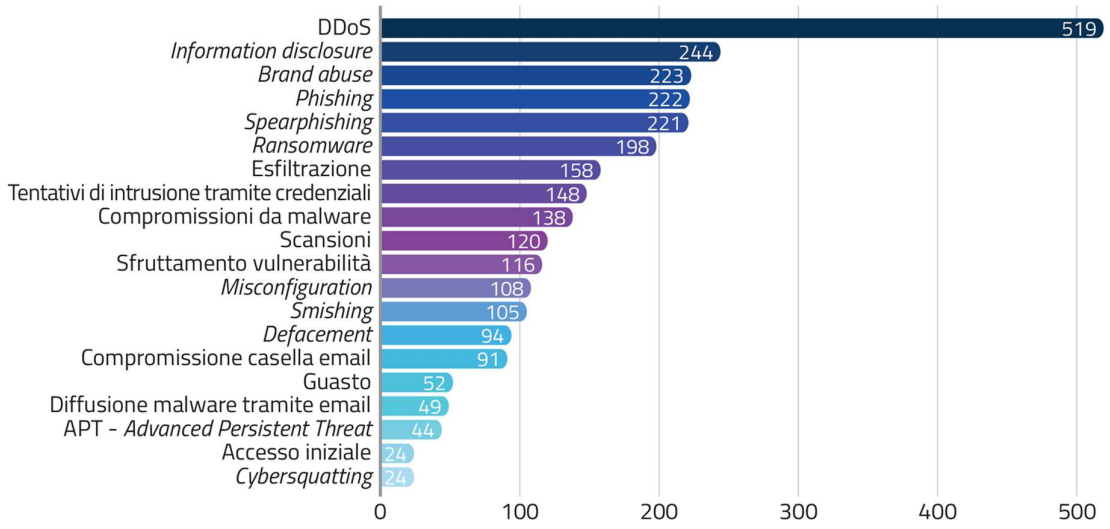


Fig. 3.3.1-3 (Fonte: CSIRT-ACN)

La fig. 3.3.1-4 mostra le tipologie di **vittime più attaccate** (top 10) nel 2024 in Italia, ed evidenzia come le PA siano tra le più colpite.

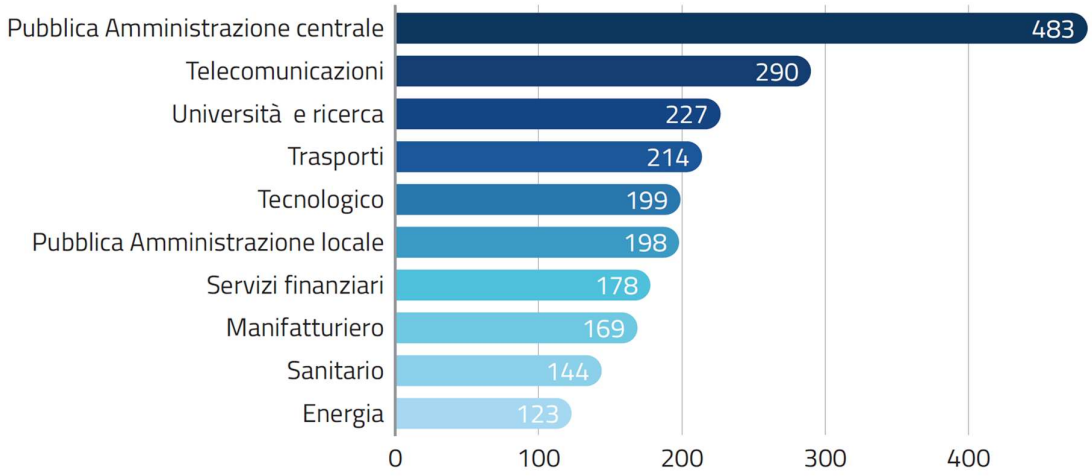


Fig. 3.3.1-4 (Fonte: CSIRT-ACN)

Interessante analizzare la distribuzione delle vittime di attacchi in base a tre livelli di criticità **(massima, intermedia, di base**) mostrata nella fig. 3.3.1-5.

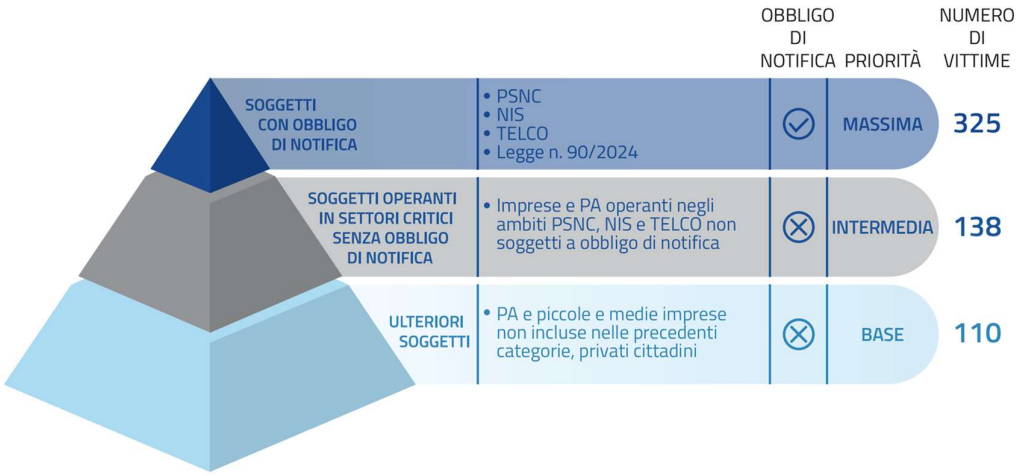


Fig. 3.3.1-5 (Fonte: CSIRT-ACN)

Il numero più elevato di vittime si registra nella fascia di criticità massima anche in ragione degli obblighi normativi di notifica, dato che tali vittime rientrano nei parametri di notifica obbligataria prevista dal PSNC, Perimetro di Sicurezza Nazionale Cibernetica, dalla Direttiva NIS/NIS2, dal Decreto TELCO e dalla legge n. 90/2024.
Per maggiori approfondimenti si ricorda che da maggio 2024 ACN pubblica, scaricabile dal suo sito web, una versione "pubblica" dell'**Operational Summary**, il documento mensile che riporta i numeri relativi alle principali fenomenologie cyber gestite e censite dal CSIRT Italia.

3.3.2 Aziende e Pubbliche Amministrazioni in Italia

Per comprendere il fenomeno degli attacchi digitali in Italia è opportuno/necessario avere il quadro delle aziende/enti attive per numero di dipendenti (medio nell'anno). I dati più aggiornati di ISTAT[25], Istituto Nazionale di Statistica, sono relativi al 2023 , e riportati nella fig. 3.3.2-1.

Numero addetti	*Numero imprese*	*% aziende/classe addetti*
0-9	**4.469.118**	**94,8%**
10-49	**214.793**	**4,6%**
50-249	**27.223**	**0,6%**
da 250 in su	**4.619**	**0,1%**
Totale imprese	**4.715.753**	
Totale PMI	**4.711.134**	**99,9%**

Fig. 3.3.2-1 (Fonte: elaborazione su dati ISTAT - 2023)

Dalla figura emerge che le **PMI,** Piccole e Medie Imprese (fino a 249 addetti)**,** costituiscono complessivamente il **99,9% del totale**, e fra queste le più piccole, fino a 9 dipendenti, sono la stragrande maggioranza con un **94,8%** del totale.
La fig. 3.3.2-1 riporta il numero di addetti[26] per le varie classi considerate da ISTAT.

[25] https://esploradati.istat.it/databrowser/

[26] Il termine addetto indica qualsiasi persona occupata in un'azienda, sia essa dipendente, lavoratore autonomo o altro. I dipendenti sono un sottoinsieme degli addetti.

Indicatore	Numero imprese attive (*)	Numero addetti delle imprese attive (valori medi annui) (*)
Classe di addetti		
0-9	4.469.118	7.717.413,4
10-49	214.793	3.874.240
50-249	27.223	2.650.694
250 e più	4.619	4.402.074
Totale	4.715.753	18.644.421,3

Fig. 3.3.2-2 (Fonte: ISTAT)

Per i dati sulle PA si è fatto riferimento sia al registro **ASIA di Istat**, aggiornato al 2022 (https://www.istat.it/tavole-di-dati/registro-asia-istituzioni-pubbliche-anno-2022/), al portale **OpenBDAP** (https://openbdap.rgs.mef.gov.it/it/) del Ministero dell'Economia e delle Finanze, aggiornato al 2023, all'**Indice PA** (https://www.indicepa.gov.it/ipa-portale/) aggiornato al 2024.
Questi tre portali, essendo aggiornati in tre anni diversi, riportano numeri diversi soprattutto per il variare nel tempo degli addetti nei vari enti. Inoltre questi tre portali aggregano o dettagliano dati in modalità diverse, e *l'autore ha usato quelli più idonei per OAD, senza preoccuparsi delle differenze numeriche tra un anno e l'altro: quello che interessa OAD, come in più punti evidenziato in questo Rapporto, sono le logiche ed i trend del fenomeno attacchi digitali, gli ordini di grandezza coinvolti, non uno specifico numero relativo ad un anno.*
Le Pubbliche Amministrazioni (PA) sono articolate, anche nel questionario OAD 2025,nelle seguenti voci:

- Pubbliche Amministrazioni Centrali (PAC): sono nel complesso **2.239**, secondo i dati del 2024 dell'Indice PA, che raggruppa istituti, ministeri, enti e agenzie statali. Il questionario OAD 2025 non ha richiesto di specificare a quale PAC appartenesse chi compilava il questionario per motivi di riservatezza. Nel dettaglio le PAC sono articolate in:
  - Presidenza del Consiglio, Ministeri e Avvocatura dello Stato: 17 amministrazioni.
  - Organi Costituzionali e di Rilievo Costituzionale: 9 amministrazioni.
  - Istituti Zooprofilattici Sperimentali:10 amministrazioni.
  - Altre categorie: le restanti amministrazioni rientrano in altre categorie nel calcolo totale di 2.239.

- Pubbliche Amministrazioni Locali (PAL): sono nel complesso in **11.118**. Il questionario OAD 2025 ha specificato per le PAL le seguenti possibili risposte:
  - Regione ed Enti della Regione
  - Provincia ed Enti della Provincia
  - Comune metropolitano o Comune capoluogo
  - Altri comuni con popolazione superiore a 15 000 abitanti
  - Comune con popolazione compresa fra 5 000 e 15 000 abitanti
  - Piccoli comuni
  - Altra PAL.

La ripartizione dei dipendenti per tutte le PA è riportato in fig. 3.3.2-3.

Comparto	Aggregato	Dipendenti PA
FUNZIONI LOCALI	REGIONI ED AUTONOMIE LOCALI	401.795
FUNZIONI LOCALI	REGIONI A STATUTO SPECIALE E PROVINCE AUTONOME	92.172
ISTRUZIONE E RICERCA	SCUOLA	1.222.015
ISTRUZIONE E RICERCA	ENTI DI RICERCA	24.718
ISTRUZIONE E RICERCA	IST. FORM.NE ART.CO MUS.LE	10.735
ISTRUZIONE E RICERCA	UNIVERSITA'	49.473
SANITA'	SERVIZIO SANITARIO NAZIONALE	701.170
PERSONALE IN REGIME DI DIRITTO PUBBLICO	FORZE ARMATE	175.117
PERSONALE IN REGIME DI DIRITTO PUBBLICO	CARRIERA DIPLOMATICA	1.068
PERSONALE IN REGIME DI DIRITTO PUBBLICO	CORPI DI POLIZIA	303.706
PERSONALE IN REGIME DI DIRITTO PUBBLICO	MAGISTRATURA	10.797
PERSONALE IN REGIME DI DIRITTO PUBBLICO	CARRIERA PENITENZIARIA	282
PERSONALE IN REGIME DI DIRITTO PUBBLICO	VIGILI DEL FUOCO	35.970
PERSONALE IN REGIME DI DIRITTO PUBBLICO	PROFESSORI E RICERCATORI UNIVERSITARI	51.324

Comparto	Aggregato	Dipendenti PA
PERSONALE IN REGIME DI DIRITTO PUBBLICO	CARRIERA PREFETTIZIA	1.058
FUNZIONI CENTRALI	MINISTERI	123.507
FUNZIONI CENTRALI	ENTI PUBBLICI NON ECONOMICI	40.471
FUNZIONI CENTRALI	ENTI ART.70 - E.N.A.C.	1.114
FUNZIONI CENTRALI	AGENZIE FISCALI	39.956
FUNZIONI CENTRALI	ENTI ART.70 - C.N.E.L.	58
FUNZIONI CENTRALI	AGENZIA PER L'ITALIA DIGITALE	98
COMPARTO AUTONOMO O FUORI COMPARTO	ENTI ART.70 - UNIONCAMERE	55
COMPARTO AUTONOMO O FUORI COMPARTO	AUTORITA' INDIPENDENTI	2.539
COMPARTO AUTONOMO O FUORI COMPARTO	ENTI LISTA S13 ISTAT	31.017
COMPARTO AUTONOMO O FUORI COMPARTO	ENTI ART.60 - COMMA 3- D.165/01	5.374
COMPARTO AUTONOMO O FUORI COMPARTO	PRESIDENZA CONSIGLIO MINISTRI	2.265
COMPARTO AUTONOMO O FUORI COMPARTO	PRESIDENZA CONSIGLIO MINISTRI	2.265
COMPARTO AUTONOMO O FUORI COMPARTO	PRESIDENZA CONSIGLIO MINISTRI	2.265
COMPARTO AUTONOMO O FUORI COMPARTO	PRESIDENZA CONSIGLIO MINISTRI	2.265

Fig. 3.3.2-3 (Fonte: OpenBDAB aggiornata al 2023)

Numero dipendenti	*Numero PA*	*%*	*Dipendenti (media annua)*	*%*	*Dimensione (media)*
da 0 a 9	6.384	47,8	21.894	0,6	3,4
da 10 a 49	4.580	34,3	101.668	2,9	22,2
da 50 a 249	1.721	12,9	176.123	5,0	102,3
da 250 a 999	349	2,6	164.110	4,6	470,2
da 1,000 a 24,999	316	2,4	1.180.491	33,3	3.735,7
25,000 e oltre	7	0,1	1.903.758	53,7	271.965,4
Totale	**13.357**	**100,0**	**3.548.043**	**100,0**	**265,6**
PA <250 dipendenti	**12.685**	**95,0**			

Fig. 3.3.2-4 (Fonte: Istat - Registro Asia Istituzioni Pubbliche - Anno 2022)

Il numero di dipendenti complessivo per tutta la PA è di circa **3,3 Mln di dipendenti** su **13.357 enti**, e di questi, come evidenziato in fig. 3.3.2-4, il **95%** è di organizzazioni al di sotto dei 250 dipendenti. Questa percentuale si avvicina al 99,9% delle PMI nell'ambito privato. Molto minore nelle PA il numero di micro organizzazioni, al di sotto dei 10 dipendenti/addetti, con un **47,8%** che è quasi la metà del 94,8% delle micro imprese private.

Questi dati confermano che la realtà italiana delle imprese pubbliche e private è costituita da piccole e piccolissime organizzazioni, che costituiscono quasi il 63% delle imprese rispondenti al questionario OAD 2025: e di queste il 22% è costituito dalle micro imprese. (si veda fig. 6.1-2). L'importanza dell'indagine OAD nel contesto italiano della sicurezza digitale è anche questo: considerare anche le piccole e micro realtà nell'analizzare il fenomeno degli attacchi digitali e delle misure di sicurezza messe in atto per contrastarli.

3.3.3 La spesa in sicurezza digitale in Italia nel 2024

I dati presi a riferimento sul tema sono derivati dall'ultimo ed autorevole rapporto **Anitec-Assinform, (**patrocinatore di OAD 2025) "Il Digitale in Italia 2025"[27].
La fig. 3.3.3-1 mostra il valore nel 2024 della spese per la sicurezza digitale , con il superamento di € 2 Mld ed un incremento dell'11% rispetto all'anno precedente.

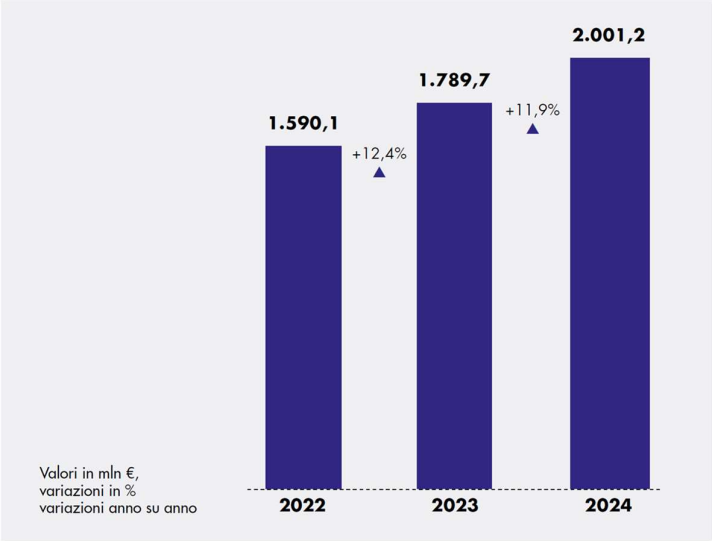


Fig. 3.3.3-1 (Fonte: Il Digitale in Italia 2025 di Anitec-Assinform)

La fig. 3.3.3-2 dettaglia la ripartizione di questi € 2 Mld per i diversi settori considerati nell'indagine, e si evidenziano come settori principali i "Servizi MSS e Cloud" e il "Security hardware"; quest'ultimo include le appliance ad hoc che contegono uno o poù strumenti di sicurezza digitale.

[27] https://www.anitec-assinform.it/pubblicazioni/il-digitale-in-italia/edizioni/il-digitale-in-italia-2025.kl

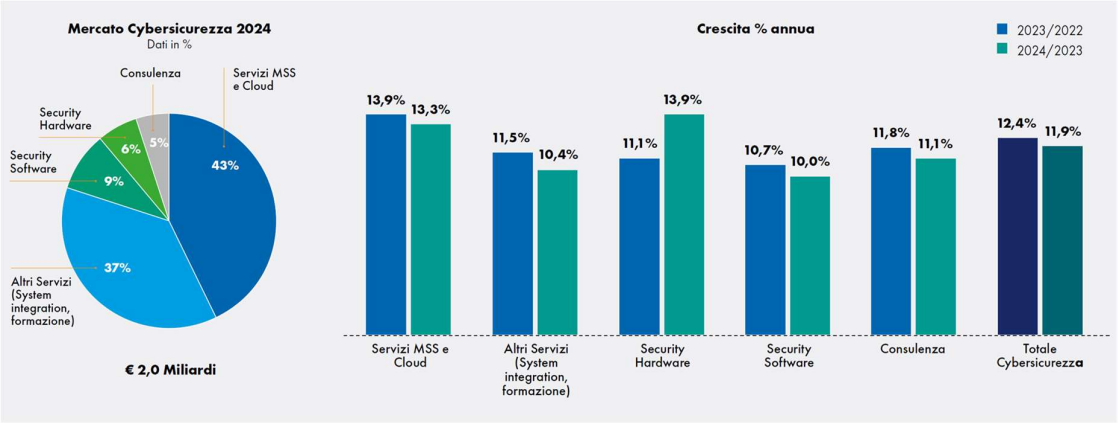


Fig. 3.3.3-2 (Fonte: Il Digitale in Italia 2025 di Anitec-Assinform)

3.4 Le vulnerabilità causa degli attacchi digitali

Tutte le minacce cibernetiche, intenzionali e non, si basano su **vulnerabilità** (definibile come la predisposizione ad essere facilmente attaccato, offeso) che possono essere categorizzate in **tecniche**, **delle persone**, **dell'organizzazione**.

Le vulnerabilità delle persone sono le più critiche, dato che riguardano il comportamento umano in ambito digitale sia per gli utenti finali sia, in particolar modo, per gli utenti privilegiati: il comportamento umano non è sempre prevedibile ed è difficilmente limitabile/controllabile. La vulnerabilità di una persona in ambito ICT è spesso involontaria e deriva da fattori come inconsapevolezza, imprudenza, imperizia o ignoranza, spesso aggravati dalla mancanza di formazione e addestramento. Queste ultime sono tipiche vulnerabilità organizzative, alle quali si aggiungono frequentemente altre carenze ed inefficienze, come l'assenza di procedure scritte e divulgate o la mancanza di controlli efficaci.

3.4.1 Le vulnerabilità tecniche

A livello tecnico esistono autorevoli ed aggiornati siti che elencano, classificandole, le vulnerabilità tecniche individuate su tutti i prodotti/sistemi/servizi ICT a livello mondiale: in particolare i più noti ed usati sono il CVE/MITRE[28] (https://cve.mitre.org/) e lo statunitense NVD, National Vulnerability Database, (https://nvd.nist.gov/) che a sua volta fa riferimento ai dati e alla numerazione CVE. Per ciascuna vulnerabilità questi siti riportano le modalità per eliminarle o ridurle, se esistono e sono state provate.

Da queste banche dati si evince che ogni prodotto/servizio ICT, di qualsiasi produttore (incluse le comunità che sviluppano sistemi opensource), ha delle specifiche vulnerabilità tecniche individuate.

CNA, CVE Numbering Authority, è l'ente che assegna l'identità CVE alle vulnerabilità individuate (a livello mondiale), assicurandone accuratezza e consistenza: si veda https://www.cve.org/programorganization/cnas

Alla data della stesura del presente rapporto OAD, settembre 2025, il totale delle vulnerabilità tecniche individuate e registrate nella banca dati CVE è di **296.000** (rispetto ai 240.830 di settembre 2024**,** e ai 212.202 di settembre 2023): le vulnerabilità tecniche individuate per i vari prodotti/sistemi ICT **continuano ad aumentare anno per anno.**

In termine generali, per le vulnerabilità tecniche, è bene evidenziare che:

[28] CVE, Common Vulnerabilities and Exposures, il database delle vulnerabilità tecniche individuate a livello mondiale su ogni sistema ICT. MITRE (https://www.mitre.org/) è una fondazione no profit statunitense creata per promuovere la sicurezza nazionale in nuovi modi e servire l'interesse pubblico in qualità di consulente indipendente.

- non tutte le vulnerabilità esistenti sono state individuate e classificate negli elenchi CVE e NVD: quelle non ancora individuate, ed indicate con il termine "**zero-day**", sono le più critiche, perché non prevedono ancora alcuna protezione e, se l'attaccante le conosce, può attaccare senza trovare alcun contrasto;
- per alcune vulnerabilità conosciute, sono occorsi talvolta mesi prima di avere a disposizione una patch correttiva; pertanto, esistono vulnerabilità note ma senza una correzione disponibile.

Ogni vulnerabilità tecnica di un codice software ha un diverso **livello di severità**, ossia la gravità degli impatti nel caso fosse sfruttata da attaccanti, che è stabilito da una metrica associata alle vulnerabilità registrate nella banca dati CVE, il **CVSS**, Common Vulnerability Scoring System. CVSS fornisce una metrica ed una logica per stabilire un punteggio indicatore del livello di **gravità** della vulnerabilità, basandosi sulle sue principali caratteristiche di base, su quelle che potrebbero cambiare nel tempo, sul contesto nel quale potrebbe essere sfruttata. La valutazione della severità di una vulnerabilità è importante nell'ambito dell'analisi dei rischi e per poter dare priorità ai processi di gestione delle vulnerabilità ICT. Attualmente il CVSS è alla versione 4.0 ed **è composto da tre gruppi di metriche (base, temporale e ambientale) e dalle loro possibili combinazioni.**
Per ogni vulnerabilità individuata in CVE, nella banca dati NVD del NIST è pubblicato il livello di severità di base, l'unico che non cambia nel tempo ed è comune a tutti gli ambienti d'utilizzo. Questo punteggio della severità di base, da 0 a 10, con 10 la massima gravità, fa riferimento alle **caratteristiche intrinseche di una vulnerabilità** nel caso fosse sfruttata, ed è fornito dal produttore della risorsa ICT per la quale è stata individuata la vulnerabilità.
Le vulnerabilità individuate e classificate in NVD con le più alte severità di base sono numerose ed arrivano **al 18%** circa delle vulnerabilità totali.
Per approfondimenti si veda https://nvd.nist.gov/vuln-metrics/cvss e https://www.first.org/cvss/ (First è l'ente che attualmente gestisce CVSS e la sua evoluzione).
Una ulteriore banca dati sulle vulnerabilità tecniche ICT è la CWE, Common Weakness Enumeration, un catalogo di vulnerabilità software e hardware, di problemi di sicurezza e di errori di programmazione comuni. Serve come riferimento per le vulnerabilità note della sicurezza del software ed è fondamentale per migliorare la comprensione e la mitigazione di queste vulnerabilità durante il processo di sviluppo del software.
Importante evidenziare la **differenza tra CVE e CWE**: il primo è uno standard per identificare e nominare vulnerabilità specifiche, mentre il secondo è uno standard per classificare e descrivere i tipi di debolezze che possono portare a vulnerabilità**.**

3.4.2 Le vulnerabilità delle persone

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 di cui in §3.4.3.
Per le vulnerabilità personali lo strumento di contrasto più importante è la formazione continua e la consapevolezza che, nell'uso dei sistemi informatici, 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. In Italia tale consapevolezza è ancora carente, così come lo sono le competenze specialistiche informatiche, cui si aggiunge, a livello generale, un ancor forte gender gap.

Il primo significativo indicatore sulle competenze ICT è stato, fino al 2022, l'**indice DESI**[29] sul livello di digitalizzazione dell'economia e della società, grazie alla voce **competenze digitali** tra i 36 indicatori considerati e raggruppati nelle quattro dimensioni illustrate nella fig. 3.4.2-1.

[29] DESI, Digital Economy and Society Index, è un indice composito che sintetizza vari rilevanti indicatori sulle prestazioni digitali in Europa e traccia l'evoluzione dei vari membri EU nella competitività digitale.

Dimensione	Sottodimensione
Competenze digitali	Uso di internet
	Competenze avanzate e di sviluppo
Infrastrutture digitali	Banda larga fissa
	Banda larga mobile
Trasformazione digitale delle imprese	Intensità digitale delle PMI
	Tecnologie digitali per le imprese
	e-Commerce
Digitalizzazione dei servizi pubblici	e-Government
	e-Health

Fig. 3.4.2-1 (Fonte: Commissione Europea)

Ora i dati DESI[30] sono inclusi nel rapporto "Digital Decade Report 2024"[31], la pubblicazione annuale della Commissione Europea che valuta i progressi dell'Unione Europea e degli Stati membri, inclusa l'Italia, verso gli obiettivi del programma strategico europeo per la trasformazione digitale entro il 2030[32].
La fig. 3.4.2-2 estratta dagli ultimi dati DESI disponibili al 2024, mostra **il numero di specialisti in ICT operanti in Italia**, pari al 4,0% sul totale degli occupati, e che pone l'Italia al terz'ultimo posto tra i 28 paesi dell'UE.
Tale gravissima carenza si accompagna, negativamente, alle **competenze ICT di base** nella popolazione italiana, evidenziata nella 3.4.2-3 che mostra l'Italia, con un **45,75%** sul totale degli italiani tra i 16 e 74 anni, ancora agli ultimi posti in UE . E altrettanto allarmante, anche se aggiornato solo al 2022, il trend di crescita di **laureati in materie scientifiche**, mostrato in fig. 3.4.2-4 con la linea verde in basso, che vede l'Italia **sempre ultima** in UE dal 2018 al 2022; dalla indicazioni avute dall'autore, la situazione negli ultimi anni dal 2022 ad oggi non è migliorata, anzi forse è leggermente peggiorata.

Il problema delle competenze ICT in Italia, anche solo di base, costituisce un grave "minus" per la competitività del paese, non solo in ambito europeo ma anche mondiale.
Le specifiche competenze per la sicurezza digitale **sono ancor più ridotte**, essendo un di cui delle più generali competenze avanzate nel digitale, ed **incidono profondamente sul livello di sicurezza digitale delle singole organizzazioni e dell'intero sistema paese**.
Considerando l'enorme numero di piccole e piccolissime organizzazioni sia nel privato che nel pubblico, la fisiologica, quasi normale, incompetenza sulla sicurezza digitale da parte di queste organizzazioni lascia ampio spazio al millantato credito e a comportamenti scorretti di numerosi attori ed interlocutori dell'offerta, che rasentano sovente la truffa.
La bassa competenza nella sicurezza digitale da parte di piccole-medie organizzazioni è un effetto leva per una sua forte terziarizzazione, a livello operativo, ma al contempo pone difficoltà nella scelta del fornitore (anche il singolo consulente) idoneo a fornire una soluzione adeguata alla propria realtà.

[30] https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts
[31] https://digital-strategy.ec.europa.eu/en/factpages/state-digital-decade-2024-report
[32] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_it
https://digital-decade-desi.digital-strategy.ec.europa.eu/

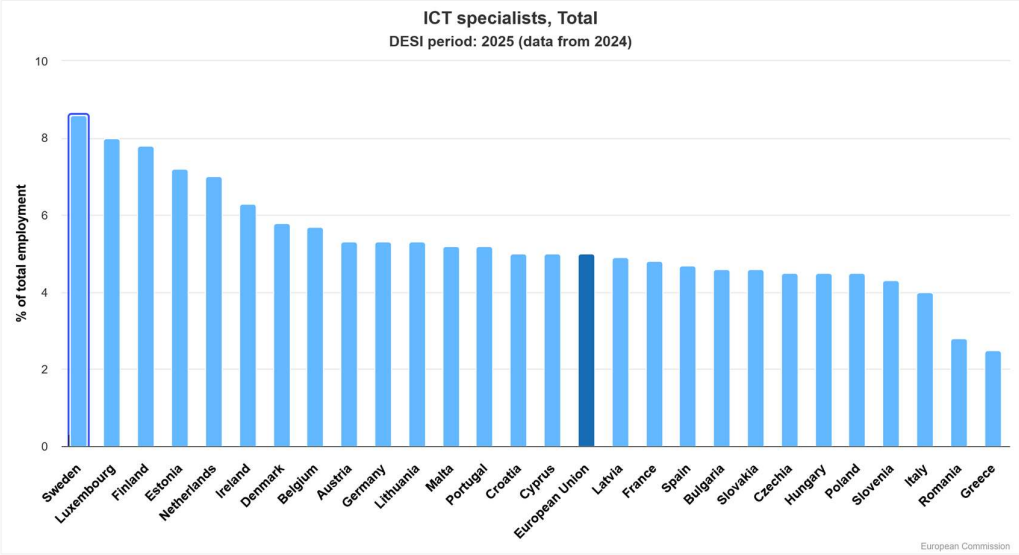


Fig. 3.4.2-2 (Fonte: Commissione Europea)

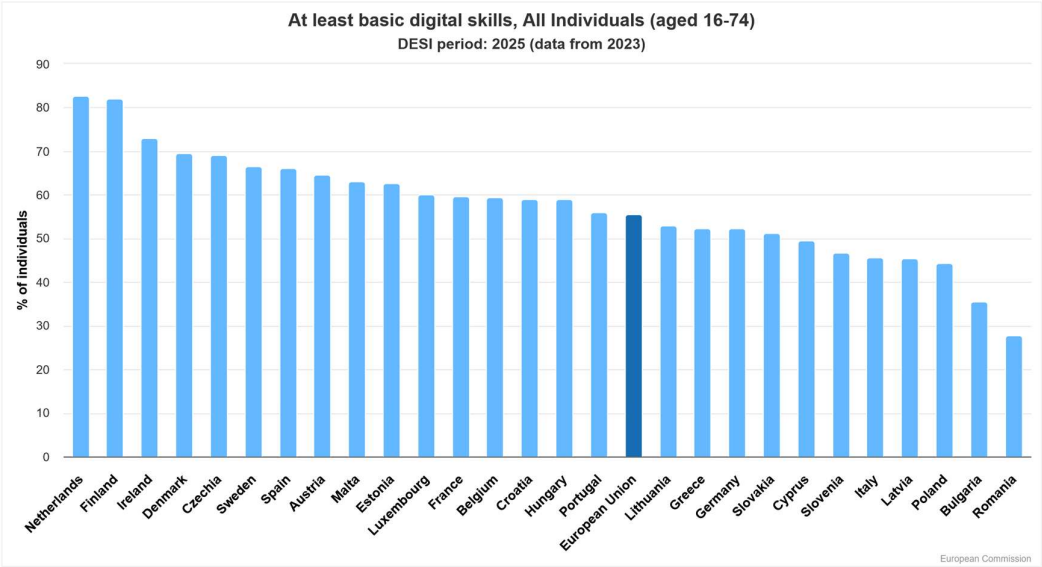


Fig. 3.4.2-3 (Fonte: Commissione Europea)

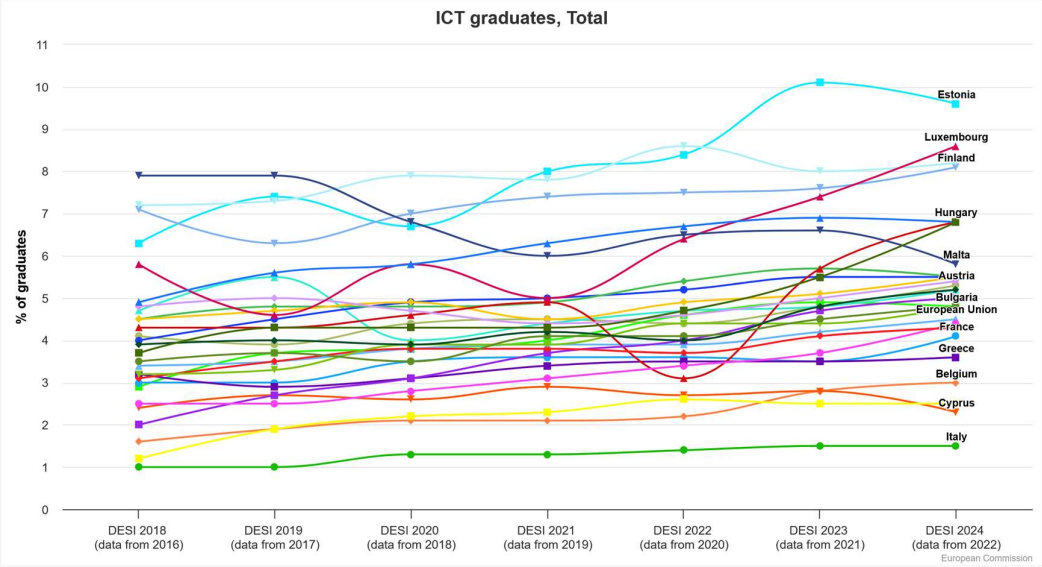


Fig. 3.4.2-4 (Fonte: Commissione Europea)

3.4.2 Le vulnerabilità organizzative

Gli aspetti organizzativi sono determinanti per l'attuazione di una reale ed effettiva sicurezza digitale, ed impattano sul personale utente del sistema informativo.

Le piccole e medie organizzazioni, ma talvolta anche quelle piuttosto grandi, difficilmente possono disporre al proprio interno delle competenze tecniche ed organizzative aggiornate per la sicurezza digitale: sarebbe opportuno che le terziarizzassero ma, al contempo, devono saperle controllare ed indirizzare rispetto al loro specifico contesto. In caso contrario dipenderanno sempre più dagli outsourcer e dagli altri fornitori esterni, in primis i consulenti, che a loro volta potrebbero avere non adeguate competenze nella sicurezza digitale: in tal senso, il cerchio delle incompetenze si chiude con possibili conseguenze molto negative per l'azienda/ente cliente.

In termini di figure e ruoli preposti alla sicurezza digitale, il responsabile è indicato con l'acronimo **CISO**, Chief Information Security Officer: questa figura negli anni passati operava prevalentemente nell'ambito della struttura dei sistemi informativi, indicata nei rapporti OAD con l'acronimo **UOSI** , Unità Organizzativa Sistemi Informativi, alle dipendenze del suo responsabile, il **CIO**, Chief Information Officer.

La tendenza è ora di porre il CISO nell'ambito di altre strutture, non in UOSI, per garantire una effettiva separazione delle responsabilità tra CIO e CISO.

Lato domanda ICT, almeno a livello di vertice, occorrerebbe possedere le competenze necessarie per "governare" a livello strategico l'evoluzione del sistema informativo in funzione delle necessità e del business dell'azienda/ente. In tale "governo" il vertice deve/dovrebbe saper scegliere fornitori competenti e affidabili, e saperli supervisionare nella loro gestione della sicurezza digitale; essa non rappresenta solo un problema tecnico, ma soprattutto di business, dato che ormai è determinante per la continuità operativa dell'intera azienda/ente.

3.5 Le contromisure per la sicurezza digitale e la loro evoluzione

Così come si sono e si stando evolvendo le tecniche di attacco digitali, allo stesso modo si stanno evolvendo le tecniche per la difesa dei sistemi digitali. Le misure e le tecniche fino ad oggi usate sono state di tipo reattivo[33], solo in parte proattive e preventive[34], e pochissime predittive[35].

Con l'attuale alta densità di vulnerabilità tecniche, **si fa ricadere spesso la responsabilità** dell'occorrenza di un attacco **all'incapacità e agli errori dell'utente**, o finale o privilegiato. L'uso di soluzioni con misure di sicurezza by default (oltre che by design) e che non richiedano specifiche competenze per usarle, per una sicurezza digitale "always on" ed integrata in ogni risorsa ICT, è una tendenza ed un obiettivo **a lungo termine**, perseguito anche dall'Unione Europea con il Cyber Security Act[36], che dovrebbe portare alla realizzazione di sistemi ICT intrinsecamente sicuri, indipendentemente dal buono o cattivo uso da parte dell'utente: sistemi senza vulnerabilità tecniche intrinseche e così facili da usare da ridurre, se non eliminare, le possibili vulnerabilità personali ed organizzative.

Le logiche evolutive e le tecniche più innovative per la sicurezza digitale, spesso indicate con il generico termine di "**Next Generation Security**", includono:

- Il passaggio dalla tradizionale logica "statica" di misure e strumenti di difesa in funzione delle vulnerabilità e rischi individuati, ad una logica "dinamica", basata sull'analisi predittiva e comportamentale dei sistemi ICT e dei loro utenti, effettuata anche tramite sistemi di Machine Learning (ML);
- una crescente e forte automazione dei processi e delle attività della gestione operativa della sicurezza digitale, con l'uso di tecniche di ML e di altre tecniche di IA[37];
- l'adozione di logiche, approcci ed architetture "Zero Trust" e di un mix, con questa, di altre logiche ed architetture quali SASE, SIEM, SOAR, EDM, etc., con una loro crescente interoperabilità, integrazione ed automazione;
- l'adozione di tecniche di IA e di ML sia nella gestione operativa, ad esempio nella correlazione dei log e delle segnalazioni di sistema, sia nella threat intelligence e nell'analisi dei rischi;
- l'adozione di tecniche di autenticazione forte "passwordless" degli utenti basate su riconoscimenti biometrici, seppur ancora embrionale data anche la necessità di autorizzazione da parte del Garante della privacy;
- l'introduzione di soluzioni EDR, Endpoint[38] Detection & Response[39], che si affiancano o integrano con soluzione SIEM, SASE, etc. sulla base di logiche ed architetture "zero trust";
- il rafforzamento della sicurezza digitale nella "supply chain", dato che alcuni gravi attacchi sono partiti da vulnerabilità di fornitori e/o di clienti interoperanti con il sistema informativo target;

---

[33] Misure reattive: reagiscono quando individuano il problema, tipicamente un attacco digitale, cercando di bloccarlo. Strumenti principali usati includono: sensibilizzazione e formazione degli utenti, controllo dei loro accessi ai sistemi ICT, monitoraggio funzionalità dei sistemi ICT, antivirus, firewall perimetrali, backup, Disaster Recovery.

[34] Misure proattive e preventive: cercano di prevenire possibili malfunzionamenti ed attacchi. Oltre alle misure, tecniche ed organizzative, necessarie per la sicurezza reattiva, le misure preventive includono l'uso di sistemi IPS/IDS, analisi vulnerabilità e dei log, crittografia dei dati più critici e delle comunicazioni, l'auditing, etc.

[35] Misure predittive: sono la logica evoluzione di quelle preventive, con l'obiettivo non solo di prevenire attacchi, ma di rilevare quei segnali che anticipano un attacco. Usando anche tecniche di AI, queste misure cercano di scoprire ed anticipare le minacce prima che possano accadere; includono la raccolta e l'analisi di informazioni in tempo reale, l'analisi dei modelli di comportamento, l'analisi "avanzata" e la valutazione dei rischi nel proprio contesto informatico.

[36] In particolare per la certificazione europea della sicurezza digitale in prodotti/sistemi/servizi con un logica, rivista, simile a quella dei ben noti Common Criteria. Si veda https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act e https://www.commoncriteriaportal.org/

[37] L'Intelligenza Artificiale generativa, la più diffusa attualmente a fianco del ML, può essere utilizzata sia come arma d'attacco sia come strumento di difesa.

[38] Endpoint: dispositivi fisici che si connettono e scambiano informazioni in una rete di computer, da smartphone a PC, da server ai vari dispositivi OT quali IoT.

[39] EDR, Endpoint Detection & Response: strumenti di sicurezza degli endpoint che includono il monitoraggio e la raccolta in tempo reale dei dati di comportamento e sicurezza degli endpoint mediante meccanismi automatici, e che consentono una più veloce risposta alle minacce.

- l'utilizzo di soluzioni di "Threat Intelligence"[40];
- la crescente adozione di misure di sicurezza digitale "as a service", la Cybersecurity as a Service, e più in generale la crescente terziarizzazione della sicurezza digitale, soprattutto a livello di gestione operativa, chiamata MSS, **Managed Security Services**;
- l'uso di **SOC, Security Operation Centre**, per una proattiva ed efficace gestione della sicurezza digitale, in particolare per la gestione delle infrastrutture (soprattutto quelle critiche), la rilevazione di incidenti e le relative azioni di contrasto e contenimento. Il SOC è una struttura iper specializzata, che alcune grandi organizzazioni, ad esempio di fornitori ICT e TLC, hanno al proprio interno, ma che è anche fornito "as a service" dai MSSP, Managed Security Service Provider;
- l'adozione, oggi ancora embrionale, di soluzioni XR, Extended Reality, e del metaverso[41], per attività di formazione, simulazione ed analisi nella sicurezza digitale, oltre che di assistenza, gestione e manutenzione, il tutto anche (e soprattutto) da remoto, e quindi fornibili "as a service";
- la tendenza alla realizzazione di soluzioni di sicurezza digitale intrinseche (embedded) nei vari sistemi digitali, in modo che tale sicurezza sia di default ed impostata fin dal progetto del sistema stesso (by design).

La sicurezza digitale assoluta non esiste, ma nel mondo ormai dominato dall'ICT in Internet, la sicurezza digitale è e deve essere un obbligo di tutte le aziende/enti, non solo di quelle critiche, ed occorre pertanto:

- attivare e gestire al meglio tutte le misure di sicurezza in essere, sia tecniche sia organizzative;
- far crescere la consapevolezza e le competenze sulla sicurezza digitale a tutti i livelli, sia lato domanda che offerta di sistemi ICT;
- bloccare e reprimere i cracker ed il cybercrime, riducendo gli alti guadagni illegali con pochissimi rischi dei criminali ICT, grazie a specifiche leggi e ad una maggiore collaborazione internazionale, sia a livello legislativo sia a livello di forze di Polizia;
- far crescere l'**etica professionale di chi si occupa di sicurezza digitale lato domanda e lato offerta**: lato domanda non si dovrebbe scendere sotto certi valori come pagamento giornaliero di riferimento, anche in caso di gare, e lato offerta non si dovrebbero vendere soluzioni e sistemi ICT obsoleti o non utili al cliente, approfittando della sua non competenza in merito.

In ambito europeo, un driver fondamentale per l'innalzamento del livello ed il miglioramento "continuo" della sicurezza digitale sono le "nuove" normative della UE in merito sulla sicurezza digitale, già indicate nella fig. 3.2-1.
Si rammenta che un regolamento UE si applica direttamente agli Stati membri, mentre una direttiva UE deve prima essere recepita e tradotta in legge in ogni Stato membro.

3.5.1 La terziarizzazione della sicurezza digitale

Nella maggior parte dei casi, in particolare per le piccole e medie organizzazioni, non si può disporre al proprio interno di qualificate ed aggiornate competenze sulla sicurezza digitale: in questi casi è opportuno terziarizzarla, dal progetto alla gestione operativa: ma questo non significa rinunciare totalmente alle competenze in merito, occorre sempre controllare ciò che la/le terza/e parte/i fa/fanno e come, altrimenti si diverrà preda e si sarà in balia dei fornitori e dei consulenti.
Moderne piattaforme e soluzioni quali SIEM, SOAR, SESA, e le stesse tecniche di blockchain, costituiscono sistemi molto complessi e difficili da gestire anche per grandi organizzazioni con elevate competenze al proprio interno.

[40] Threat Intelligence è la raccolta e la selezione di informazioni dettagliate ed utilizzabili sulle minacce digitali, in moda consentire una prevenzione proattiva e predittiva dei reali rischi alla sicurezza del sistema informativo
[41] Metaverso: ecosistema immersivo, persistente, interattivo e interoperabile, composto da molteplici mondi virtuali interconnessi in cui gli utenti possono socializzare, lavorare, effettuare transazioni, giocare e creare asset, accedendo anche tramite dispositivi immersivi (definizione della School of Management del Politecnico di Milano).

Vulnerabilità e rischi digitali esistono, e della stessa complessità e sofisticazione, sia per grandi che per piccole organizzazioni. La citata necessità di terziarizzare la sicurezza digitale, soprattutto per le piccole organizzazioni italiane sta creando un crescente mercato di fornitori di servizi di sicurezza gestiti, indicati con MSSP, Managed Security Services Provider, ed incominciano ad essere utilizzati simili servizi erogati dai grandi player digitali, da Google a AWS, da Microsoft ad IBM. Come già indicato in precedenza, in questo contesto vanno crescendo i servizi tipo **CSaa**S, Cybersecurity as a Service, e **MSS**, Managed Security Services.

3.6 Le Istituzioni per la sicurezza digitale

In Italia è stata effettuata una importante riorganizzazione dei vari enti pubblici dedicati alla sicurezza digitale, attualmente in fase di completamento operativo, a partire dalla Legge 124/2007 che ha riordinato tutti i servizi segreti italiani, che si occupano anche della cyber intelligence.
La fig. 3.6-1 schematizza gli enti preposti e loro relazioni: tutti fanno riferimento alla Presidenza del Consiglio dei Ministri, con il **CISR**, Comitato Interministeriale per la Sicurezza della Repubblica, ed il **COPASIR**, Comitato parlamentare per la sicurezza della Repubblica, quale organo di controllo parlamentare.

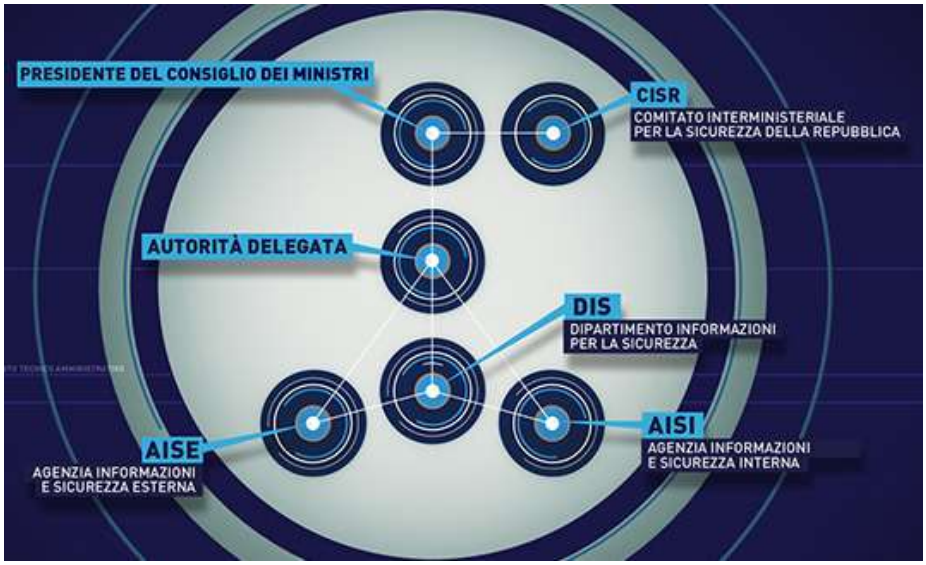


Fig. 3.6-1

La figura evidenzia le due Agenzie operative, l'**AISI** per l'intelligence in ambito interno al paese, e l'**AISE** per l'intelligence in ambito esterno, quindi all'estero negli altri paesi europei e non. A quest'ultima fanno riferimento, quando operano all'estero, anche gli organismi militari italiani di intelligence.
Questa logica di centralizzazione decisionale è stata applicata dal Governo anche con la creazione dell'**Agenzia Cybersicurezza Nazionale, ACN**, con compiti di resilienza e sicurezza in ambito informatico, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, e assicura il coordinamento tra i soggetti pubblici coinvolti nella materia (https://www.acn.gov.it/). E' bene evidenziare come ACN non si occupa di intelligence (compito del DIS) o di contrasto al cybercrime (compito di Polizia di Stato e altre forze dell'ordine), ma coordina e si interfaccia con queste realtà per assicurare un approccio integrato.
Ad ACN rispondono i seguenti principali enti interni:

- **CSIRT**, Computer Security Incident Response Team Italia (https://csirt.gov.it/). E' significativo il ruolo dello CSIRT soprattutto per il monitoraggio degli incidenti a livello nazionale ed i relativi interventi,

l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate, la pubblicazione delle Guide CSIRT su possibili vulnerabilità ed attacchi, ultimamente in particolare su ransomware, si veda https://www.acn.gov.it/portale/csirt-italia/pubblicazioni

- **CVCN,** Centro di Valutazione e Certificazione Nazionale, che ha il compito di valutare la sicurezza di beni, sistemi e servizi ICT destinati a essere impiegati nel contesto del perimetro di sicurezza nazionale cibernetica e che rientrano nelle categorie previste dal DPCM 15 giugno 2021;
- **NCC-IT,** Centro Nazionale di Coordinamento Italiano, supporta l'europeo ECCC nella sua missione di potenziamento dell'autonomia strategica dell'UE e funge da punto di contatto tra la "community" nazionale degli stakeholders attivi nel settore della cybersicurezza e l'ECCC;
- **NCS**, Nucleo per la cybersicurezza: ha funzioni di prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento;
- **OCSI,** Organismo di Certificazione della Sicurezza Informatica: istituito fin dal 2003 ed operante sotto l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero delle Comunicazioni, poi accorpato nel Ministero dello Sviluppo Economico (oggi MIMIT - Ministero delle Imprese e del Made in Italy), si avvale di una rete di Laboratori per la Valutazione della Sicurezza (LVS), abilitati dall'OCSI stesso.

A livello militare la struttura operativa è il **COR**, **Comando Operazioni in Rete**: sotto la supervisione dello Stato Maggiore della Difesa (SMD), coordina le attività di sicurezza e difesa cibernetica delle Forze Armate e del Ministero della Difesa (https://www.difesa.it/smd/cor/la-missione-e-i-compiti/32647.html).

A livello di contrasto dei crimini e delle frodi informatiche operano le strutture già esistenti:

- **Polizia Postale e per la Sicurezza Cibernetica**: preposta al contrasto delle frodi postali e del crimine informatico (https://www.commissariatodips.it/)
  - **C.N.A.I.P.I.C**, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (https://www.commissariatodips.it/profilo/cnaipic/index.html)
- **NSTPFT,** Nucleo Speciale Tutela Privacy e Frodi Tecnologiche: Reparto Speciale della Guardia di Finanza che si occupa di contrastare le frodi telematiche ed informatiche, nonché tutelare la privacy (https://www.gdf.gov.it/it/reparti-del-corpo/lazio/roma/nucleo-speciale-tut.priv-frodi-tec-roma)

A livello dell'Unione Europea (UE) due sono i principali organismi per la sicurezza digitale:

- **CRRT**, Cyber Rapid Response Teams and mutual assistance in cyber security (https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/#:~:text=Cyber%20Rapid%20Response%20Teams%20(CRRTs,operations%20as%20well%20as%20partners), nell'ambito di PESCO, Permanent Structured Cooperation, per migliorare la difesa anche cibernetica dei vari paesi membri dell'UE;
- **ECCC**, European Cybersecurity Competence Centre and Network (https://cybersecurity-centre.europa.eu/): ha il compito di potenziare l'autonomia strategica e le capacità tecnologiche dell'UE in materia di cybersicurezza, di aumentare la competitività del settore industriale europeo e di gestire gli investimenti nei programmi Digital Europe e Horizon Europe;
- **ENISA**, European Union Agency for Cybersecurity: ha l'incarico di di creare le condizioni per un elevato livello comune di cibersicurezza in tutta l'Unione Europea. Si focalizza in particolare su: sensibilizzazione e responsabilizzazione delle comunità europee, politiche di cybersecurity, cooperazione operativa, rafforzamento delle capacità, soluzioni affidabili, previsioni (https://www.enisa.europa.eu/about-enisa/about/it).

A livello mondiale un ruolo importante potrebbe essere tenuto dalle **Nazioni Unite**, https://www.un.org/: il Comitato intergovernativo delle Nazioni Unite di esperti l'8 agosto 2024 ha approvato all'unanimità la

Convenzione contro la Criminalità Informatica e questa convenzione è stato approvata formalmente dall'Assemblea Generale il 24 dicembre 2024 tramite la risoluzione 79/243 (https://docs.un.org/en/A/RES/79/243).
La convenzione è il primo trattato globale completo sul tema e mira a rafforzare la cooperazione internazionale per prevenire e combattere in modo più efficace ed efficiente la criminalità informatica. Il condizionale usato all'inizio è necessario in quanto questa approvazione, che ha richiesto più di 5 anni di lavoro, è solo il primo passo. Per entrare in vigore, la convenzione deve essere ratificata da almeno 40 Paesi firmatari. E' prevista la firma in una cerimonia ufficiale che si terrà ad Hanoi, in Vietnam, il 25 e 26 ottobre 2025. Poi gli Stati firmatari dovranno adattare il loro diritto interno per allinearlo agli obiettivi della Convenzione, inclusa l'istituzione di misure per l'accesso ai dati e la cooperazione tra autorità. Inoltre gli Stati firmatari dovranno assicurare che l'implementazione della convenzione nei loro paesi sia compatibile con i diritti umani e il diritto internazionale.

Questo lungo e complesso processo per raggiungere obiettivi che per l'autore sono ovvi evidenzia come ben difficilmente delle "leggi" sovranazionali, o addirittura universali, possano effettivamente contrastare una criminalità digitale, in taluni casi finanziata e supportata da alcuni stati, capace di operare a livello mondiale sfruttando le più avanzate tecnologie digitali in tempi brevissimi in una logica, dal suo punto di vista, di "time to market".

Sempre a livello internazionale la crescente importanza della **NATO**[42] nella sicurezza digitale: riconosce il cyberspazio come un dominio strategico, e la difesa informatica è parte integrante del compito fondamentale della NATO in materia di deterrenza e difesa. investe fortemente nel settore, supporta e promuove la collaborazione tra i paesi membri, la condivisione di informazioni, lo sviluppo di capacità di risposta rapida come il Virtual Cyber Incident Support Center (VISIC). Nella sua struttura organizzativa ha creato il **Joint Warfare Centre** (**JWC**): è il punto focale dell'addestramento della NATO per la guerra congiunta a spettro completo, sia operativa che strategica. Come parte della Struttura di Comando NATO, il JWC supporta direttamente le missioni del Comandante Supremo Alleato per la Trasformazione (SACT) e del Comandante Supremo Alleato in Europa (SACEUR). Il Centro contribuisce alla prontezza operativa complessiva del Comando e della Struttura di Forza NATO e, su richiesta, dei Quartier Generali Nazionali e/o NATO impegnati in operazioni.

Da evidenziare l'importante lavoro svolto e messo a disposizione gratuitamente e tempestivamente da **agenzie ed enti statunitensi**, tra le quali il ben noto **NIST**, la Fondazione **MITRE**, che ha realizzato e gestisce la banca dati CVE, **CISA**, Cybersecurity and Infrastructure Security Agency (https://www.cisa.gov/) che gestisce la banca dati KEV, Known Exploited Vulnerabilities, che è il sottoinsieme delle vulnerabilità elencate in CVE e che sono usate negli attacchi, **FIRST**, Forum of Incident Response and Security Teams (https://www.first.org/).

3.7 Le leggi italiane in vigore per la sicurezza digitale

Per concludere l'inquadramento della sicurezza digitale in Italia è opportuno fornire qualche indicazione sulla normativa vigente, che è complessa e assai articolata.
La legislazione sulla sicurezza e sul crimine informatico in Italia ha iniziato ad apparire nei primi anni 90 del secolo scorso, con l'introduzione della Legge 547/1993 sul crimine informatico.

[42] NATO, è l'Organizzazione del Trattato dell'Atlantico del Nord, un'alleanza politica e militare intergovernativa fondata nel 1949 con il Trattato di Washington, che conta 32 paesi membri provenienti da Europa, Nord America e Vicino Oriente. Il suo scopo è garantire la libertà e la sicurezza dei propri membri attraverso strumenti politici e militari, basandosi sulla difesa collettiva: un attacco contro uno Stato membro è considerato un attacco contro tutti (Articolo 5).

Sono poi seguite varie leggi, decreti legislativi e DPCM[43], alcuni dei quali sono aggiornamenti di precedenti normative, o normative nazionali per le Direttive UE.
Norme di riferimento per la sicurezza digitale sono poi incluse in diverse altre normative, sia per specifici settori merceologici, quali ad esempio le telecomunicazioni, le banche, le assicurazioni, e le Pubbliche Amministrazioni, sia per specifiche tematiche quali ad esempio la privacy, il documento informatico, la firma elettronica e digitale, il diritto d'autore e la tutela del software.

La maggior parte delle normative italiana sulla sicurezza digitale rientrano nel codice civile, ma alcuni **reati informatici sono sanzionati anche a livello di codice penale**: si vedano ad esempio gli art. 392, 420, 491bis, 615, 616, 617, 621, 623bis, 635, 640 del Codice Penale.

La Legge del 28/06/2024 n. 90 - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, modifica il Codice Penale, introducendo il reato di "estorsione mediante attacco informatico": il riferimento all'ampiezza del fenomeno dei ransomware in Italia è evidente.

In estrema sintesi, dato che ogni approfondimento sulla normativa italiana esulerebbe dall'indagine OAD e dal presente Rapporto, a giudizio dell'autore le norme cardine, a livello generale e più recenti per la sicurezza digitale in Italia includono:

- La **Strategia Nazionale di Cybersicurezza 2022 – 2026**, si veda https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza, volta a pianificare, coordinare e attuare misure tese a rendere il Paese più sicuro e resiliente con il raggiungimento di 82 misure entro il 2026.
- Il **Perimetro nazionale di sicurezza cibernetica** (D.L. 105/2019 convertito con modificazioni dalla L. 18 novembre 2019, n. 133), cui si associa il relativo **Regolamento** (con il DDPCM 30 luglio 2020)**,** volto ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato.
- **Recepimento della Direttiva UE NIS 2 - 2022/2555** (D.Lgs. 4 settembre 2024 , n. 138).
- La già citata **Legge del 28/06/2024 n. 90** - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

[43] Una "legge" è un atto normativo del Parlamento. Un "decreto legge", D.L., è un atto normativo "urgente" emanato dal Governo, che deve essere approvato e convertito in legge dal Parlamento entro 60 giorni. Un "decreto legislativo", D.Lgs., è una "delega" del Parlamento al Governo per l'emanazione di leggi, tipicamente complesse ed articolate. Un DCPM è un Decreto del Primo Ministro.

4. Gli attacchi digitali in Italia dall'indagine OAD 2025

Il questionario OAD 2025 ha posto due sole domande sugli attacchi digitali subiti nel 2024 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, ed ha approfondito gli attacchi digitali rilevati nel 2024:

- alle applicazioni ed agli ambienti web;
- ai sistemi OT, Operation Technology;
- agli ambienti che utilizzano sistemi di Intelligenza Artificiale.

La fig. 4-1 mostra che il **71,18%** delle aziende/enti rispondenti ha rilevato attacchi intenzionali nel 2024, e conferma il gran numero di attacchi digitali portati ai Sistemi Informativi (SI) delle aziende/enti rispondenti.

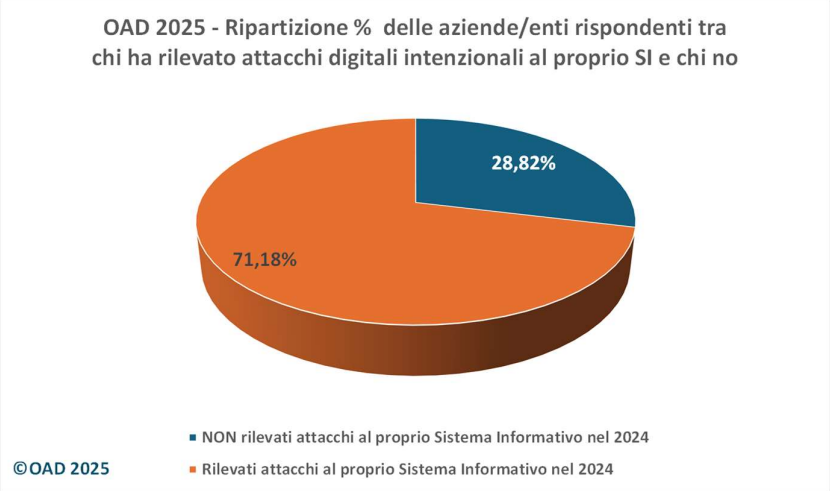


Fig. 4-1

La fig. 4-2 mostra il numero di attacchi rilevati nei diversi Rapporti OAI/OAD **dall'anno 2007 all'anno 2024**.
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 (+/- del 5% circa) del numero di attacchi rilevati rispetto ad un trend che si attesta attorno al 40% dei rispondenti un sali-scendi, evidenziato in figura dalla riga rossa scura. L'onda altalenante 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.
Nel 2017 e nel 2018 la figura evidenzia la **forte crescita** percentuale degli attacchi rilevati, che nel 2018 con il primo picco di 55,7%, porta la percentuale di attacchi rilevati a superare, e per più di 10 punti, la percentuale di quelli non occorsi/rilevati. Nel 2019 il trend di crescita dei precedenti tre anni si arresta, con una diminuzione al 46,6%, confermando ancora il trend di rafforzamento delle misure di sicurezza dopo una fase di maggiori e più sofisticati attacchi.

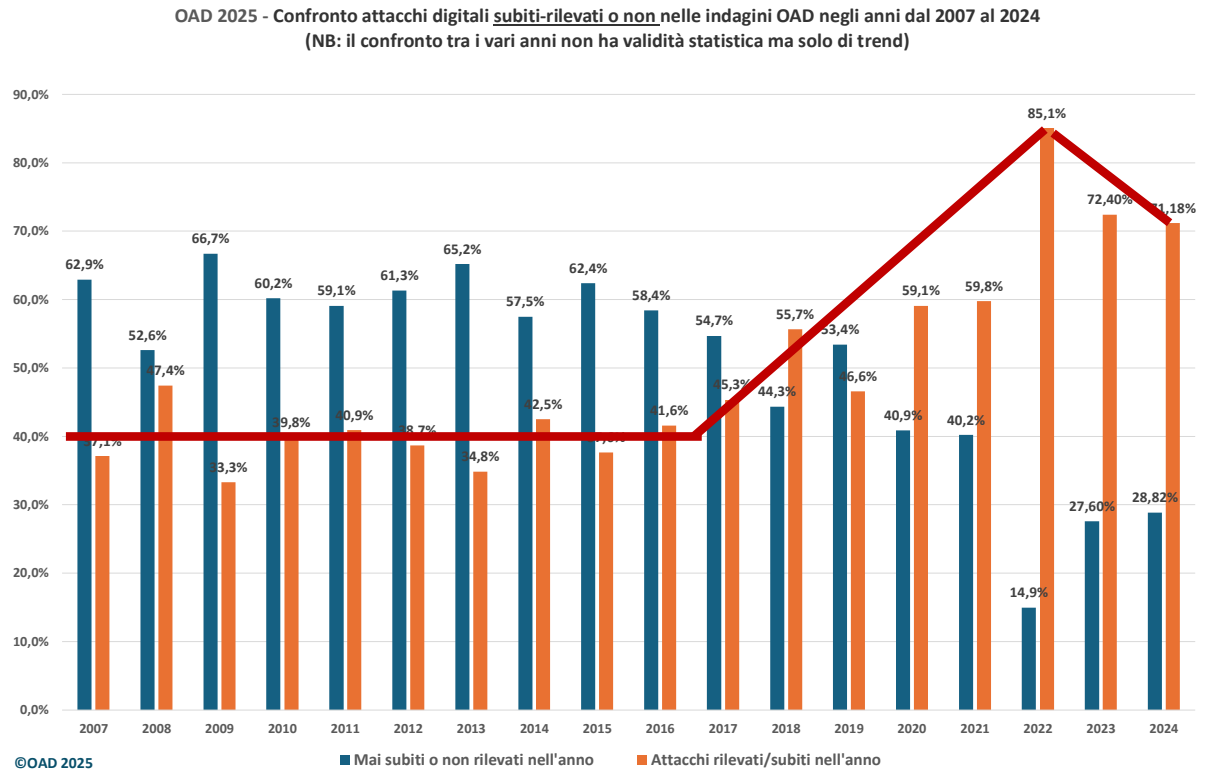


Fig. 4-2

Nel 2020 e nel 2021, nel campione dei rispondenti, la percentuale di chi ha rilevato attacchi cresce ancora avvicinandosi al 60%. Nel 2022 si rileva un vero e proprio balzo all'**85,1%** dei SI dei rispondenti che hanno rilevato attacchi, con un delta tendenziale di poco più del 25%. Nel 2023 si ha una riduzione di tale percentuale al **72,4%**, percentuale sempre molto alta, che continua anche nel 2024 con un **71,18%.**

Nella fig. 4-2 la riga rosso scuro evidenzia nei 18 anni di indagine OAD il mega trend degli attacchi subiti. Dal 2020 la percentuale di attacchi rilevati supera sempre, e nettamente, quella di attacchi non subiti, e conferma che **dal 2020** anche in Italia si è entrati nell'**era della insicurezza digitale sistemica** (**systemic cyber insecurity**). 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.
Le piccole e piccolissime organizzazioni nella maggior parte dei casi non hanno, e non possono avere, competenze e capacità economiche per acquisire e gestire gli strumenti di sicurezza digitale, tecnici ed organizzativi, necessari; ma esse non rappresentano un obiettivo di interesse specifico per i cyber criminali, soprattutto per gli attacchi mirati (targeted attack), mentre esse possono essere coinvolte in attacchi di massa, come quelli basati sul phishing e sul ransomware, così come avviene tipicamente o per cogliere qualcuno nella massa, o per azioni di attivismo o di terrorismo informatico.

Questo è confermato analizzando la fig. 4-3 che mostra la distribuzione percentuale degli **attacchi NON subiti** nel 2024 per dimensione (numero di dipendenti) delle aziende/enti rispondenti (si veda §6.1 e in particolare

fig. 6.1-2). La linea verde nella figura evidenzia come le organizzazioni dimensionalmente **più piccole** sono quelle che hanno subito/rilevato **meno attacchi digitali**. Logica e tendenza anche nelle precedenti indagini OAD: gli attacchi digitali, soprattutto quelli mirati ad una specifica impresa, o a un gruppo similare di imprese (attacchi "targeted"), sono effettuati prevalentemente a organizzazioni di grandi dimensioni, ben note come brand, e con un grande giro d'affari.

Alcune grandi organizzazioni rispondenti hanno dichiarato di non aver subito/rilevato attacchi: la maggior parte di esse ha SI con elevatissimi livelli di sicurezza, che plausibilmente hanno respinto e/o scoraggiato gli attacchi digitali. Per le misure di sicurezza dei SI dei rispondenti si rimanda al Capitolo 7.
Come già indicato in precedenza, per una corretta interpretazione delle correlazioni elaborate per produrre questa figura che correla dati relative a diverse domande, si deve tener conto che le percentuali emerse dipendono e sono influenzate anche dal numero di risposte ricevute: quello che interessa all'indagine OAD è evidenziare un determinato fenomeno, i numeri delle percentuali che emergono fanno solo riferimento al bacino di rispondenti. *Si deve tener conto di questo aspetto per tutte le figure che correlano dati nel presente rapporto.*

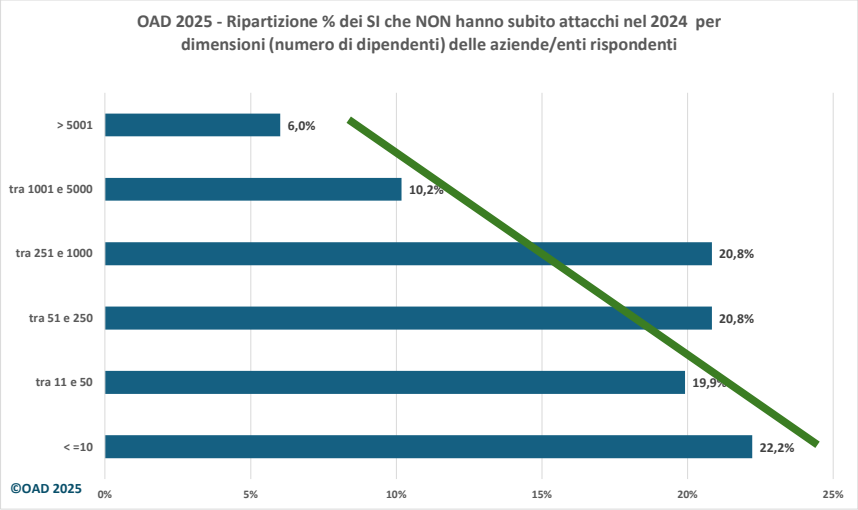


Fig. 4-3

4.1 Tipologie e tecniche di attacco emerse da OAD 2025

La fig. 4.1-1 mostra la **diffusione**, in percentuale, dei diversi **tipi di attacchi** subiti e rilevati tra il bacino di aziende/enti rispondenti. Come precisato nell'Allegato A, OAD nettamente distingue "**il che cosa si attacca"** (indicata come "tipologia di attacco") dal **come si attacca** (indicata come "tecnica di attacco").

L'indagine OAD 2025 ha considerato nel questionario 16 diverse "famiglie di tipologie": queste "famiglie" o gruppi di attacco simili, consentono di non chiedere troppi dettagli e semplificare la scelta di chi compila il questionario.
OAD 2025 ha introdotto una nuova tipologia di attacco, rispetto a quelle considerate negli anni precedenti, relativa agli **attacchi alle applicazioni e agli ambienti del SI basati su IA, Intelligenza Artificiale.**

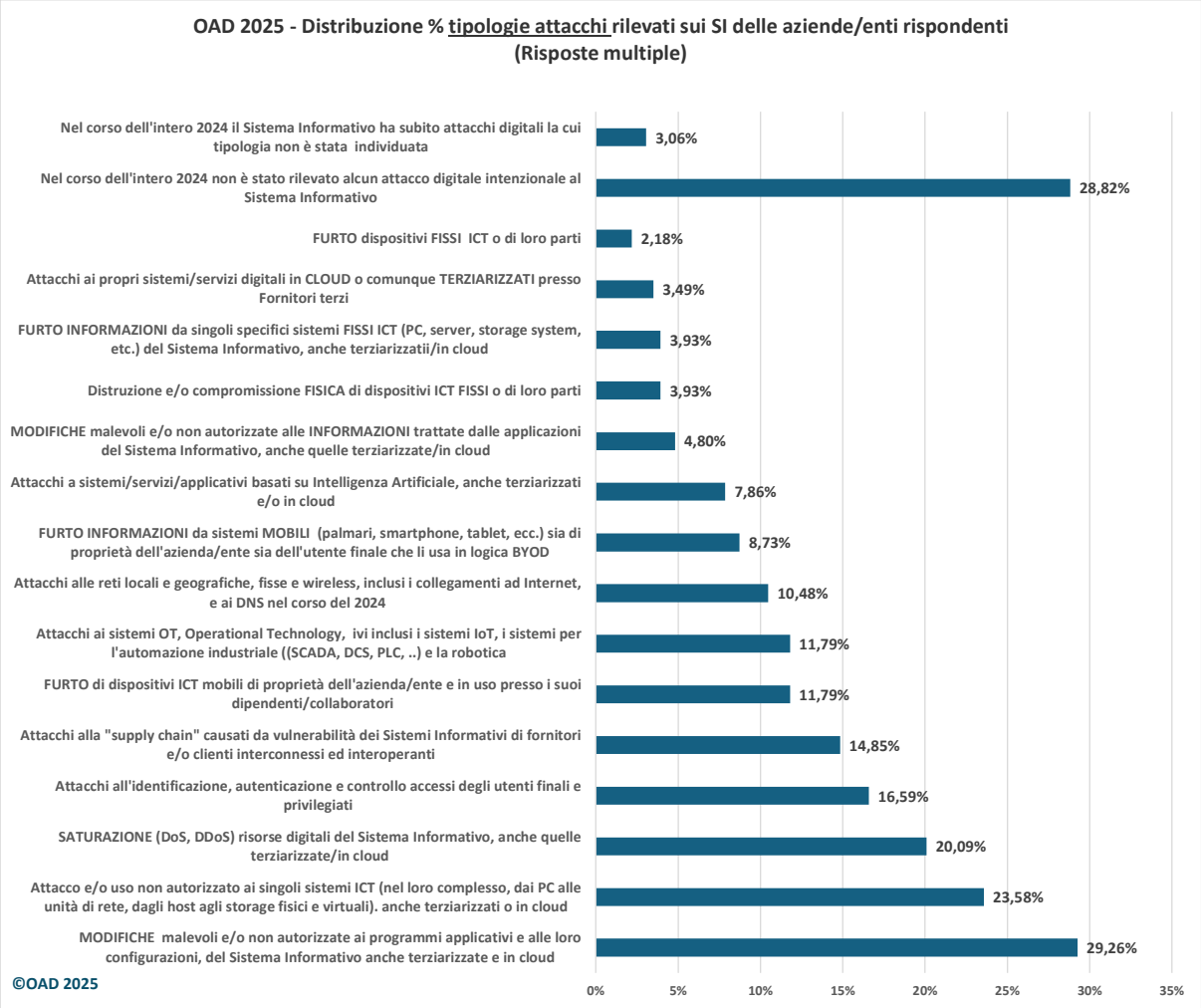


Fig. 4.1-1

La fig. 4.1-1 mostra che il **28,82%** dei SI delle aziende/enti rispondenti non ha riportato/rilevato attacchi digitali, come già analizzato in §4, e che il **3%** , pur avendo rilevato attacchi digitali, non li ritiene inquadrabili nelle tipologie considerate (ma non sono ste fornite indicazioni in merito negli spazi disponibili nel questionario per commenti).

La tipologia di attacco più diffusa tra i rispondenti, con un **29,26%,** riguarda le **modifiche malevoli/non autorizzate ai programmi e alle configurazioni dei sistemi ICT,** analogamente alle ultime edizioni dell'indagine OAD. A questo primo posto sicuramente contribuisce la larghissima diffusione di malware e di ransomware in Italia, confermata anche dai molti commenti in merito inseriti nelle risposte sulle tipologie di attacco rilevate.

Al secondo posto di diffusione, con un **23,58%**, gli attacchi digitali per **l'uso non autorizzato di sistemi ICT nel loro complesso**. Seguono con un **20,09%** gli attacchi **DoS/DDoS**, che come si è visto in §3, sono stati uno dei mezzi più usati nell'ambito delle cyber warfare, in particolare da parte delle organizzazioni hacker schierate pro Russia.

Al quarto posto **gli attacchi ai sistemi di identificazione, autenticazione e controllo accessi** degli utenti finali e privilegiati, con un **16,59%**.

Gli attacchi alla **supply chain informatizzata,** con un **14,85%,** si posizionano in questa edizione al quinto posto come diffusione**,** a conferma della criticità di questa tipologia d'attacco, considerata uno dei principali rischi a livello mondiale (si vedano le previsioni del World Economic Forum in §3).
Il **furto di dispositivi mobili**, in particolare gli smartphone, rimane un fenomeno significativo, con un **11,79%**: in essi non solo sono normalmente contenute tutte le password e le modalità di accesso ai servizi informatici utilizzati, come gli account di posta elettronica ed i conti in banca (e talvolta tali dati non sono protetti nel dispositivo, tutti i dati basilari per furti, frodi e furti di identità digitali, ma lo stesso dispositivo ha sovente un alto valore sul mercato dell'usato.
Per gli attacchi ai sistemi OT e a quelli basati su Intelligenza Artificiale si rimanda agli approfondimenti in §4.3 e §4.4 rispettivamente.
Un importante dato da segnalare in questa figura: la diffusione nel 2024 di **attacchi ai propri sistemi/servizi digitali in cloud o comunque terziarizzati** presso Fornitori terzi è molto bassa, con un **3,49%**.
Questo significa che i sistemi ICT terziarizzati, tipicamente gli applicativi in hosting e/o cloud, hanno mediamente elevati livelli di sicurezza.

La fig. 4.1-2 mostra la **diffusione**, in percentuale, delle **tecniche di attacco** riscontrate nei più gravi attacchi subiti nel corso del 2024.

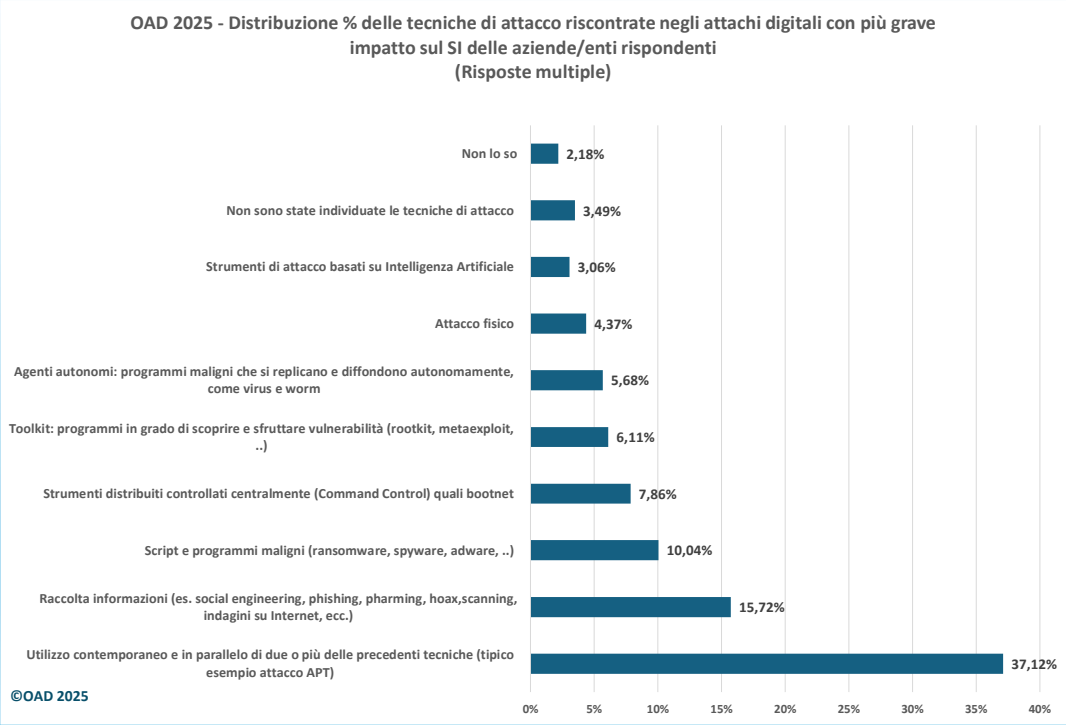


Fig. 4.1-2

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 2025 di fare riferimento **al più grave attacco subito**; e tale logica è applicata a numerose altre domande di approfondimento sugli attacchi trattati nel seguito per gli ambienti web, OT e IA approfonditi nei prossimi paragrafi.

Dalla fig. 4.1-2 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.
L'uso di **più tecniche per lo stesso attacco** risulta il metodo percentualmente più diffuso, con un **37,12%**. 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 email 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, con un **15,72%**, la **raccolta illegale di informazioni**, ottenute tipicamente con il **social engineering**, sfruttando la poca attenzione del soggetto interlocutore. Al terzo posto, con il **10,04%,** i **codici maligni**, alla base degli assai diffusi attacchi di ransomware.

E' opportuno ricordare nuovamente che i dati emersi dall'indagine OAD 2025 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 dei loro impatti

4.2 Gli attacchi digitali alle applicazioni ed agli ambienti web in Italia

Come già sottolineato nei precedenti capitoli, l'indagine OAD 2025 ha effettuato, come nelle due precedenti edizioni, un'indagine "verticale" sugli **attacchi digitali in ambiti web**, che costituiscono ormai nei sistemi informativi la maggior parte degli ambiti applicativi, e per questo motivo, essendo esposte in Internet, attirano gran parte degli attacchi, sia di tipo target sia di tipo massivo.
Già con OAD 2017 era stata effettuata un'indagine "verticalizzata" sugli attacchi agli applicativi, ripresa e citata da AGID[44], e le indagini sugli attacchi ai sistemi web di OAD del 2025 e dei precedenti anni possono essere considerate un suo parziale aggiornamento.
La fig. 4.2-1 mostra in % quanti dei SI delle aziende/enti rispondenti **utilizza soluzioni web**, sia in locale che terziarizzate. La stragrande maggioranza, il **94,15%** li usa, mentre quasi un **6%** dichiara di non usarli. Salvo eventuali errori da parte di chi ha compilato il questionario, questa piccola percentuale fa riferimento a micro imprese che utilizzano applicativi solo in locale su propri PC , al massimo connessi un LAN, ma senza servere senza neppure utilizzare applicativi in cloud SaaS, Software as a Service.
La fig. 4.2-1 mostra se i SI che utilizzano sitemi web sono stati attaccati intenzionali nel 2024, dettagliando anche (con risposte multiple) quali sistemi web sono stati attaccati, a seconda della loro modalità di gestione, in locale (on premise) o terziarizzati. Il **68,94%** dei rispondenti hanno rilevato nel 2024 attacchi alle applicazioni ed agli ambienti web dei propri SI; di questi il **30,43%** ha rilevato attacchi ai propri sistemi web

[44] Il Rapporto 2017 OAD è scaricabile gratuitamente da https://www.oadweb.it/it/rapporti-e-relativi-convegni/2017.html.
I dati emersi da questo Rapporto sono stati citati e considerati nelle Linee guida AgID per la sicurezza del software, si veda Cap 5 di https://www.agid.gov.it/sites/default/files/repository_files/documentazione/linee_guida_per_la_configurazione_per_adeguare_la_sicurezza_del_software_v1.0.pdf

gestiti internamente, mentre il **11,18%** li ha subiti nei propri ambienti web **in cloud**, e il **8,7%** in quelli in hosting. La forte differenza % indica come la gestione di sistemi web in locale è il più delle volte meno sicura degli ambienti terziarizzati. Ma anche sistemi terziarizzati presso fornitori di alto livello, anche per la sicurezza digitale, possono essere attaccati digitalmente, con seri impatti sui sistemi dei clienti.
Si noti che l'autore volutamente non ha considerato sistemi web in housing, perché questi sono gestiti direttamente dall'azienda/ente proprietaria, ed il fornitore fornisce solo il posto dove porre l'hardware dei sistemi e le facility di supporto (alimentazione elettrica, aria condizionata, etc.): i sistemi in housing sono quindi gestiti dall'azienda/ente proprietaria, e sono di fatto equivalenti ad una gestione in locale.

La fig. 4.2-3, con risposte multiple, mostra la diffusione in percentuale di quali siano state le **vulnerabilità probabilmente sfruttate per l'attacco più critico rilevato** (o quelli più critici rilevati). Come già indicato in §3 e in §4.1, gli attacchi digitali odierni sfruttano più vulnerabilità, sia quelle tecniche che quelle personali e dell'organizzazione, e sono in grado, nel corso dell'attacco stesso, di cambiare l'obiettivo sulle risorse del sistema informativo bersaglio di maggior valore, per l'attaccante, e con minori difese.
Dalla figura emerge che le **vulnerabilità tecniche** sono state (stimate) assai più diffuse tra i rispondenti, **con un 93,83%**, rispetto a **quelle personali**, che in parte dipendono anche dall'organizzazione (ad esempio dalla non formazione degli utenti sia finali sia privilegiati), che ammontano a **44,44%**.

Fig. 4.2-1

Tra le vulnerabilità tecniche, al primo posto si posizionano quelle delle **piattaforme web di supporto,** che il più delle volte influiscono molto sul corretto funzionamento di una applicazione web supportata. Le **vulnerabilità specifiche ed intrinseche** di una applicazione web si collocano al secondo posto, con un **40,74%**. Le **vulnerabilità dei dispositivi d'utente** che si interfacciano ed interagiscono con gli ambienti web, hanno un **8,64**%, assai basso rispetto alle due altre vulnerabilità tecniche.

Tra le vulnerabilità personali, quella **dell'utente privilegiato**, con il **29,63%**, sono praticamente il doppio, in %, di quelle dell'**utente finale**, con il **14,81%**. Anche questo è un importante indicatore di come il ruolo di un utente privilegiato, tipicamente un amministratore di sistema o un sistemista, sia particolarmente cruciale per la sicurezza digitale.

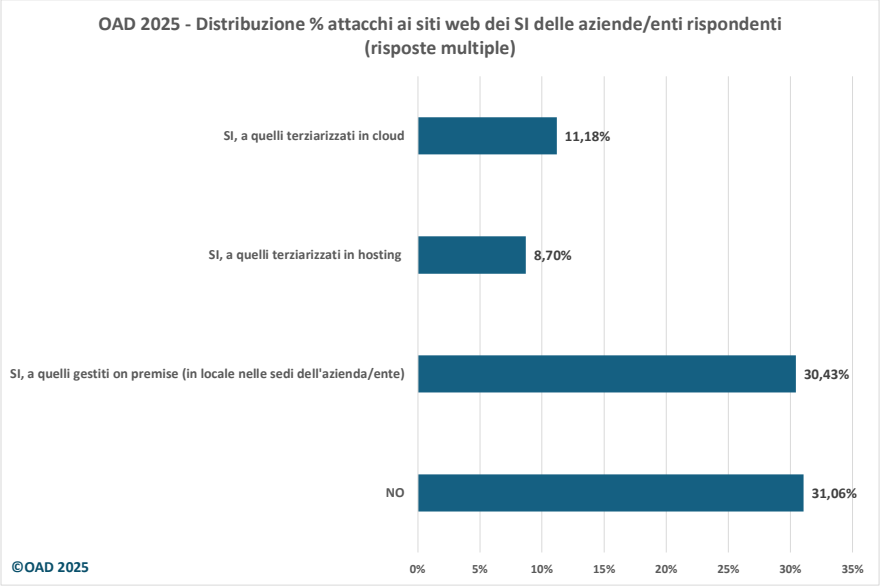


Fig. 4.2-2

A distanza di otto anni dal precedente Rapporto 2017 OAD sulla sicurezza degli applicativi (web e non), le ***vulnerabilità intrinseche dell'applicazione e delle piattaforme*** *su cui poggiano hanno ancora valori percentuali alti. Applicazioni e soprattutto le piattaforme di supporto non sono ancora sufficientemente sicure, anche se ormai esse sono fornite e gestite nella maggior parte dei casi dai provider in hosting e/o in cloud, che dovrebbero erogare e garantire alti livelli di sicurezza ed affidabilità.*

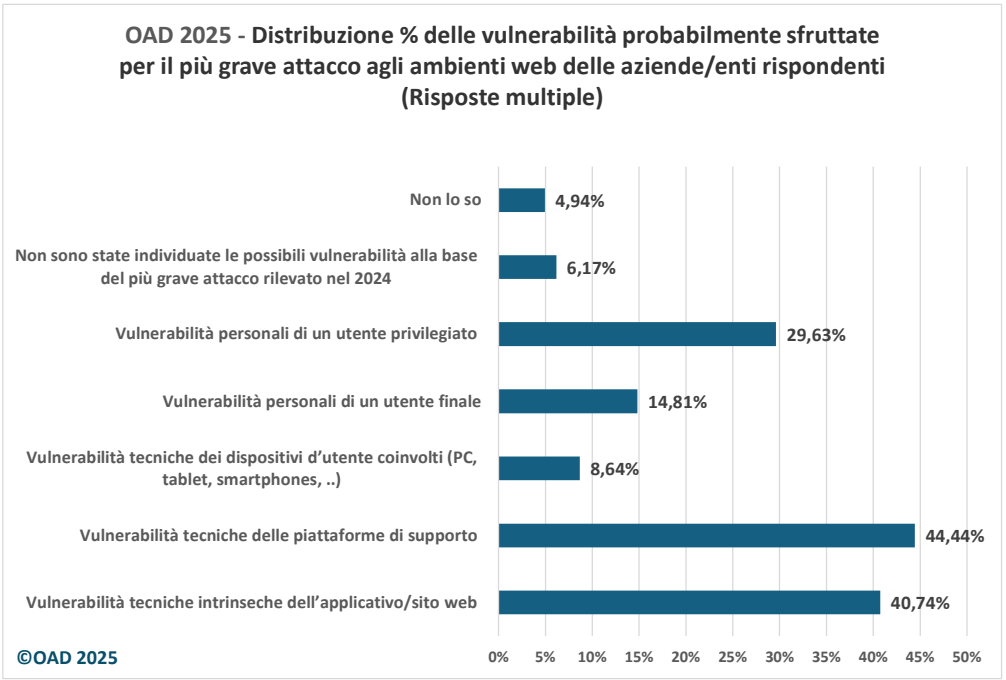


Fig. 4.2-3

Sulle vulnerabilità tecniche degli ambienti web, il questionario OAD 2024 ha posto una domanda tecnica di dettaglio, basata sui risultati delle analisi **OWASP**[45] a livello mondiale, sempre in riferimento all'attacco più grave e critico rilevato nel 2023 agli ambienti web del SI delle aziende/enti rispondenti. Come mostrato in fig. 4.2-4 si è fatto riferimento alle **OWASP Top Ten: le 10 principali vulnerabilità tecniche** per attacchi digitali nel mondo web (si veda https://owasp.org/Top10/it/).
La fig. 4.2-4 elenca tali vulnerabilità nell'ordine di diffusione "mondiale", dal più diffuso al meno tra i 10 "top".

Nome vulnerabilità	Breve spiegazione	Dettagli OWASP
Broken Access Control	Per superare in maniera non autorizzata, e quindi illegale, il controllo dell'accesso alle applicazioni e ai dati da queste trattate.	https://owasp.org/Top10/A01_2021-Broken_Access_Control/
Cryptographic Failures	Errori/caduta/superamento delle tecniche crittografiche	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/
Injection	Vari tipi di "punture" ed inserimenti non autorizzati: dai comandi al sistema operativo all'interfacciamento a banche dati (Sql, NoSql), a LDAP, etc., prevalentemente causati da errori/cattiva programmazione	https://owasp.org/Top10/A03_2021-Injection/
Insecure Design	Progettazione non sicura	https://owasp.org/Top10/A04_2021-Insecure_Design/
Security Misconfiguration	Cattiva o incompleta configurazione dei sistemi e degli strumenti di sicurezza	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
Vulnerable and Outdated Components	Componenti non aggiornati e quindi vulnerabili	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
Identification and Authentication Failures	Errori/caduta/superamento delle misure di identificazione ed autenticazione	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/
Software and Data Integrity Failures	errori e malfunzionamenti del software e dell'integrità dei dati trattati.	https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/
Security Logging and Monitoring Failures	Errori, malfunzionamento e caduta degli strumenti di monitoraggio e di logging	https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/
Server-Side Request Forgery	Falsificazione di richieste lato server	https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/

Fig. 4.2-4 (fonte: OWASP)

La fig. 4.2-5, con risposte multiple, riporta la **diffusione** percentuale tra i rispondenti a OAD 2025 dello sfruttamento (probabile) delle **Top Ten vulnerabilità elencate da OWASP** nell'attacco più grave agli ambienti web dei loro SI.

[45] OWASP, Open Web Application Security Project, iniziativa che formula a livello mondiale linee guida, strumenti e metodologie per migliorare la sicurezza delle applicazioni in ambito web. (https://owasp.org/),

La vulnerabilità in testa a questa classifica per il bacino di rispondenti 2025 che hanno rilevato attacchi ai sistemi web del loro SI, è quella dei **componenti software non aggiornati o obsoleti, con il 39,51%**, cui segue, con il **30,86%**, **l'errata configurazione** degli strumenti di sicurezza.
Si noti come queste due vulnerabilità dipendono da errati comportamenti di utenti previlegiati quali l'amministratore di sistema, i sistemisti, i fornitori dei prodotti, oltre al CISO ed al CIO. Una conferma della criticità dei ruoli degli utenti privilegiati.

Al terzo posto, con il **25,93%**, la perforazione delle **misure di identificazione ed autenticazione**.
A scalare, ma con percentuali molto minori, le altre vulnerabilità "top" indicate da OWSAP.
Per il **13,58%** dei rispondenti la vulnerabilità causa dell'attacco più grave ai sistemi web non rientra tra le top ten OWASP. Infatti alcuni diffusi attacchi, quali ad esempio il DDoS/DoS, non hanno bisogno di alcuna vulnerabilità nel software del web e della sua piattaforma, ma solo della mancanza di strumenti atti a bloccare e/o dirottare l'enorme flusso di dati di attacco che satura le linee. Quasi il **10%** indica che non sono stati in grado di individuare le vulnerabilità tecniche causa dell'attacco più grave agli ambienti web dei loro SI.

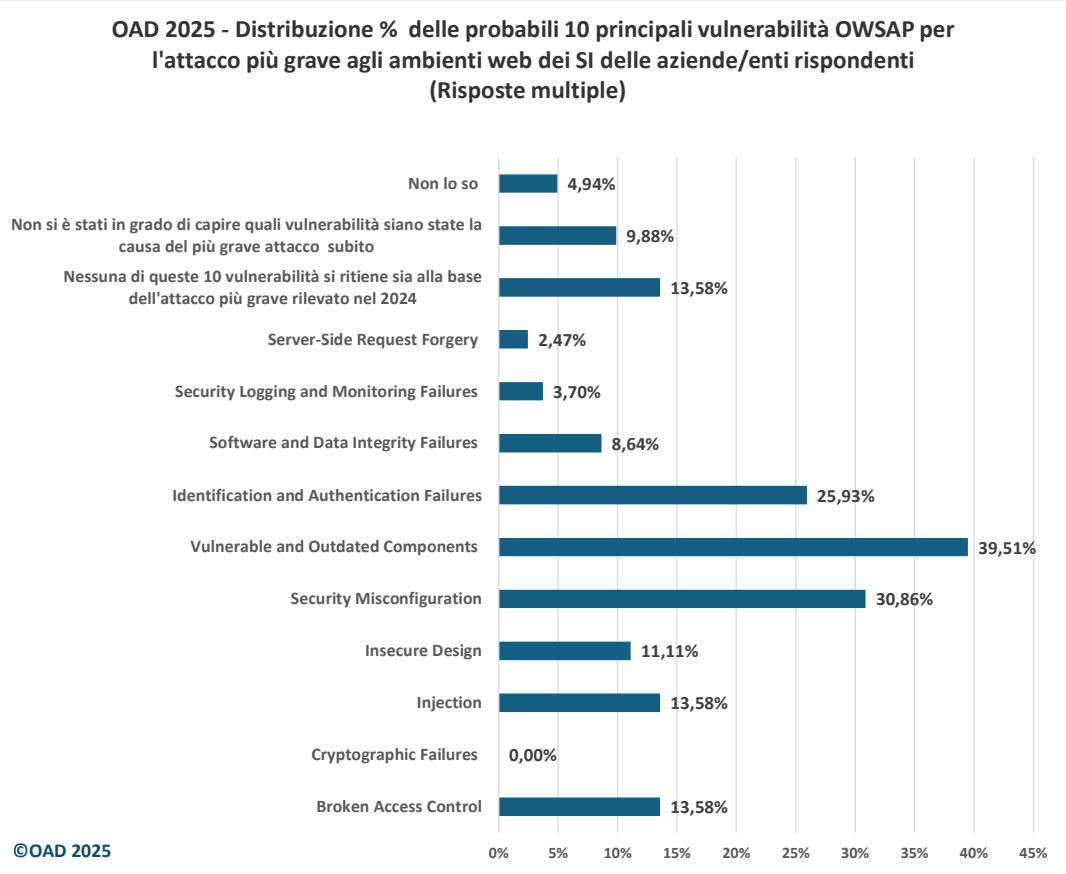


Fig. 4.2-5

Nel complesso quanto emerge dalle risposte a questa domanda è ragionevole, per l'autore, considerando la realtà dei siti web di aziende/enti di ogni dimensione in Italia (ma non solo). Molti siti/applicazioni web utilizzano piattaforme e sistemi opensource non correttamente configurati soprattutto in termini di sicurezza digitale, in taluni casi con l'uso di moduli e componenti obsoleti e non aggiornati. Gli aspetti di sicurezza di un software, se esistenti, sono normalmente da settare a livello di configurazione del software, e spesso sono

lasciati di default per la fretta e/o per la loro non conoscenza; ed il default il più delle volte coincide con il settaggio non attivo dei parametri/misure di sicurezza.

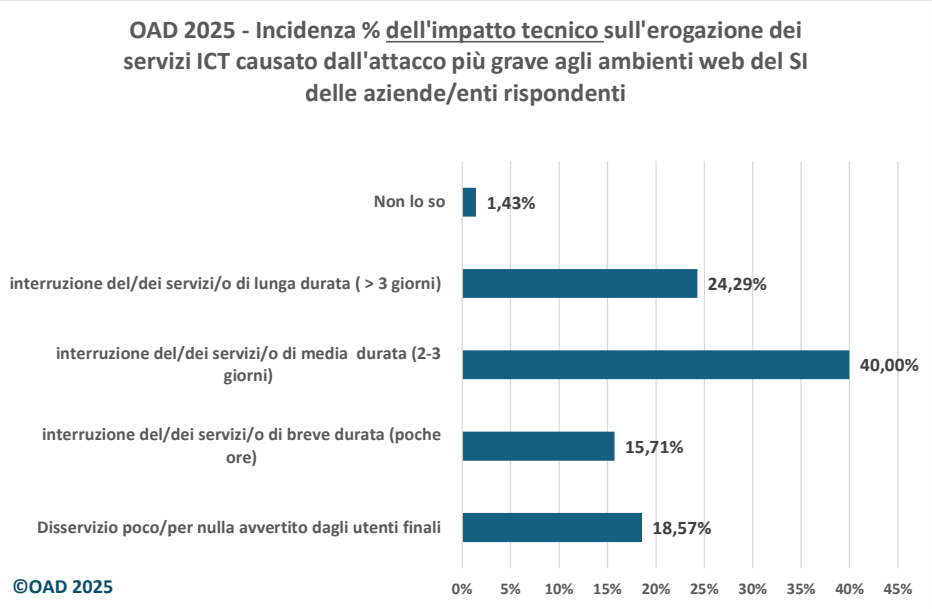


Fig. 4.2-6

Le fig. 4.2-6 e 4.2-7 forniscono precise ed interessanti informazioni sull'impatto tecnico, in termini di disservizio causato, e sull'impatto economico (qualitativo) dell'attacco più critico rilevato nel 2024 in ambito web.

L'**impatto a livello tecnico** dell'attacco più grave è stato **pesante** per i SI delle aziende/enti rispondenti, con il **64,29%** dei casi con un disservizio durato **da 2 giorni in su**.

L'impatto economico, a seguito dell'attacco più grave ai sistemi web, ha causato per il **61,73%** un **aumento dei costi** sul **budget del SI**, e per il **12,35%** ha causato anche il ripercuotersi di questi costi **sul bilancio dell'azienda/ente** vittima.

Significativo il fatto che **nessuno dei rispondenti** che ha subito attacchi ai sistemi web del SI, abbia indicato che il più grave attacco ai sistemi web abbia comportato **un impatto molto significativo sul bilancio** dell'azienda/ente.

Le indicazioni emerse dall'indagine sulla gravità dell'impatto sono qualitative e lasciate all'opinione di chi ha compilato il questionario, ma danno la chiara indicazione che molti degli attacchi subiti hanno causato forti problemi alla funzionalità del SI attaccato, con i conseguenti costi diretti ed indiretti sul budget del SI e, almeno in parte, sul bilancio dell'azienda/ente.

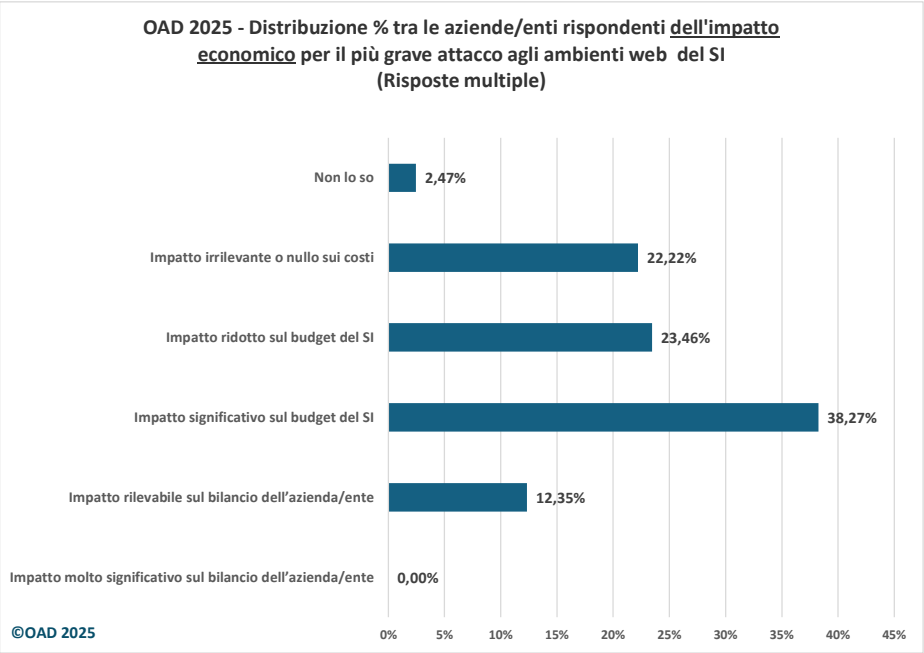


Fig. 4.2-7

La fig. 4.2-8 mostra, con risposte multiple, la distribuzione percentuale delle **probabili motivazioni**, stimate da chi ha compilato il questionario, per l'attacco più grave sui siti e sulle applicazioni web del sistema informativo delle aziende/enti rispondenti.
Al primo posto il **sabotaggio,** che per la prima volta arriva in questa posizione con un **44,44%** e che è considerato come probabile causa soprattutto da piccole imprese e dagli studi professionali, superando percentualmente la **frode** e il **ricatto,** che tradizionalmente si scambiavano il primo posto nelle precedenti edizioni di OAD.
Seguono l'**hactivism** e la **guerra informatica** (cyber warfare) segno che le gravi tensioni geopolitiche approfondite nel Capitolo 3, stanno sempre più impattando i Sistemi Informativi, soprattutto quelli "critici" per il sistema paese.

Il primo posto al sabotaggio significa, secondo l'autore, aver compreso, almeno da parte di chi ha compilato il questionario, l'importanza della continuità operativa delle attività e dei processi di aziende/enti, e come tale continuità si basi ormai soprattutto sulla affidabilità disponibilità e resilienza dei Sistemi Informativi.

I **probabili attaccanti per l'attacco più grave agli ambienti web** del SI delle aziende/enti rispondenti sono mostrati in fig. 4.2-9, con risposte multiple. La stragrande maggioranza delle risposte**, 66,67%,** fa riferimento ad un **attacco dall'esterno**, ossia via Internet e da attaccanti il più delle volte sconosciuti. Al secondo posto, ma con circa il **10%**, gli **"ex dipendenti"**: possono conoscere il SI, essere usciti dall'azienda/ente con rancori, ed essere quindi motivati ad effettuare un attacco digitale, o contribuire ad esso con le loro specifiche conoscenze del SI. Seguono in questa classifica i Clienti ed i Fornitori, che possono aver contribuito, volontariamente o non, ad attacchi soprattutto alla **supply chain** informatica.
Tutti gli altri probabili attaccanti hanno percentuali trascurabili.

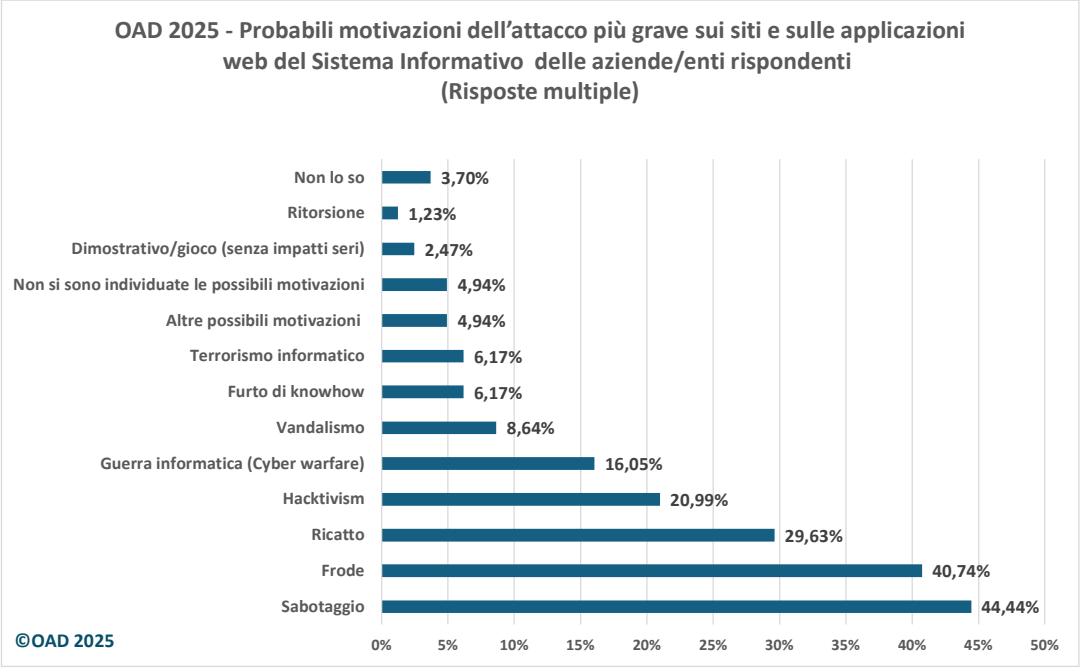


Fig. 4.2-8

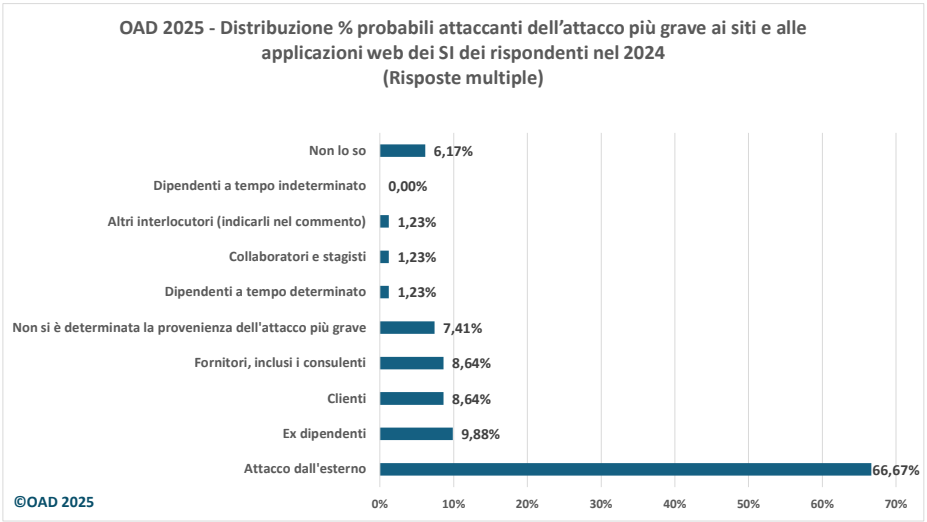


Fig. 4.2-9

.

La fig. 4.2-10, con risposte multiple, mostra la distribuzione percentuale, tra i rispondenti che subito attacchi ai sistemi web del proprio SI, degli **interlocutori esterni all'azienda/ente ai quali si comunica l'attacco subito**, in taluni casi anche per obblighi di legge, ad esempio all'Autorità Garante per la privacy in caso di un data breach su informazioni personali o all'ACN per gli attacchi subiti se si è nell'ambito degli obblighi della NIS2.

Quasi il **60%** dei rispondenti comunica l'accaduto **ai propri fornitori e consulenti** per farsi aiutare nel ripristinare la situazione ex ante l'attacco subito. Quasi un 1**/5 dei rispondenti** comunica l'attacco subito **al Servizio Polizia Postale e per la Sicurezza Cibernetica**. Il **17,28%** lo comunica al **Garante della privacy**, dato che l'attacco ha impattato su dati personali. Una percentuale inferiore di rispondenti, **12,35%,** lo comunica all'**ACN**, in ottemperanza alla normativa NIS2, in quanto gestiscono infrastrutture critiche e servizi essenziali per la nazion. Il **17,28%** non comunica nulla a nessuno, e le motivazioni includono: per il 57,14% perché anche il più grave attacco rilevato non è così significativo e per il 35,71% per la tutela dell' immagine dell'azienda/ente. *Subire un attacco digitale, nella percezione comune, è riprovevole, fa presupporre (come spesso è vero) che non fossero presenti le idonee misure di sicurezza, quindi perdita di affidabilità, autorevolezza, immagine: meglio quindi non comunicare alcuna informazione, non si sa mai che possa arrivare ai media.*

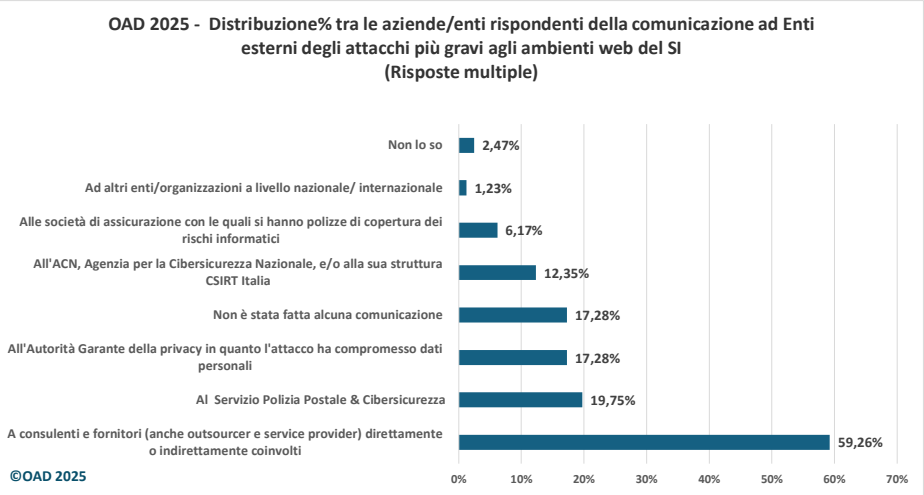


Fig. 4.2-10

La fig. 4.2-11, con risposte multiple, indica, in percentuale, la diffusione delle principali attività intraprese dopo aver subito il più grave attacco ad ambienti web. Al primo posto, con il **67,90%**, l'implementazione di **nuovi strumenti di sicurezza digitali**, che causano l'aumento dei costi sul budget informatico di cui alla fig. 4.2-7.

Poco più della metà dei rispondenti **attiva delle indagini interne**, ma è interessante riscontrare come nessuno coinvolge dei legali, interni o esterni, nelle attività post attacco digitale. Seguono a decrescere ma con percentuali significative, altri interventi sul sistema informativo, quali la sostituzione delle risorse ICT vulnerabili, gli aggiornamenti, etc.; tutti interventi che causano l'aumento di costi.

Poco più di **1/4** delle aziende/enti rispondenti attiva **corsi di sensibilizzazione e di formazione** sulla sicurezza digitale, che almeno in parte tende a ridurre il grave problema delle competenze digitali degli utenti, sia finali che privilegiati. Nessuna delle aziende/enti rispondenti ha attivato una **assicurazione sui rischi informatici,** a seguito dell'attacco subito.

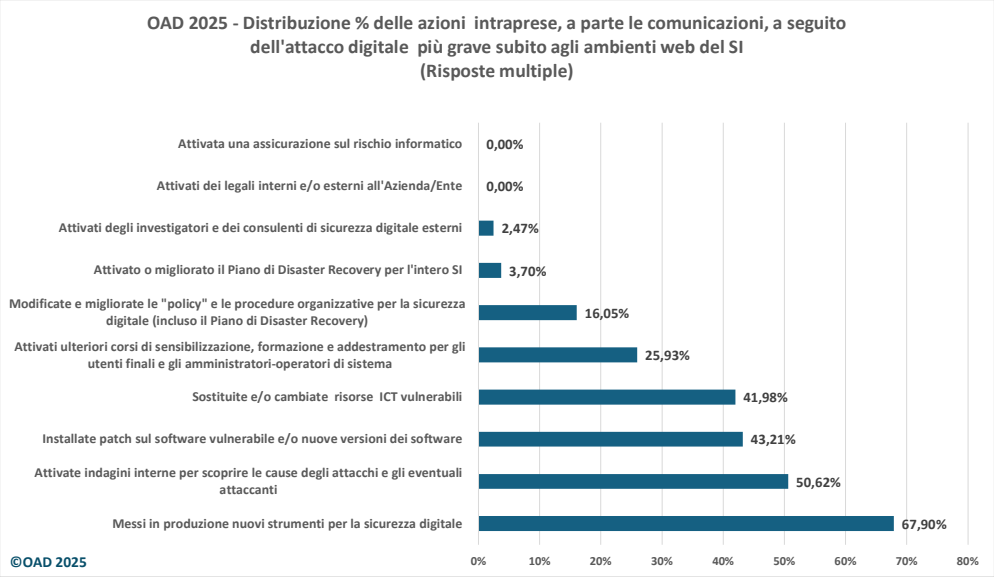


Fig. 4.2-11

4.3 Gli attacchi digitali ai sistemi OT in Italia da OAD 2025

Come già anticipato in §2, l'indagine OAD 2025 ha voluto continuare ad effettuare un'indagine "verticale" sugli **attacchi digitali agli ambienti OT,** eventualmente presenti nei ed interoperanti con i SI dei rispondenti, indagine già effettuata nella precedente edizione OAD 2024.

Il termine **OT, Operation 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.

I sistemi OT includono i sistemi **ICS**, Industrial Control System, i **robot** industriali e di ricerca, i sistemi **IoT**, Internet of Thinks e gli **IIoT**, gli Industrial IoT. I sistemi ICS includono sistemi **SCADA**, Supervisory Control And Data Acquisition, e i sistemi **DCS**, Distributed Control Systems. A livello di attuatori-controllori (dispositivi distribuiti che attuano e controllano localmente il funzionamento di un dispositivo ed inviano dati ad un sistema centrale di raccolta e di elaborazione), si usano i termini di **PLC**, Programmable Logic Controller, **PAC**, Programmable Automation Controller, **RPU**, Remote Processor Unit.

I sistemi OT non rientravano, e sovente ancora non rientrano, nell'ambito della gestione e del governo del SI, considerati come strumenti per la produzione, il più delle volte sotto il controllo della Direzione Produzione e non del CIO. La sempre più forte digitalizzazione dei dispositivi OT e la loro interazione con applicazioni del SI (sovente indicata come integrazione IT/OT) li ha fatti divenire componenti del SI e, soprattutto, ha fatto ampliare significativamente la superficie di vulnerabilità dell'intero SI.

I problemi, gli incidenti e gli attacchi digitali agli ambienti OT possono riguardare non solo la sicurezza dei sistemi ICT (**security**) e del loro funzionamento, ma anche la sicurezza delle persone (**safety**) che interagiscono o che possono essere coinvolte nei processi controllati/attuati dai sistemi OT.

Data l'ampiezza e la complessità del mondo OT, per comprendere i relativi problemi di sicurezza digitale ed i possibili attacchi è opportuno introdurre, almeno a livello architetturale, come operano i sistemi OT.

Le fig. 4.3-1 e 4.3-2 schematizzano esempi di funzionamento per tipici sistemi di automazione industriale.

La fig. 4.3-2 mostra un esempio di schema ICS, dove l'acronimo OPC sta per OLE for Process Control (OLE, Object Linking and Embedding), e PID sta per Proportional-Integral-Derivative.
Per approfondimenti sulle tematiche OT e della loro sicurezza digitale si rimanda all'ampia letteratura disponibile.

Nell'ambito dell'intero bacino di aziende/enti rispondenti al questionario OAD 2025, il **40,58% utilizza sistemi OT**, come indicato nella fig. 4.3-3, e di questi il **32,1%**. **ha subito attacchi ad essi**, come mostrato nella fig. 4.3-4**.**

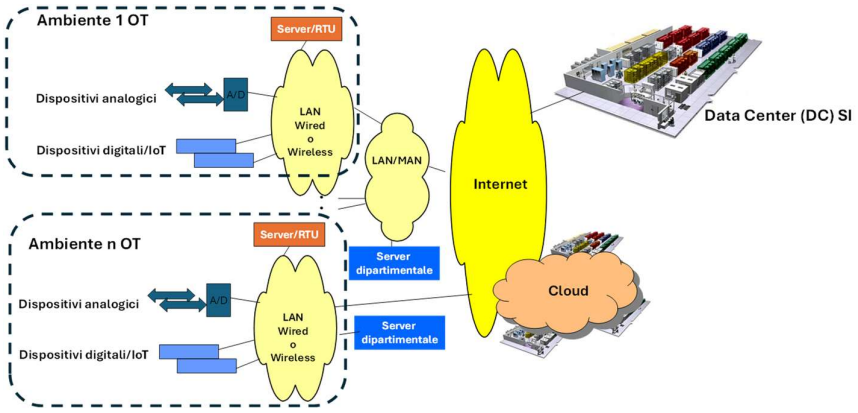


Fig. 4.3-1 (Fonte: Malabo)

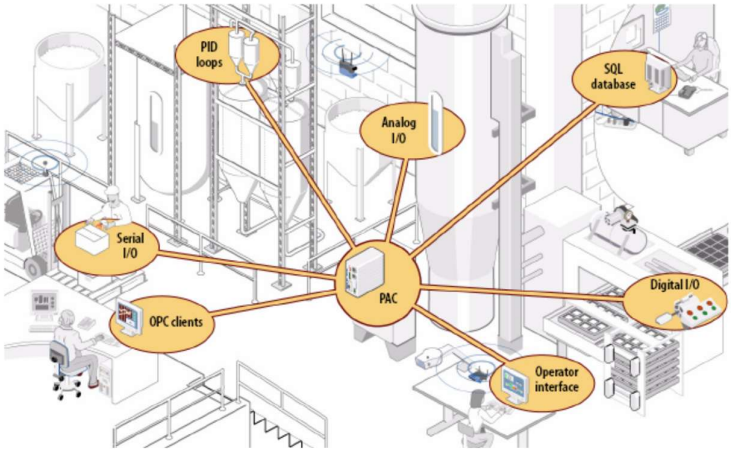


Fig. 4.3-2 (Fonte: OPTO 22)

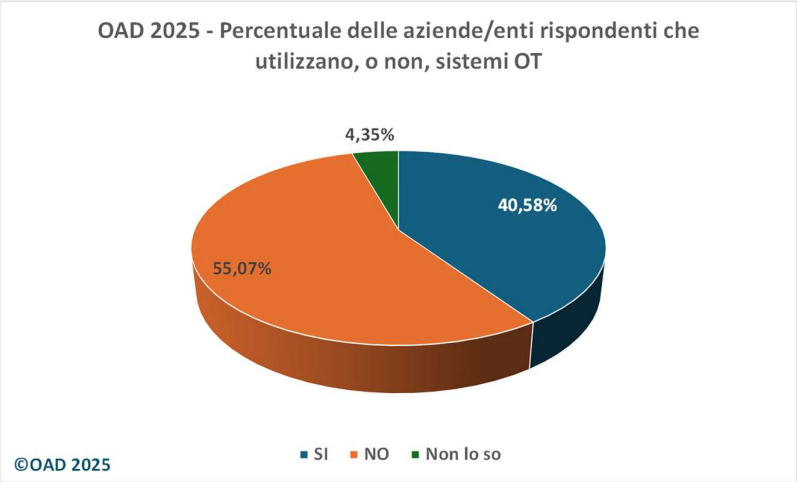


Fig. 4.3-3

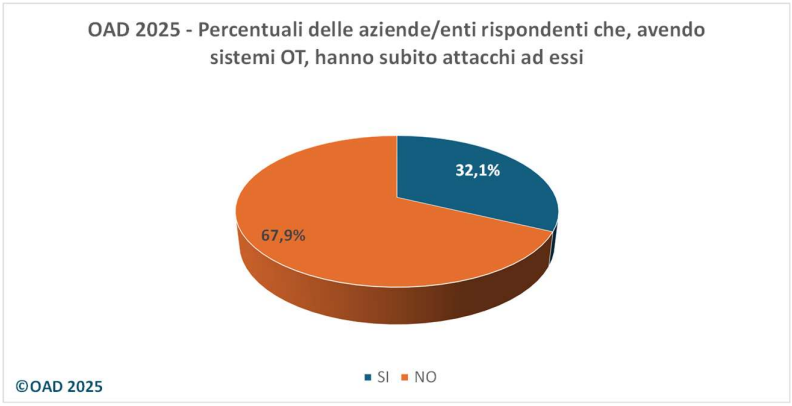


Fig. 4.3-4

La fig. 4.3-5 dettaglia, con risposte multiple, a quali dei vari tipi di sistemi OT in uso sono stati portati i più gravi attacchi. La maggior parte, **il 74,07%**, ha riguardato **robot e sistemi robotizzati**, tipicamente usati per automazione industriale e dei magazzini, cui seguono per il **55,56%** i **sistemi IoT/IIoT**, usati anche chioschi informativi.
Le altre tipologie di sistema hanno % inferiori a scalare, ma tutte non trascurabili.

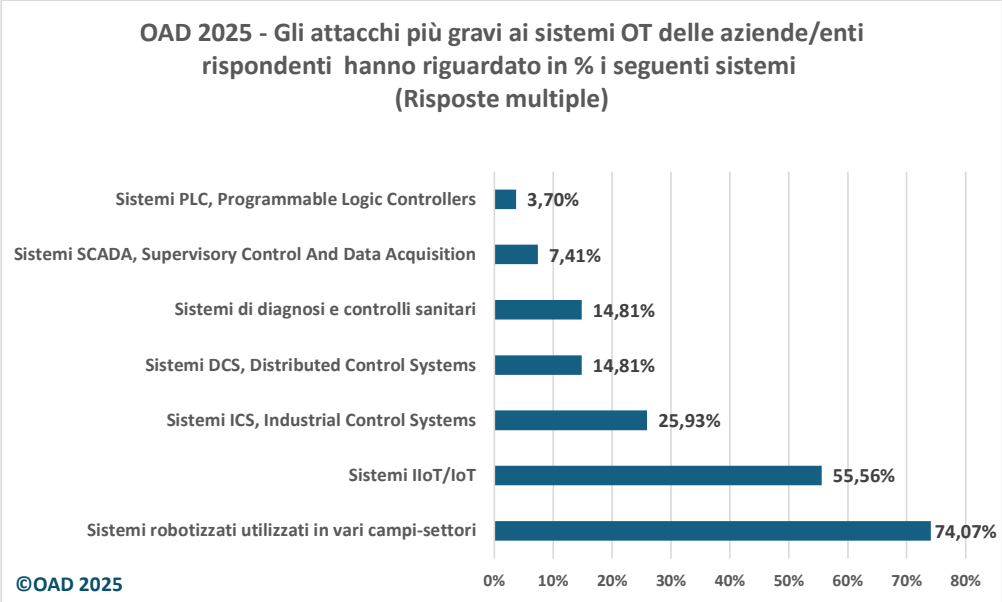


Fig. 4.3-5

Per questa indagine verticale agli attacchi ai sistemi OT sono state poi effettuate, nel questionario online, domande simili a quelle effettuate per gli attacchi agli ambienti web: i seguenti grafici riportano quanto emerso.

Per non appesantire il presente rapporto, vengono sintetizzati i principali dati emersi:

- disservizio causato dall'attacco più grave allo specifico sistema OT
  - il **blocco del funzionamento** del sistema OT fino alla ripresa della sua attività dopo l'attacco è durato **più di 2 giorni** per **più dell'85%** dei casi più gravi
  - il **propagarsi** dell'attacco e del disservizio da locale ad **altre parti del SI** ha causato a quest'ultimo un **blocco di poche ore** per **poco più del 55%** dei casi più gravi, e un **blocco tra 2-3 giorni per quasi il 30%** dei casi più gravi. **Nessuna caso** ha superato i **3 giorni** di blocco del SI o di sue parti.
- Danni economici causati dal più grave attacco ai sistemi OT, con risposte multiple:
  - Impatto significativo sui **costi/budget del SI** per il **37%** dei casi più gravi
  - Impatto anche sul **bilancio dell'azienda/ente** nel **30%** dei casi più gravi.
- Probabili motivazioni per l'attacco più grave ai sistemi OT, con risposte multiple:
  - il **sabotaggio** è la motivazione per quasi il **93%** dei rispondenti
  - il **vandalismo** è al secondo posto con un **37%**, ed il **ricatto** è al terzo posto con un **22%**.
- Tempo massimo richiesto per il ripristino dall'attacco più grave ai sistemi OT:
  - I tempi di ripristino emersi sono veramente lunghi, in quanto alcuni dei dispositivi OT sono sul territorio e in certi casi occorre un intervento in loco per sostituirli o ripararli. Nel **41%** dei casi più gravi l'intervento avviene **entro 3 giorni**, e per il **51%** dei casi **tra i 3 ed i 7 giorni**.
- Interventi che l'attaccato effettua dopo aver subito l'attacco più grave ai sistemi OT, con risposte multiple:
  - **La sostituzione/aggiornamento delle risorse ICT vulnerabili** sono effettuate nel **63%** dei casi, cui segue la richiesta di interventi **a fornitori e consulenti**, con un **59%**. Seguono con la stessa percentuale del **52%** la messa in produzione di **nuovi strumenti di sicurezza** e **l'attivazione di indagini interne** per individuare le cause e gli attori dell'attacco.

4.4 Gli attacchi digitali alle applicazioni e agli ambienti basati su IA

Con l'edizione di quest'anno OAD ha introdotto le applicazioni, i sistemi e gli ambienti di un SI **basati su IA**, **Intelligenza Artificiale** (che spesso viene indicata anche con l'acronimo inglese **AI, Artificial Intelligence**) come tipologia di possibile attacco, il "che cosa" viene attaccato.

L'IA è stata anche considerata come **strumento di attacco** digitale , ossia "come" si effettua l'attacco: la fig. 4.1-2 evidenzia un **3%,** almeno in riferimento al bacino di rispondenti di OAD 2025: una percentuale bassa, ma per l'autore ragionevole, dato che l'IA è sì usato in maniera crescente, ma è ancora limitato il suo uso, e sono soprattutto ancora non ben conosciute le tecniche d'uso dell'IA come strumento d'attacco digitale.
A riprova che di fatto in Italia siano ben poco utilizzate (e conosciute) le metodiche d'uso di IA in generale, la fig. 4.4-1, derivata dall'indagine DESI (già referenziate nel §3) mostra che le imprese italiane che utilizzano qualsiasi tipo di tecnologia IA sono, nel 2024, **l'8,2%** del totale di imprese pubbliche e private con più di 10 dipendenti, contro la **media europea del 13,48%** e contro la Danimarca, Paese che nel 2024 ha la più alta percentuale di imprese che usano IA, con un **27,58%**.

La fig. 4.4-2 mostra che circa il **41%** delle aziende/enti rispondenti **già utilizza** sistemi ed applicazioni basati su IA. Considerando le basse percentuali di cui alla precedente figura, questo dato indica che le aziende/enti rispondenti si collocano in una fascia medio-alta per l'uso di strumenti informatici, oltre che per il livello di sicurezza digitale in essere sui loro SI.

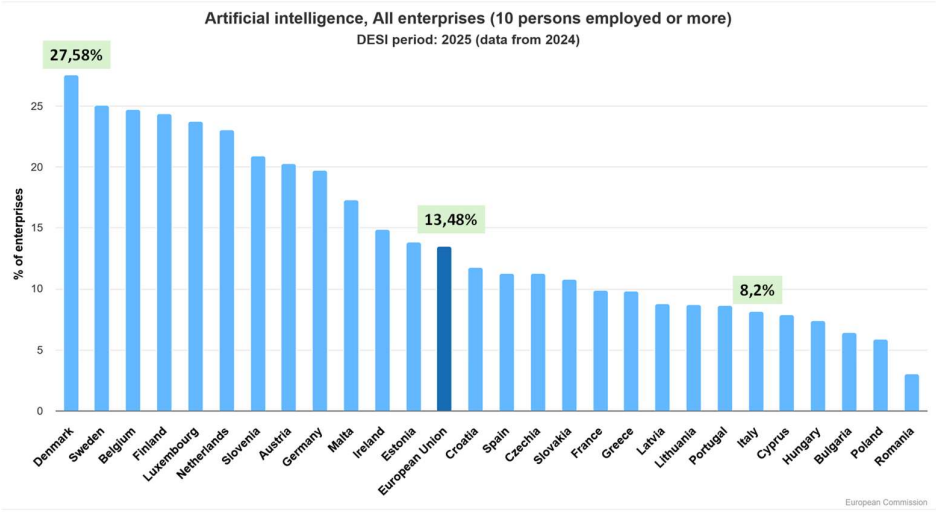


Fig. 4.4-1

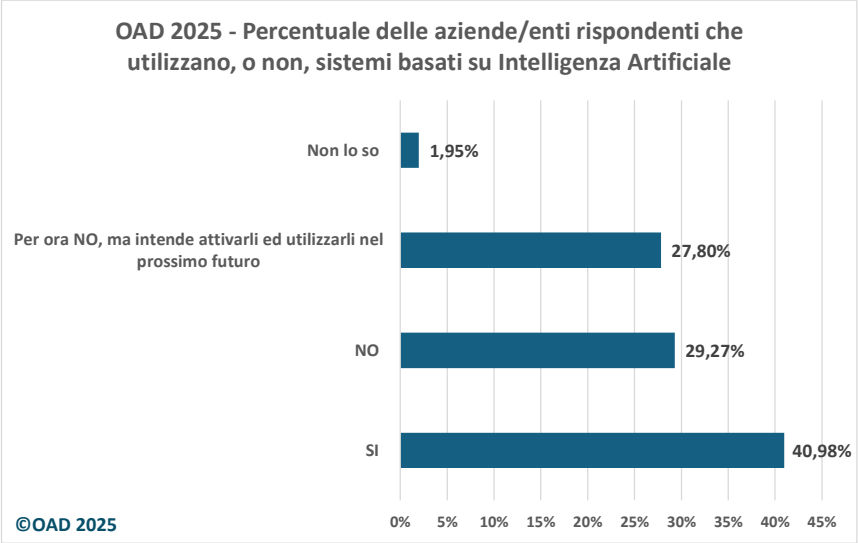


Fig. 4.4-2

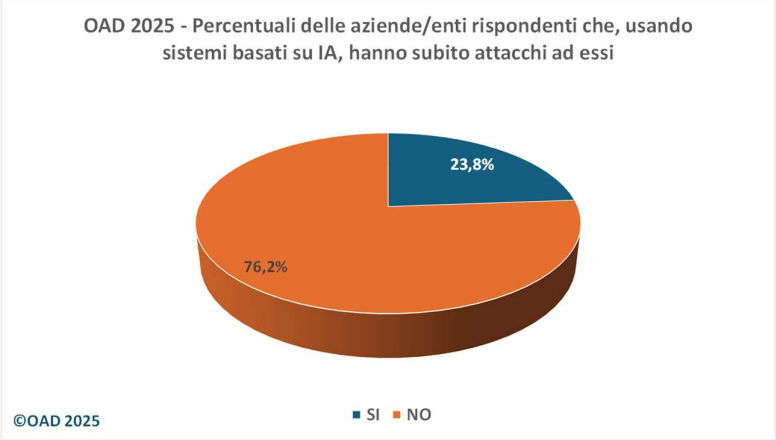


Fig. 4.4-3

Analogamente a quanto fatto per gli attacchi ai sistemi web, si veda §4.1, per gli attacchi digitali ai sistemi di Intelligenza Artificiale il questionario OAD 2025 ha fatto riferimento alle **10 principali e più diffuse vulnerabilità individuate a livello mondiale da OWASP** per i sistemi IA di tipo LLM (Large Language Model) e di Generative AI, che sono le applicazioni attualmente più diffuse. La tabella in fig. 4.4-4 elenca e brevemente illustra queste "top ten" vulnerabilità.
Per maggiori dettagli si rimanda al documento "OWASP Top 10 for LLM Applications 2025", pubblicato a novembre 2024, si veda https://owasp.org/www-project-top-10-for-large-language-model-applications/.
Si rimanda a tutta la documentazione disponibile in Internet sui sistemi LLM e sulla GEN AI.

Si noti come la maggior parte di queste vulnerabilità riguarda i "prompt", ossia le informazioni che si passano al sistema di IA per avere le adeguate risposte, e le modalità di "istruzione" e messa a punto (di contenuti) del sistema stesso. Vulnerabilità che in qualche misura l'AI ACT dell'Unione Europea cerca di ridurre.

La fig. 4.4-5 mostra, con risposte multiple, la **diffusione** percentuale tra i rispondenti a OAD 2025 dello sfruttamento (probabile) delle **Top Ten vulnerabilità elencate da OWASP** nell'attacco più grave ai sistemi di IA .
La vulnerabilità in testa a questa classifica per il bacino di rispondenti 2025 che hanno rilevato attacchi ai sistemi IA (praticamente tutti di tipo LLM e Gen-AI) del loro SI, è quella dei "**Data and Model Poisoning**" (Avvelenamento dei dati e del modello) con un **35%** cui segue, con **20%**, l'"**Improper Output Handling**" (Gestione impropria dell'output)
Il **25%** dei rispondenti, che hanno rilevato un attacco ai loro sistemi di IA, specifica che **non sono stati in grado di individuate le vulnerabilità causa del più grave attacco ai sistemi basati su IA**.
A scalare, ma con percentuali dal 15% allo 0%, molto minori, le altre vulnerabilità "top" indicate da OWSAP.

Questa domanda sugli attacchi ai sistemi IA è molto tecnica e richiede precise conoscenze cui probabilmente molte persone che hanno risposto hanno avuto difficoltà a rispondere. Altre domande, come quelle per i sistemi web e quelli OT dei paragrafi precedenti, volutamente non sono state poste anche per alleggerire il questionario online e non renderlo troppo lungo per la compilazione.

Nome vulnerabilità	Breve descrizione
Prompt Injection (iniezione di prompt)	Questa vulnerabilità si verifica quando i prompt dell'utente alterano il comportamento o l'output dell'LLM in modi non intenzionali. Questi input possono influenzare il modello anche se sono impercettibili agli esseri umani, quindi le iniezioni di prompt non devono essere visibili/leggibili agli esseri umani, purché il contenuto venga analizzato dal modello. Le vulnerabilità di Prompt Injection sono presenti nel modo in cui i modelli elaborano i prompt e nel modo in cui l'input può forzare il modello a passare in modo errato i dati dei prompt ad altre parti del modello, causando potenzialmente la violazione delle linee guida, la generazione di contenuti dannosi, l'abilitazione di accessi non autorizzati o l'influenza di decisioni critiche.
Sensitive Information Disclosure (Divulgazione di informazioni sensibili)	Nella dizione statunitense i dati sensibili non sono solo quelli che fanno riferimento alle informazioni personali, in EU protette secondo i dettami della norma GDPR, ma tutte le informazioni "critiche" e confidenziali. Esse possono influenzare sia l'LLM che il suo contesto applicativo. Ciò include informazioni personali identificabili (PII), dettagli finanziari, cartelle cliniche, dati aziendali riservati, credenziali di sicurezza e documenti legali. Gli LLM, soprattutto quando incorporati nelle applicazioni, rischiano di esporre dati sensibili, algoritmi proprietari o dettagli riservati tramite il loro output. Ciò può comportare accesso non autorizzato ai dati, violazioni della privacy e violazioni della proprietà intellettuale.
Supply Chain	Le catene di fornitura LLM sono soggette a varie vulnerabilità, che possono influire sull'integrità dei dati di formazione, dei modelli e delle piattaforme di distribuzione. Esse possono causare output distorti, violazioni della sicurezza o guasti del sistema. Mentre le vulnerabilità software tradizionali si concentrano su problemi come difetti del codice e dipendenze, qui i rischi si estendono anche a modelli e dati pre-addestrati da terze parti. Questi elementi esterni possono essere manipolati tramite attacchi di manomissione (tampering) o di avvelenamento (poisoning).
Data and Model Poisoning (Avvelenamento dei dati e del modello)	L'avvelenamento dei dati si verifica quando i dati di pre-addestramento, messa a punto o incorporamento vengono manipolati per introdurre vulnerabilità, backdoor o pregiudizi. Questa manipolazione può compromettere la sicurezza, le prestazioni o il comportamento etico del modello, portando a output dannosi o a capacità compromesse. L'avvelenamento dei dati può colpire diverse fasi del ciclo di vita LLM, tra cui la pre-formazione (apprendimento da dati generali), la messa a punto (adattamento dei modelli a compiti specifici) e l'incorporamento (conversione del testo in vettori numerici). L'avvelenamento dei dati è considerato un attacco all'integrità poiché la manomissione dei dati di addestramento incide sulla capacità del modello di fare previsioni accurate. I rischi sono particolarmente elevati con fonti di dati esterne, che possono contenere contenuti non verificati o dannosi.
Improper Output Handling (Gestione impropria dell'output)	La gestione impropria dell'output si riferisce specificamente a una convalida, sanificazione e gestione insufficienti degli output generati da grandi modelli linguistici prima che vengano trasmessi a valle ad altri componenti e sistemi. Poiché il contenuto generato da LLM può essere controllato tramite input rapido, questo comportamento è simile alla fornitura agli utenti di un accesso indiretto a funzionalità aggiuntive. Lo sfruttamento riuscito di una vulnerabilità di gestione impropria dell'output può causare XSS (cross-site scripting, vulnerabilità dei siti web che consente ad un attaccante remoto di "iniettare" script dannosi causa insufficienti/improri controlli dell'input nei form) e CSRF (Cross-Site Request Forgery, vulnerabilità a cui sono esposti i siti web dinamici quando sono progettati per ricevere richieste da un client senza meccanismi per controllare se la richiesta sia stata inviata intenzionalmente oppure no. Diversamente da XSS, che sfrutta la fiducia di un utente in un particolare sito, il CSRF sfrutta la fiducia di un sito nel browser di un utente) nei browser web, nonché SSRF (Server-side request forgery, vulnerabilità che consente a un aggressore di far sì che l'applicazione lato server effettui richieste a servizi/applicazioni cui non potrebbe collegarsi ed accedere), escalation dei privilegi o esecuzione di codice remoto sui sistemi backend.
Excessive Agency (Agenzia eccessiva)	Vulnerabilità che consente di eseguire azioni dannose in risposta a output inaspettati, ambigui o manipolati da un LLM, indipendentemente da ciò che sta causando il malfunzionamento dell'LLM. Un sistema LLM dispone spesso di capacità per chiamare funzioni o interfacciarsi con altri sistemi tramite estensioni (chiamate anche strumenti, competenze o plugin da diversi fornitori) per intraprendere azioni in risposta a un prompt.
System Prompt Leakage (Perdita di prompt di sistema)	Questa vulnerabilità negli LLM si riferisce al rischio che i prompt di sistema o le istruzioni utilizzate per guidare il comportamento del modello possano contenere anche informazioni sensibili che non erano destinate a essere scoperte. I prompt di sistema sono progettati per guidare l'output del modello in base ai requisiti dell'applicazione, ma possono contenere inavvertitamente segreti. Quando vengono scoperti, queste informazioni possono essere utilizzate per effettuare attacchi. È importante comprendere che il prompt di sistema non deve essere considerato un segreto, né deve essere utilizzato come controllo di sicurezza. Di conseguenza, dati sensibili come credenziali, stringhe di connessione, ecc. non devono essere contenuti nel linguaggio del prompt di sistema.
Vector and Embedding Weaknesses (Vulnerabilità dei vettori e degli incorporamenti)	Vulnerabilità significative nei sistemi che utilizzano Retrieval Augmented Generation (RAG), tecnica di adattamento del modello che migliora le prestazioni e la pertinenza contestuale delle risposte dalle applicazioni LLM, combinando modelli linguistici pre-addestrati con fonti di conoscenza esterne. Le modoalità in cui i vettori e gli incorporamenti vengono generati, archiviati o recuperati possono essere sfruttate da azioni (intenzionali o non intenzionali) per iniettare contenuti dannosi, manipolare gli output del modello o accedere (intenzionali o non intenzionali) per iniettare contenuti dannosi, manipolare gli output del modello o accedere a informazioni sensibili.
Misinformation (Disinformazione dovuta ad errori e non intenzionale, come invece è la "disinformation")	Vulnerabilità che si verifica quando gli LLM producono informazioni false o fuorvianti che sembrano credibili. Una delle principali cause è l'allucinazione, quando l'LLM genera contenuti che sembrano accurati ma sono inventati. Le allucinazioni si verificano quando gli LLM colmano le lacune nei loro dati di formazione utilizzando modelli statistici, senza comprendere veramente il contenuto. Di conseguenza, il modello può produrre risposte che sembrano corrette ma sono completamente infondate. Oltre alle allucinazioni, altre cause di disinformazione sono i pregiudizi introdotti dai dati di formazione dell'LLM e le informazioni incomplete, dovute a un controllo inadeguato.
Unbounded Consumption (Consumo illimitato)	Questa vulnerabilità si riferisce al processo in cui un Large Language Model (LLM) genera output basati su query o prompt di input. L'inferenza (una proposizione viene derivata dalle premesse) è una funzione critica degli LLM, che implica l'applicazione di modelli e conoscenze appresi per produrre risposte o previsioni pertinenti. Il consumo illimitato si verifica quando un'applicazione Large Language Model (LLM) consente agli utenti di condurre inferenze eccessive e incontrollate, comportando rischi quali negazione del servizio (DoS), perdite economiche, furto di modelli e degradazione del servizio. Le elevate richieste computazionali degli LLM, in particolare negli ambienti cloud, li rendono vulnerabili allo sfruttamento delle risorse e all'uso non autorizzato.

Fig. 4.4-4 (fonte: OWASP)

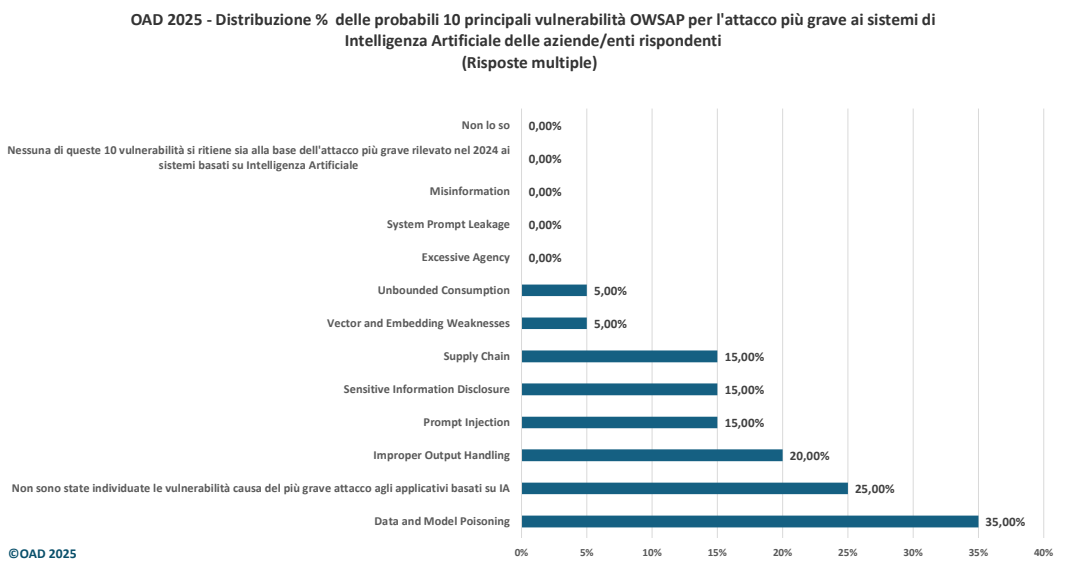


Fig. 4.4-5

Secondo l'autore le risposte avute sono ragionevoli ed interessanti, ma sono da considerare come prime indicazione del fenomeno degli attacchi ai sistemi IA. Da un lato sono relativamente pochi quelli che hanno rilevato attacchi ai loro sistemi di IA, dato che la maggior parte usa sistemi consolidati quali ***ChatGPT***, ***Copilot, Gemini, Claude*** *e che operano su piattaforme tipicamente in cloud ad alta affidabilità, disponibilità e sicurezza; dall'altra l'uso di questi sistemi è prevalentemente per ricerche e confronti di informazioni e, a parte i problemi di copyright e di privacy, i risultati sono in qualche misura verificabili. L'utilizzo di sistemi e di algoritmi di IA in altri contesti è ancora assai limitato e per iperspecialisti, come riporato in fig. 4.4-1 dall'analisi DESI.*

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

Come già evidenziato in §4.1 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 2026-2027**, e tendenzialmente le risposte sono influenzate, per le/i rispondenti, dagli attacchi subiti nel 2024, si veda il Capitolo 4 e in particolare le fig. 4.1-1 e 4.1-2.

La fig. 5-1, con risposte multiple, mostra che per poco più del **40%**, la tipologia di attacco più temuta nel prossimo futuro è data dalle "**Modifiche non autorizzate ai dati e alle informazioni trattate dal sistema informativo"**. E' in effetti l'attacco più grave che si possa subire dato che va ad **alterare i dati trattati dal SI**, dati che costituiscono un "asset", un bene aziendale, tra i più essenziali per qualsisi tipo di organizzazione, pubblica o privata, nell'attuale era della società digitale. Percentualmente seguono, con il **35%**, gli "**Attacchi ai propri sistemi in cloud o in hosting"**[46] e con un **32,1%** la "**Saturazione delle risorse ICT del SI"**.
Tutte le altre tipologie di attacco scendono a scalare in % sotto il 30%, ma con percentuali abbastanza alte.
Da evidenziare che:

- l'attacco alla **supply chain,** tipologia introdotta per la prima volta nel questionario OAD 2024, raggiunge un significativo **24,45%;** è quindi temuta da circa un ¼ delle/dei rispondenti il che conferma la criticità di questo attacco individuato tra i primi più gravi rischi del futuro da ENISA, come commentato in §3.1;
- 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 **20,52%**, 1/5 del totale delle/dei rispondenti; un tipo di attacco che ha già dato risultati notevoli con lo spear phishing e con le le fakenews/disinformazioni, e che può fortemente impattare e migliorare tante altre tecniche di attacco, si veda anche fig. 5-2;
- rimangono alte le percentuali per il furto "fisico" di dispositivi ICT fissi e mobili, e dei dati in essi contenuti.

La fig. 5-2, con risposte multiple, mostra **le famiglie di tecniche di attacco** più temute per il prossimo futuro.
Al primo posto, per più della metà delle/dei rispondenti, "**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 secondo posto, con il **35,37%**, l'uso di "**Strumenti di attacco basati su Intelligenza Artificiale**"; più di un 1/3 delle/dei rispondenti paventa l'uso dell'IA per individuare vulnerabilità nel SI target e per sfruttarle. Per gli attacchi subiti, l'uso di IA è ancora "embrionale, con un 3%, come mostrato in fig. 4.1-2
Al terzo posto, con un **34,%**, 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.

[46] 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". Rimane quindi abbastanza alto, e giustificato, il timore di attacchi ai provider tali da impattare le proprie parti di SI terziarizzate.

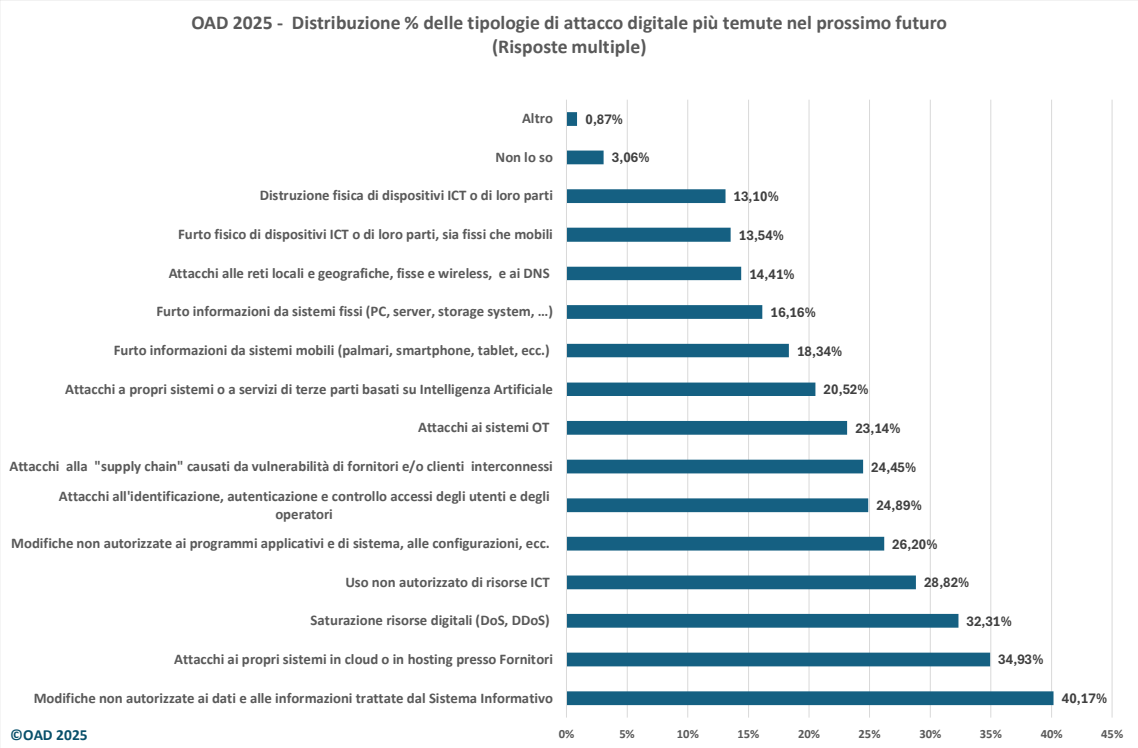

OAD 2025 - Distribuzione % delle tipologie di attacco digitale più temute nel prossimo futuro
(Risposte multiple)
Altro 0,87%
Non lo so 3,06%
Distruzione fisica di dispositivi ICT o di loro parti 13,10%
Furto fisico di dispositivi ICT o di loro parti, sia fissi che mobili 13,54%
Attacchi alle reti locali e geografiche, fisse e wireless, e ai DNS 14,41%
Furto informazioni da sistemi fissi (PC, server, storage system, ...) 16,16%
Furto informazioni da sistemi mobili (palmari, smartphone, tablet, ecc.) 18,34%
Attacchi a propri sistemi o a servizi di terze parti basati su Intelligenza Artificiale 20,52%
Attacchi ai sistemi OT 23,14%
Attacchi alla "supply chain" causati da vulnerabilità di fornitori e/o clienti interconnessi 24,45%
Attacchi all'identificazione, autenticazione e controllo accessi degli utenti e degli operatori 24,89%
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc. 26,20%
Uso non autorizzato di risorse ICT 28,82%
Saturazione risorse digitali (DoS, DDoS) 32,31%
Attacchi ai propri sistemi in cloud o in hosting presso Fornitori 34,93%
Modifiche non autorizzate ai dati e alle informazioni trattate dal Sistema Informativo 40,17%
©OAD 2025
0% 5% 10% 15% 20% 25% 30% 35% 40% 45%

Fig. 5-1

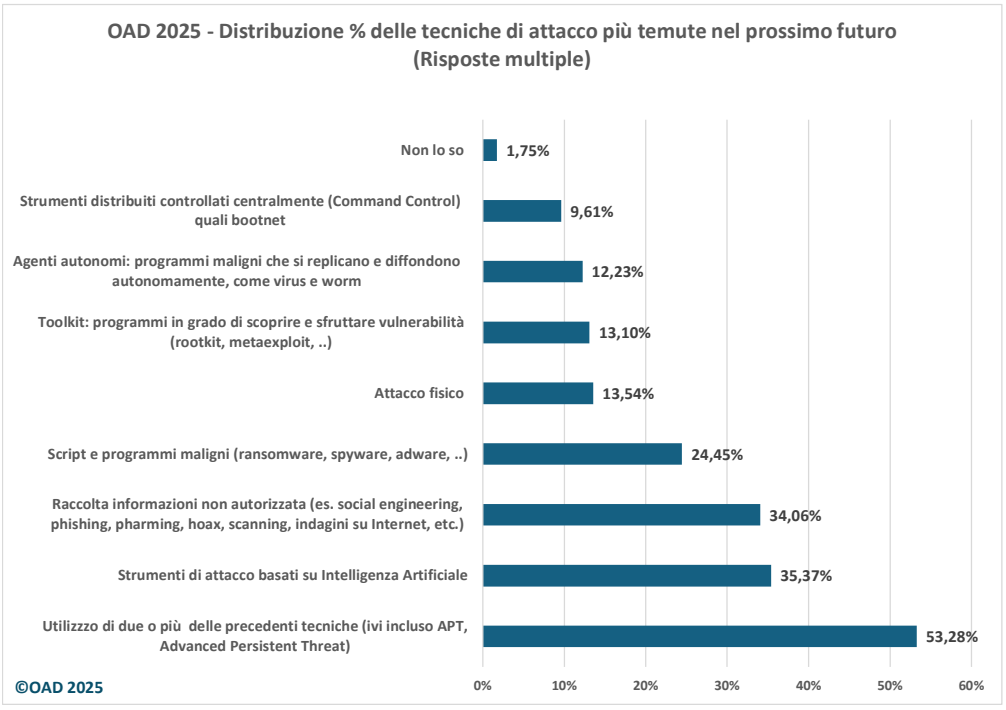

OAD 2025 - Distribuzione % delle tecniche di attacco più temute nel prossimo futuro
(Risposte multiple)
Non lo so 1,75%
Strumenti distribuiti controllati centralmente (Command Control) quali bootnet 9,61%
Agenti autonomi: programmi maligni che si replicano e diffondono autonomamente, come virus e worm 12,23%
Toolkit: programmi in grado di scoprire e sfruttare vulnerabilità (rootkit, metaexploit, ..) 13,10%
Attacco fisico 13,54%
Script e programmi maligni (ransomware, spyware, adware, ..) 24,45%
Raccolta informazioni non autorizzata (es. social engineering, phishing, pharming, hoax, scanning, indagini su Internet, etc.) 34,06%
Strumenti di attacco basati su Intelligenza Artificiale 35,37%
Utilizzzo di due o più delle precedenti tecniche (ivi incluso APT, Advanced Persistent Threat) 53,28%
©OAD 2025
0% 10% 20% 30% 40% 50% 60%

Fig. 5-2

L'**uso di script e di programmi maligni,** nei quali rientrano i malware e ransomware assai diffusi in Italia (al 3° posto tra le tecniche rilevate negli attacchi subiti nel 2024, si veda sempre fig. 4.1-2) è considerato come futura temibile tecnica di attacco **da circa ¼** (**24,45%**) delle/dei rispondenti.
Le altre tecniche seguono a scalare con una certa gradualità.

La fig. 5-3, con risposte multiple, evidenzia le **possibili motivazioni** che le/i rispondenti ipotizzano per gli attacchi digitali del prossimo futuro.
In cima alla lista **le frodi**, con un **61,4%** (nelle quali si includono i ricatti), seguite con un **47,16%** dal **sabotaggio.**
Al terzo e quarto posto si trovano **l'hactivism,** con il **36,68%** e la **guerra digitale,** con un **24,6%.**
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 hactivismo e guerre digitali, hanno purttoppo risposto in numero relativamente limitato.

Questo indica 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. Hactivism e guerre digitali possono infatti effettuare attacchi "di massa", come in qualche misura è stato fatto da gruppi filo-russi con attacchi ransomware, che investono anche piccle organizzazioni.

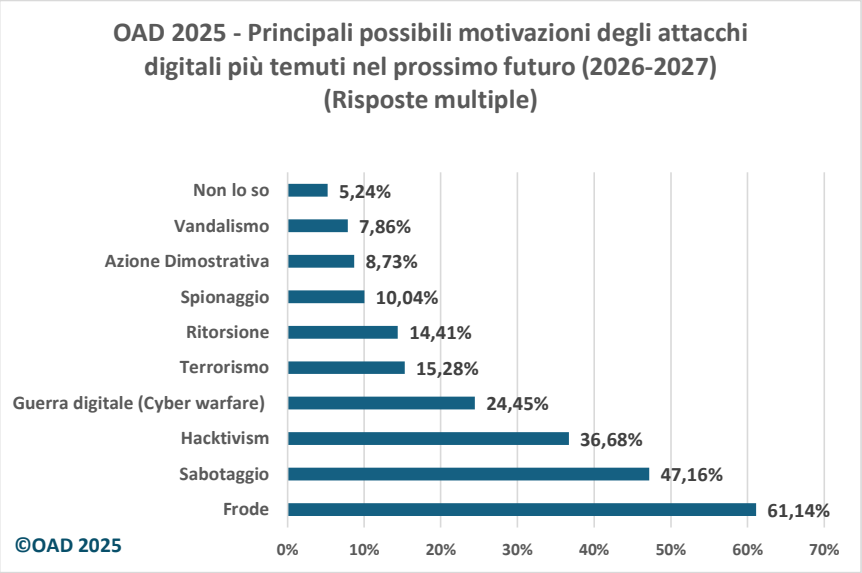


Fig. 5-3

6. Il campione delle aziende/enti rispondenti e dei loro SI

Il presente capitolo fornisce una macro descrizione dei Sistemi Informativi (SI) delle aziende/enti rispondenti, e delle aziende/enti stesse. Questa analisi 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 2025 sono state 316, sostanzialmente dello stesso ordine di grandezza rispetto alle edizioni precedenti OAD.
Pur con grandi difficoltà e nonostante un numero maggiore di associazioni patrocinanti coinvolte (si veda Allegato D) rispetto alle precedenti edizioni, si è comunque superato il minimo numero di risposte necessarie perché l'indagine via web abbia valore e sia, almeno come contenuti, paragonabile a quelle degli anni precedenti.

La Tabella in fig. 6-1 mostra i raggruppamenti dei settori merceologici considerati nelle indagini OAD, che fanno riferimento alla classificazione ATECO[47], sulla cui base si sono raggruppati alcune categorie, e alla quale si sono aggiunte le Pubbliche Amministrazioni Centrali (PAC) e Locali (PAL), oltre ad una specifica "sottocategoria", i "Service Provider ICT", distinguendola dalla sua categoria "madre" di "Servizi ICT": l'intenzione è quella di meglio individuare le società provider di servizi ICT, quali hosting, housing e cloud, data l'importanza della crescente terziarizzazione da un lato, e dall'altro l'indagine verticale sugli attacchi agli ambienti web, che sono prevalentemente terziarizzati.

[47] ATECO, ATtività ECOnomiche, è la classificazione delle attività economiche in settori merceologici adottata dall'ISTAT per le rilevazioni statistiche nazionali di carattere economico. Si veda: https://ateco.infocamere.it/ateq20/#!/home

Service Provider hosting/cloud (Codice Ateco J 63.11.30)
Altri servici ICT, esclusi Provider hosting/cloud: consulenza, produzione software, servizi assistenza e riparazione ICT, etc. (Codici Ateco J62, J63, S95.1)
Settore primario: agricoltura, allevamento, pesca, estrazione (Codici Ateco A e B)
Industria manifatturiera e costruzioni: meccanica, chimica, farmaceutica, elettronica, alimentare, edilizia, etc. (Codici Ateco C e F)
Utility: Acqua, Energia, Gas, etc. (Codici Ateco D ed E)
Commercio all'ingrosso e al dettaglio, incluso quello di apparati ICT (Codici Ateco G)
Trasporti e magazzinaggio (Codici Ateco H)
Attività finanziarie ed assicurative: assicurazioni, banche, istituti finanziari, broker, intermediazione finanziaria, etc. (Codici Ateco M)
Servizi turistici, di alloggio e ristorazione: agenzie di viaggio, tour operator, hotel, villaggi turistici, campeggi, ristoranti, bar, etc. (Codici Ateco I e N79)
Attività artistiche, sportive, di intrattenimento e divertimento: teatri, biblioteche, archivi, musei, lotterie, case da gioco, stadi, piscine, parchi, discoteche, etc. (Codici Ateco R)
Stampa e servizi editoriali (Codici Ateco J58)
Servizi professionali e di supporto alle imprese: attività immobiliari, notai, avvocati, commercialisti, consulenza imprenditoriale, ricerca scientifica, noleggio, call center, etc. (Codici Ateco L, M, N77, N78, N80, N81, N82)
Telecomunicazioni e Media: produzione musicale, televisiva e cinematografica, trasmissioni radio e televisive, telecomunicazioni fisse e mobili (Codici Ateco J59, J60, J61)
Sanità e assistenza sociale: ospedali pubblici o privati, studi medici, laboratori di analisi, etc. (Codici Ateco Q)
Istruzione: scuole e università pubbliche e private (Codici Ateco P)
Associazioni, associazioni imprenditoriali e sindacati (Codici Ateco S94)
PAC, Pubblica Amministrazione Centrale
PAL, Pubblica Amministrazione Locale

Fig. 6-1

6.1 L'Azienda/Ente rispondente

La fig. 6.1-1 mostra la distribuzione percentuale dei rispondenti per le macro famiglie di settori merceologici considerati. Le voci dei raggruppamenti merceologici della figura sono sintetizzate, per i dettagli coi codici ATECO si veda fig. 6-1.
Al primo posto si posizionano i Servizi ICT, con un 15,72%, esclusi i servizi dei Provider di hosting e cloud. Se si aggiungono questi ultimi ed anche il settore delle telecomunicazioni e media, ora tutti digitali, si arriva ad un totale del 21,40% . Le aziende/enti rispondenti dell'intero mondo digitale, come offerta, rappresentano più di 1/5 del totale dei rispondenti.
Al secondo posto le industrie manifatturiere e di costruzioni, con un 14,85%, molto vicino al 14, 41% della sanità e servizi sociali
Al quarto posto, con un 10,48%, i servizi professionali e di supporto alle imprese.
La distribuzione percentuale emersa dal bacino di aziende/enti a OAD 2025 è simile a quella delle edizioni di OAD 2023 e precedenti. Per la scorsa edizione OAD 2024 era emerso al primo posto il settore dell'Istruzione, grazie all'attività di promozione svolta da AICA. Pur avendo effettuato una analoga promozione nel 2025, AICA ha collaborato ed ha patrocinato OAD 2025, la compilazione del questionario per questa edizione è stata assai ridotta per il settore "Istruzione".

Per le dimensioni di un'organizzazione per numero di dipendenti, come per le ultime edizione di OAD, il questionario 2025 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.

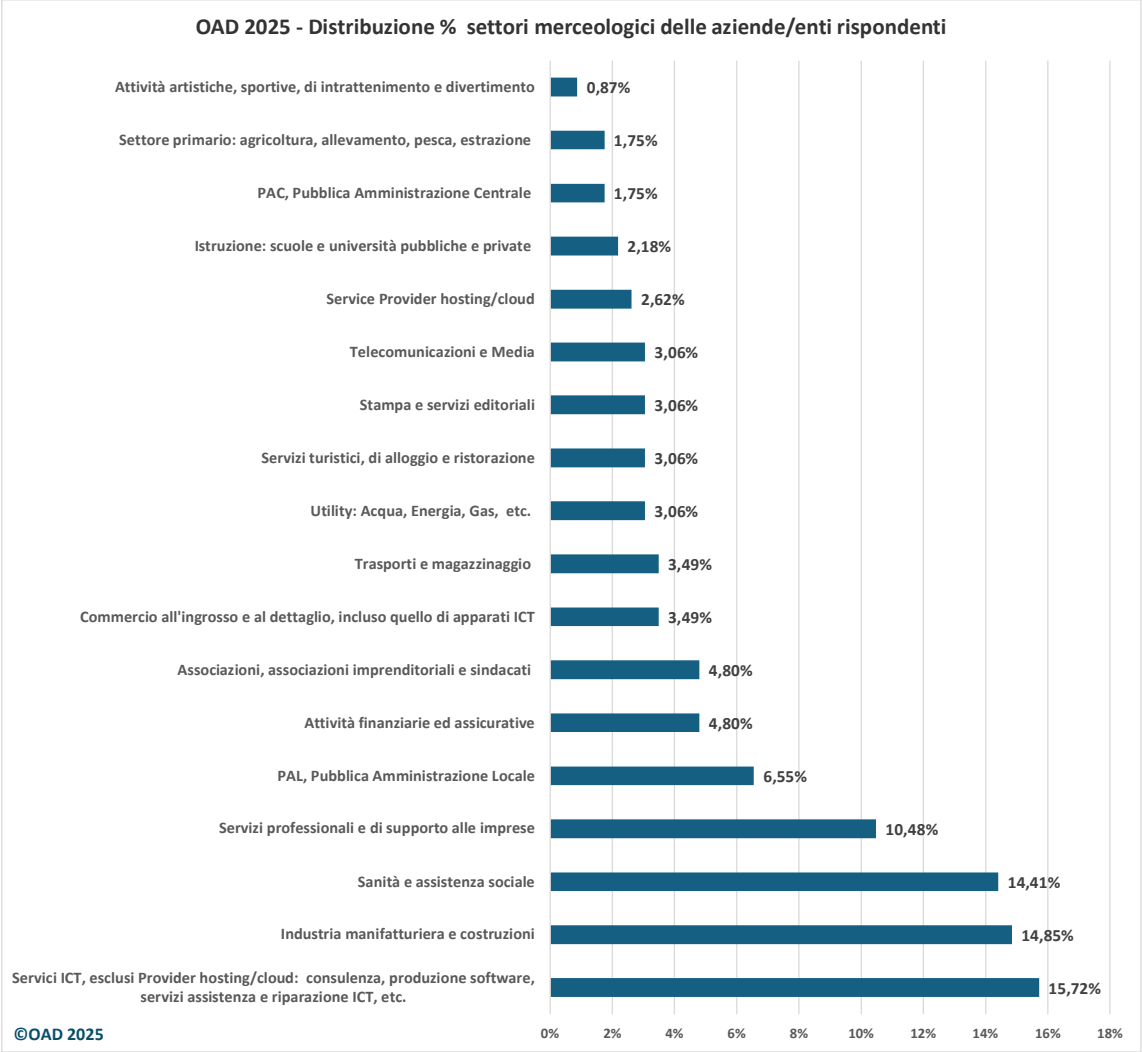


Fig. 6.1-1

La fig. 6.1-2 mostra la ripartizione percentuale delle aziende/enti rispondenti in base al numero di loro dipendenti. Hanno risposto il 62,96% di piccole e medie organizzazioni, ossia quelle fino a 250 dipendenti (le PMI, Piccole Medie Imprese, in ambito aziende private). Significativa, con un 22,22%, la presenza tra queste delle piccolissime organizzazioni con meno di 10 dipendenti, che, come indicato in §3.3.2, costituiscono la stragrande maggioranza delle imprese, private e pubbliche, in Italia.

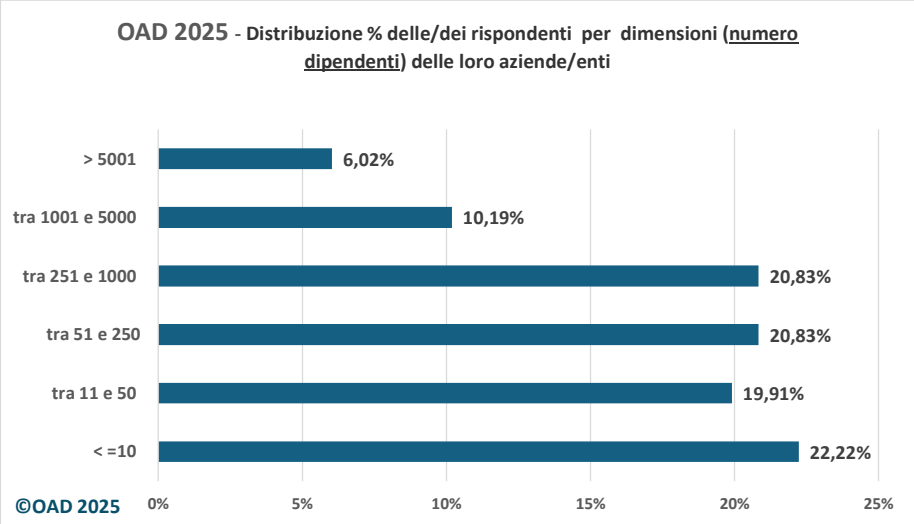


Fig. 6.1-2

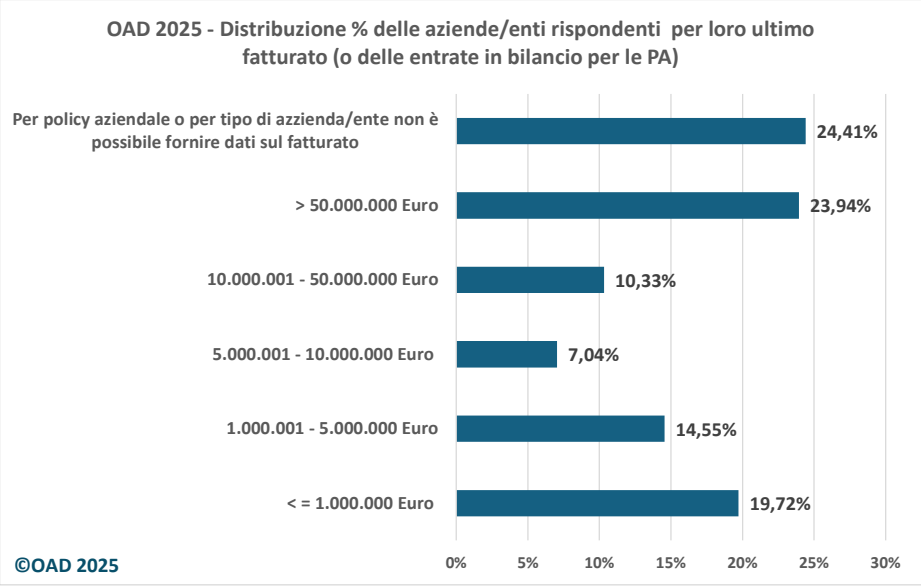


Fig. 6.1-3

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.
Nella presente indagine OAD, la percentuale più alta, 24,41%, è data da aziende/enti che non possono/vogliono fornire questo dato, pur con la totale anonimità realmente garantita da OAD.
Significativa l'alta percentuale, 23,94%, di aziende/enti rispondenti con fatturati maggiori di 50 Mln di Euro.
Un ulteriore dato caratterizzante un'azienda/ente è la estensione geografica delle sue attività e/o del suo business. La fig. 6.1-4 mostra la distribuzione percentuale delle aziende/enti rispondenti per l'estensione geografica della loro attività.

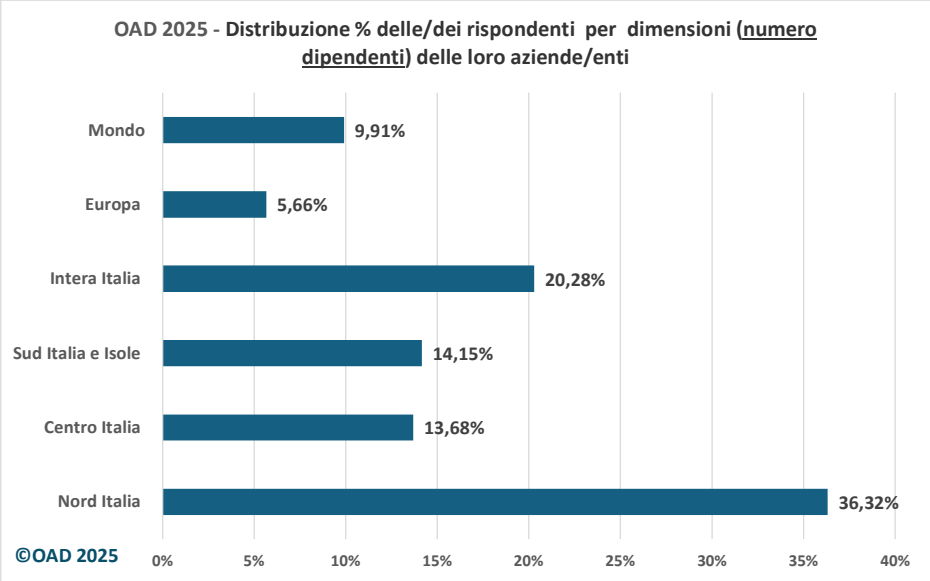


Fig. 6.1-4

La maggior parte delle azie3nde/enti rispondenti, l'84,43%, opera in Italia, ma solo il 20,28% ha attività estese a livello nazionale, la maggior parte opera nel Nord Italia.

6.2 Tipologia, ruolo e principali caratteristiche dei Sistemi Informativi delle aziende/enti rispondenti

La fig. 6.2-1 mostra che il Sistema Informativo (SI) è gestito e controllato totalmente in Italia per l'87,57% delle aziende/enti rispondenti, e per il 61,58% è di piccole-medie dimensioni senza un Data Center. Quest'ultima è la caratteristica tipica di un SI di una piccola o di una media organizzazione, che costituiscono la stragrande maggioranza in Italia (si rimanda a §3.3.2)

Uno degli aspetti di valore dell'indagine OAD è il coinvolgimento di piccole e piccolissime realtà italiane nella compilazione del questionario online, realtà che di solito non vengono prese in considerazione da molte altre indagini, sia in Italia che all'estero.

La fig. 6.2-2 mostra, come distribuzione percentuale delle risposte avute, dove è situato a livello regionale in Italia la sede principale del SI, sia essa un Data Center o una computer room "primaria", da parte dei SI delle aziende/enti rispondenti.
Grazie ai vari e ripetuti solleciti di AIPSI e dell'autore, l'indagine OAD 2025 è riuscita, seppur faticosamente, a coprire tutte le regioni d'Italia.

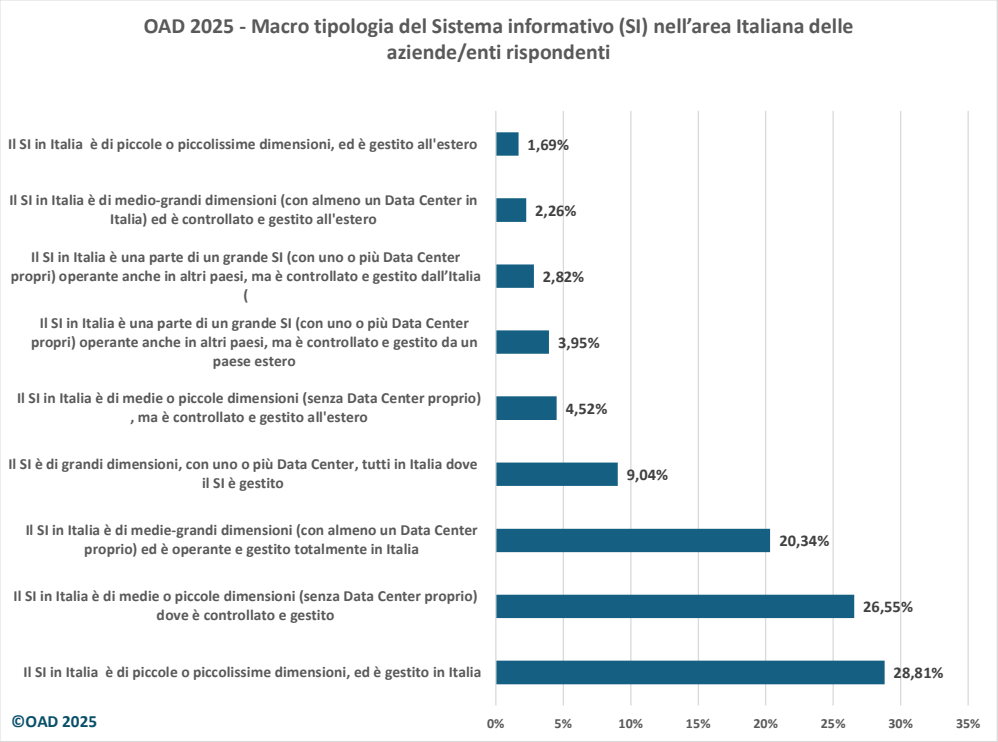


Fig. 6.2-1

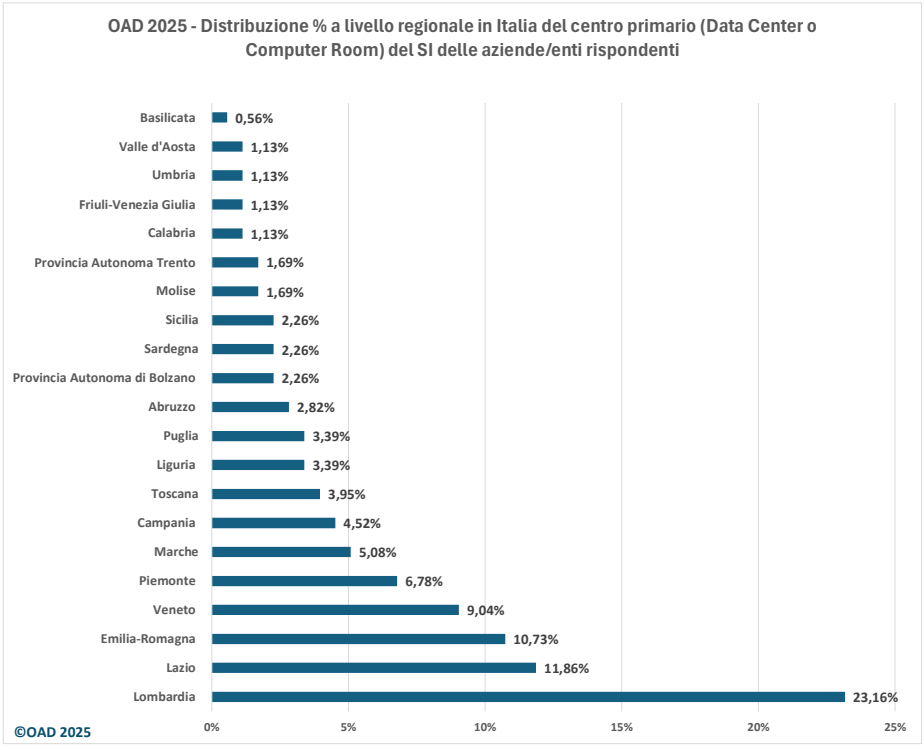


Fig. 6.2-2

La maggior parte dei "centri" dei SI delle aziende/enti rispondenti è in Lombardia, con un 26,16%, cui seguono, percentualmente a distanza, il Lazio, con un 11,86%, e l'Emilia Romagna , con un 10,73%.
Tutte le altre Regioni hanno, a scalare, percentuali inferiori al 10%.

E' importante evidenziare come tale distribuzione % fa riferimento solo a chi ha risposto al questionario OAD 2025, *e non è una indicazione assoluta di dove in Italia si concentrano i Data Center o le computer room principali.*

Per comprendere il fabbisogno di sicurezza digitale per il SI oggetto delle risposte (necessario anche per effettuare la macro valutazione del livello di sicurezza del SI oggetto delle risposte al questionario), è stato chiesto, a livello qualitativo, quale è l'importanza del SI, e quindi della sua sicurezza, per il business e per le attività dell'azienda/ente rispondente.
La fig. 6.2-3 evidenzia che per il 75,14% delle aziende/enti rispondenti il SI è essenziale per il funzionamento delle loro attività e dei loro processi, e pertanto la sua sicurezza digitale dovrebbe essere di alto livello e allo stato dell'arte.

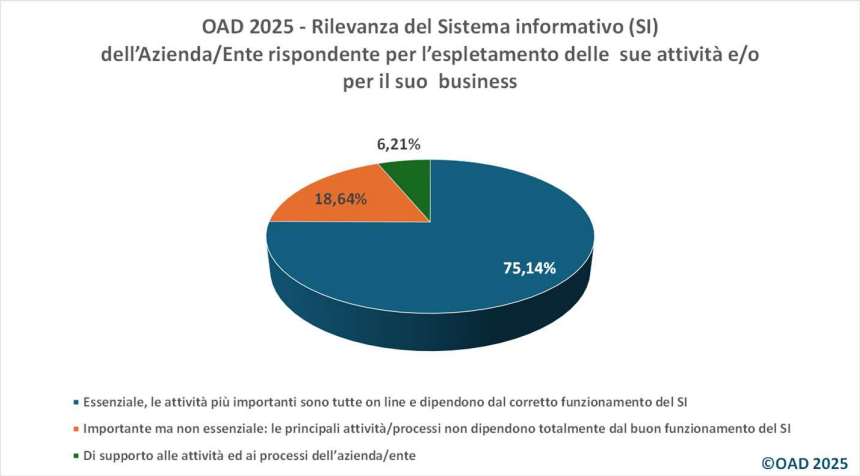


Fig. 6.2-3

Altre caratteristiche di un SI sono importanti per individuare i suoi fabbisogni di sicurezza digitale, oltre a specifiche richieste di normative tipiche del settore merceologico dell'azienda, quali ad esempio DORA per il settore finanziario ed assicurativo. Una tra tutti è la normativa sulla privacy, il GDPR, per il trattamento di dati personali.
Un ulteriore importante aspetto è la gestione dell'intero sistema informativo e della sua sicurezza digitale più o meno terziarizzata: il fenomeno della terziarizzazioni di queste gestioni operative è crescente soprattutto per le piccole e medie organizzazioni, che no possono avere al loro interno specifiche competenze in merito.
Dall'indagine OAD 2025 emerge che:

- il 95,48% dei SI rispondenti tratta dati personali, e di questi il 46,33% tratta, o potrebbe trattare, dati sensibili[48];
- il 25,42 dei SI rispondenti forniscono servizi essenziali e/o sono infrastrutture critiche per il sistema paese, e quindi soggetti alla normativa NIS2;

[48] 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. E' bene considerare che il concetto di dato sensibile nella letteratura inglese fa riferimento più in generale ad un dato critico che deve essere confidenziale.

- il 94,15 dei SI utilizza sistemi ed applicazioni terziarizzate, in particolare per SaaS e PaaS; questi SI sono peranto "ibridi", con una parte in locale (on premise) ed una parte terziarizzata;
- la gestione operativa dell'intero SI è totalmente terziarizzata per il 24,29% delle aziende/enti rispondenti, e parzialmente terziarizzata per il 43%;
- la gestione operativa della sicurezza digitale del SI è totalmente terziarizzata per il 27,43% delle aziende/enti rispondenti, e parzialmente terziarizzata per il 46,29%.

Si noti come per lo stesso bacino di rispondenti, e quindi con confronti statisticamente validi e consistenti, la terziarizzazione totale o parziale della sicurezza digitale ha circa 3 punti percentuali in più rispetto alla gestione dell'intero SI. Questo è un piccolo ma significativo indicatore di come la sicurezza digitale stia diventando sempre più critica ed ha bisogno di specialisti competenti per essere gestita.
Il dato percentuale della "completa" terziarizzazione della gestione operativa della sicurezza digitale è alto e significativo: circa 1/4 delle aziende/enti rispondenti.

Le piccole organizzazioni, salvo eccezioni, non possono essere in grado di gestire autonomamente la sicurezza digitale, e devono fare pertanto ricorso a consulenti o a società specializzate. Proprio per le piccole realtà saranno sempre più significativi i servizi tipo MSS[49] e CSaaS[50], a parte il problema del loro prezzo, spesso troppo alto proprio per le realtà più piccole.

La gestione operativa terziarizzata del SI include tipici servizi quali ad esempio il continuo monitoraggio e controllo, sia funzionale sia prestazionale, delle varie unità del SI, apparati di rete inclusi, la gestione delle varie unità a livello hardware e software (aggiornamenti, patch e fix, gestione segnalazioni ed allarmi di sistema, etc.), la gestione delle applicazioni, la gestione degli utenti e del provisioning per i nuovi utenti, la gestione dei back-up e l'eventuale ripristino, la gestione dell'help desk – trouble ticketing, la predisposizione e la gestione del Disaster Recovery, la gestione dei log dei sistemi e degli utenti finali/privilegiati, la gestione dei problemi e degli incidenti, etc.
Un conto è usare in service una applicazione, un conto è terziarizzare, in toto o in parte, la gestione operativa del SI e della sua sicurezza.

Le fig. 6.2-4 e 6.2-5 mostrano la situazione per i SI oggetto delle risposte:

- la gestione operativa dell'intero SI è terziarizzata in toto o in parte da più dei 2/3 dei rispondenti, il 67,23%, e di questi il 24,29% la terziarizza completamente;
- la gestione operativa della sicurezza digitale del SI è terziarizzata da quasi i ¾ dei rispondenti, il 73,71%, e di questi il 27,43% la terziarizza completamente.

E' bene evidenziare che:

- entrambi i dati di terziarizzazione della gestione del SI e della sua sicurezza sono alti;
- per lo stesso bacino di rispondenti, e quindi con stretta validità statistica, la percentuale della terziarizzazione della gestione della sicurezza digitale è più alta di quella della gestione del SI, e questo anche per la "completa" terziarizzazione di entrambe le gestioni operative;
- il livello della sicurezza digitale deve essere, ed è, alto e significativo: le piccole organizzazioni, salvo eccezioni, non possono essere in grado di gestire autonomamente la sicurezza digitale, e devono fare pertanto ricorso a consulenti o a società specializzate. Proprio per le piccole realtà saranno sempre più significativi i servizi tipo MSS e CSaaS, come già indicato in precedenza, a parte il problema del loro prezzo, spesso troppo alto proprio per le realtà più piccole.

[49] MSS, Managed Security Services.
[50] CSaaS, Cybersecurity as a Service.

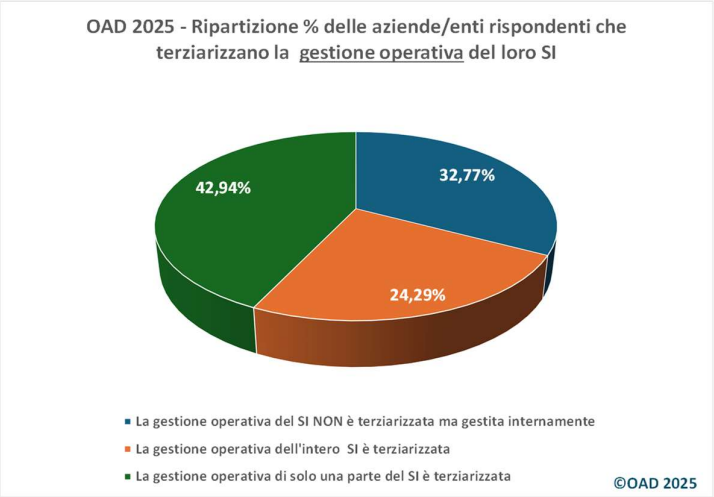


Fig. 6.2-4

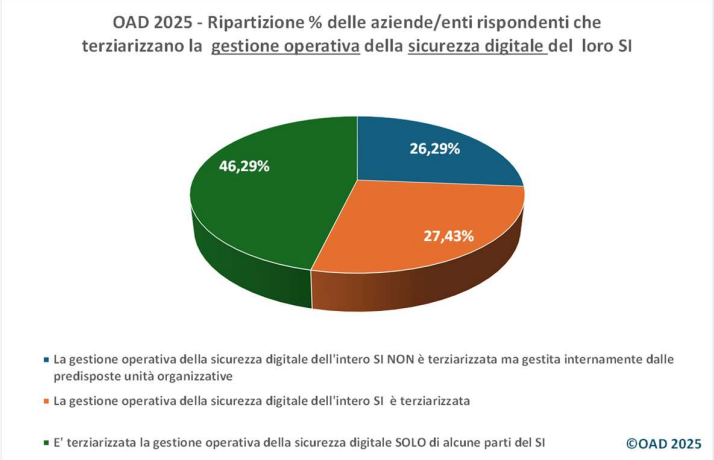


Fig. 6.2-5

Per meglio analizzare i dati emersi, si sono correlati i dati della terziarizzazione della gestione del SI e della sua sicurezza digitale con le dimensione (per numero di dipendenti) dell'azienda/ente rispondente.
Tali correlazioni mostrano chiaramente come:

- la terziarizzazione per la gestione sia del SI che della sua sicurezza digitale vede percentuale maggiori nelle piccole organizzazioni; le grandi e grandissime organizzazioni hanno strutture e capacità per una gestione interna, e terziarizzazione se mai solo alcune parti del loro SI o della sua sicurezza digitale;
- la terziarizzazione in toto sia del SI sia della sicurezza digitale trova maggior diffusione nelle organizzazioni tra gli 11 ed i 50 dipendenti: hanno già sistemi informativi abbastanza complessi, ma non possono essere autonomi nella loro gestione e devono pertanto terziarizzare;

- con percentuali diverse ma tutte le organizzazioni terziarizzano almeno alcune funzionalità sia del SI sia della sua sicurezza.

La fig. 6.2-6 mostra la correlazione tra le dimensioni, come numero di dipendenti, delle organizzazioni rispondenti e la terziarizzazione della gestione operativa della sicurezza digitale.

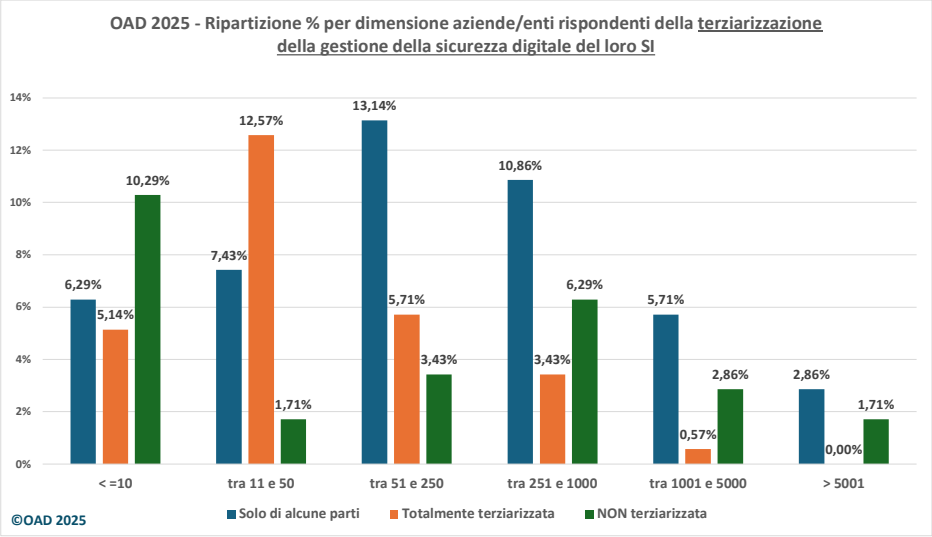


Fig. 6.2-6

Proprio per le piccole realtà saranno pertanto sempre più significativi i servizi tipo MSS e CSaaS, a parte l'eventuale problema del loro prezzo, spesso troppo alto proprio per le realtà più piccole.

6.3 Ruolo della persona rispondente

La fig. 6.3-1 mostra la ripartizione % del ruolo professionale di chi ha compilato il questionario online OAD 2025.
Al primo posto, con il 26,22%, il proprietario/socio o i vertici manageriali dell'azienda/ente, al secondo posto, con un 22,56%, il responsabile del SI (CIO), e al terzo posto 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 del SI e/o della sua sicurezza.
Al quarto posto il Responsabile della sicurezza informatica, il CISO, con un 9,76%. Teoricamente questa figura dovrebbe essere al primo posto nel compilare un questionario sulla sicurezza digitale, ma in Italia il CISO è presente prevalentemente solo nelle grandi organizzazioni.

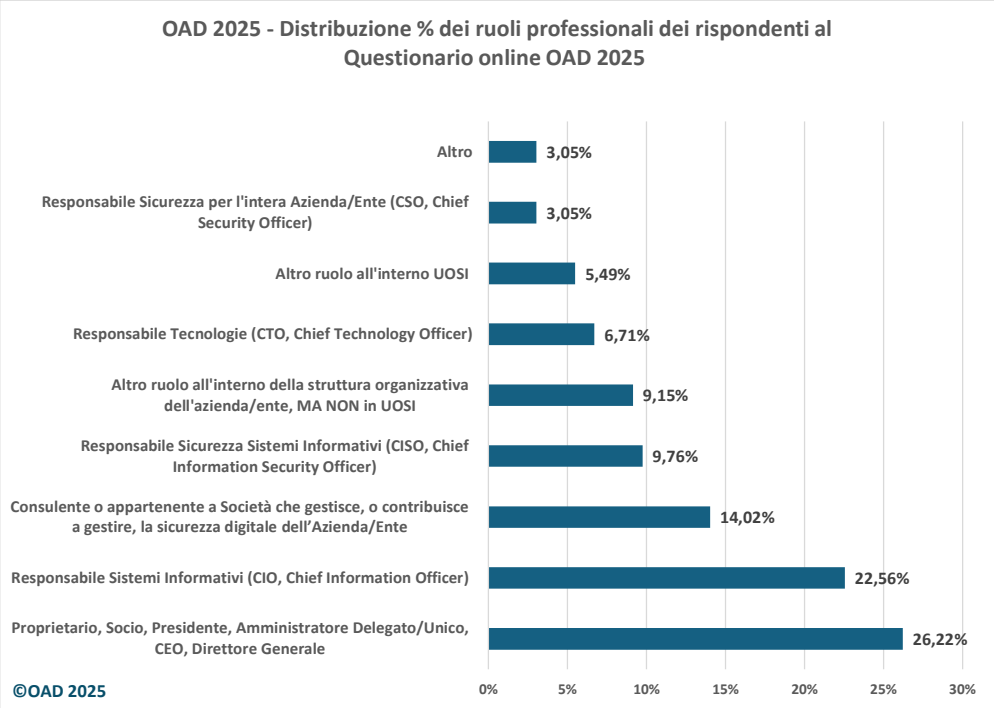


Fig. 6.3-1

Percentuali assai basse per due figure, il CTO, Chief Technology Officer, il responsabile delle tecnologie, ed il CSO, Chief Security Officer, il Responsabile della Sicurezza fisica e del personale per l'intera azienda/ente, ruoli che sono definiti ed operativi soprattutto nelle grandi organizzazioni.
Nella voce Altro è stato indicato il ruolo di DPO, Data Protection Officer, e di Auditor del SI.

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 azienda.

Cap. 7 Le misure di sicurezza digitale nei sistemi informativi (SI)

Nel questionario dell'indagine OAD 2025 le domande sulle misure di sicurezza erano opzionali, si potevano cioè saltare, anche se erano raccomandate soprattutto per le piccole/medie organizzazioni perché potessero ottenere, alla fine della compilazione del questionario, 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 e 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. Per maggiori dettagli si rimanda **all'Allegato A** del presente rapporto.

Hanno risposto alle domande sulle misure di sicurezza il **40,8%** delle/dei rispondenti.
La fig. 7-1 correla percentualmente la ripartizione per settore merceologico, incluse le PA, delle aziende/enti rispondenti che hanno compilato anche la parte opzionale sulle misure di sicurezza in essere nel SI oggetto delle loro risposte.

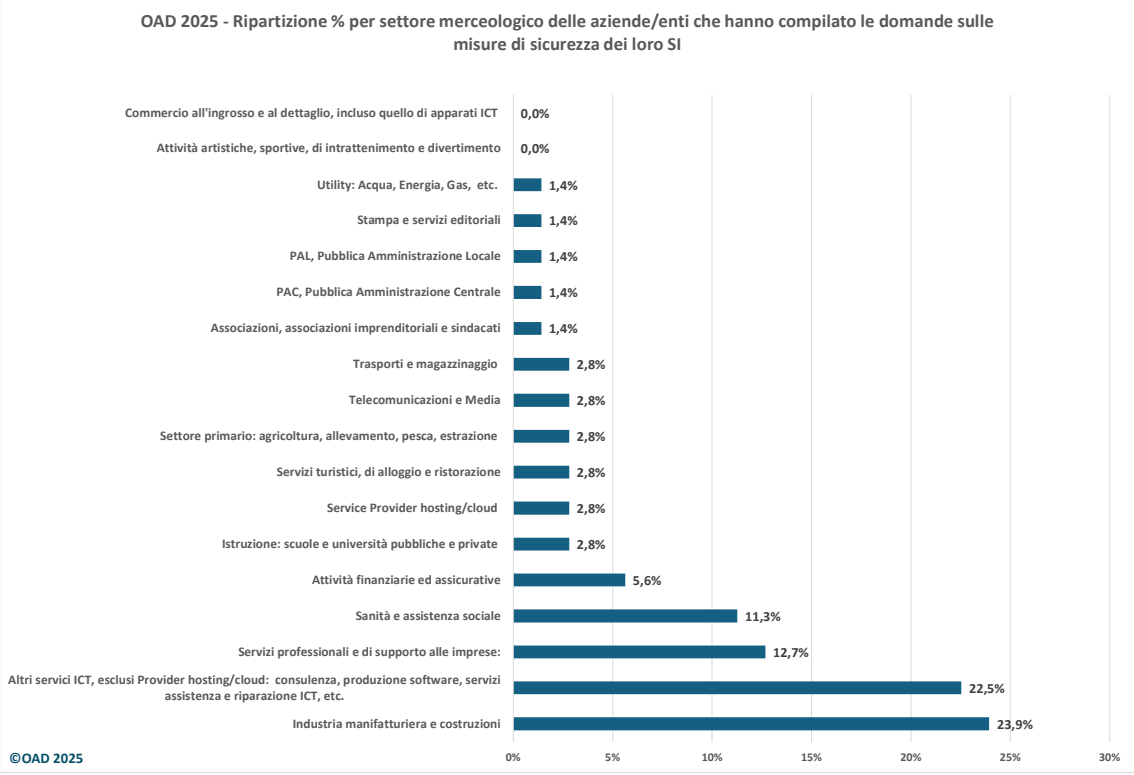


Fig. 7-1

Se si sommano nel loro complesso le aziende dell'**offerta del mondo ICT**, fornitori di hosting/cloud più telecomunicazione e media più i fornitori di altri servizi ICT, il valore complessivo di **28,2%** si posiziona al primo posto.

Singolarmente invece, al primo posto risulta il **settore manifatturiero**, con quasi il **24%**, cui segue con il **22,5%** il settore di "**altri servizi ICT**"; con il **12,7%** , al terzo posto, **i servizi professionali e di supporto alle imprese**, ed al quarto, con **11,3%**, i **servizi sanitari**. Tutti gli altri settori merceologici, incluse le PA, seguono con percentuali molto basse. Non ha compilato la parte opzionale sulle misure di sicurezza nessun compilatore dei settori "commercio" e delle "attività artistiche, sportive e di intrattenimento".
La ripartizione delle maggior parte delle risposte per settore è allineata a quella dei rispondenti all'intero questionario, si veda fig. 6.1-1.

La correlazione più importante, a giudizio dell'autore, è quella tra le aziende/enti che hanno risposto alle domande sulle misure di sicurezza del SI ripartite per dimensione d'azienda/ente come numero di dipendenti.
La fig. 7-2 mostra questa ripartizione, ed evidenzia come più dei 2/3, il **67,6%**, sono organizzazioni **fino a 250 dipendenti**: e tra queste quasi il **24%** è di micro imprese **fino a 10 dipendenti**.
Quasi un 1/3 di grandi e grandissime organizzazioni ha comunque risposto a questa parte opzionale.

La compilazione della parte opzionale consentiva la macro valutazione del livello di sicurezza in essere per il SI, e questo è stato una importante motivazione per compilare l'intero questionario per le aziende/enti di piccole dimensioni, che hanno così effettuato un primo "self assessment" della sicurezza digitale del loro SI. Per le grande e grandissime organizzazioni questa motivazione non è ovviamente determinante, hanno strumenti e consulenti che consentono analisi e assessment ben più dettagliati e sofisticati. Ma comunque quasi 1/3 di loro ha voluto vedere la macro valutazione fornita al completamento del questionario OAD, probabilmente per verificare l'attendibilità e la qualità dell'indagine stessa.
I risultati della macro valutazione del livello di sicurezza dei SI dei rispondenti sono riportati in §7.4

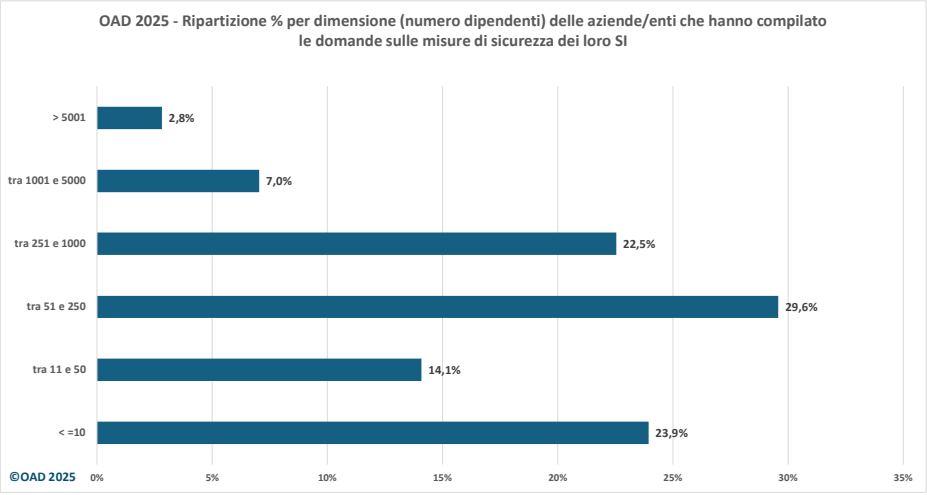


Fig. 7-2

I risultati che emergono da questa parte "opzionale" del questionario OAD 2025, e riportati nei successivi paragrafi, 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.

Il presente Capitolo 7 rileva gli strumenti di sicurezza in uso nei sistemi informativi (SI) delle aziende/enti rispondenti, le cui macro caratteristiche sono riportate nel precedente Capitolo 6.

Gli strumenti e le misure per la sicurezza digitale sono raggruppati in tre sezioni: misure organizzative, misure tecniche, misure per la gestione operativa ("management") della sicurezza digitale.

Le misure di gestione sono un mix di misure organizzative e di strumenti tecnici: l'attribuzione di alcune misure in quale sezione, sempre discutibile, è stata effettuata dall'autore nell'ottica, e nella speranza, di una maggior chiarezza concettuale degli argomenti trattati.

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 strutture, 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.
Le varie nuove direttive e regolamenti europei, oltre al ben noto GDPR per la privacy, (si veda §3.2 e fig. 3.2-1) richiedono tutti l'attuazione di gran parte delle misure organizzative considerate nel questionario OAD 2025. L'obbligatorietà della conformità a queste norme per le aziende/enti specificate, comporta significative pene pecuniarie in caso di inadempienza, e come avvenne fin dalla prima direttiva sulla privacy, dovrebbe ulteriormente favorire l'attenzione e l'effettiva attuazione di tali misure.
In termini di ruoli e competenze per la sicurezza digitale è importante e di riferimento il documento di ENISA **ECSF**, European Cybersecurity Skills Framework, che specifica 12 figure professionali e relativi profili[51], la prima delle quali è il **CISO, Chief Information Security Officer.**

7.1.1 La struttura organizzativa per la sicurezza digitale ed il ruolo di CISO nelle aziende/enti rispondenti

La prima misura organizzativa per la sicurezza digitale è data dalla definizione ed assegnazione del ruolo e delle responsabilità di chi la deve gestire nell'ambito dell'azienda/ente, con l'eventuale relativa struttura organizzativa, piccola o grande, interna o esterna. In funzione del tipo di azienda/ente, in particolare delle sue dimensioni, della sua attività, del settore merceologico di appartenenza, delle certificazioni e delle normative che deve seguire, esistono varie modalità di assegnazione di questo ruolo.
La fig. 7.1.1-1 mostra che nel **35%** delle aziende/enti rispondenti **non** è definito internamente il ruolo di CISO, che è invece di fatto **espletato dal CIO e/o da persone della sua struttura organizzativa** (indicata in OAD come UOSI, Unità Organizzativa Sistemi Informativi). Nel **25,4%** dei casi il ruolo del CISO è **terziarizzato** a consulenti o a società specializzate, in logica MSS, Managed Security Services. Per il **20,63%** delle risposte il ruolo del CISO è ufficialmente definito ed attuato. Nel **19%** delle aziende/enti rispondenti il ruolo del CISO non è definito ed assegnato, probabilmente in queste organizzazzioni nemmeno quello del CIO, in caso di

[51] I 12 profili per la sicurezza digitale specificati in ECSF sono: CISO, cyber incident responder, cyber legal - policy & compliance officer, cyber threat intelligence specialist, cybersecurity architect, cybersecurity auditor, cybersecurity educator, cybersecurity implementer, cybersecurity researcher, cybersecurity risk manager, digital forensics investigator, penetration tester.

bisogno/problemi è il vertice dell'azienda/ente che decide che cosa e come fare; questa in Italia è la tipica situazione per le piccole e micro organizzazioni. Interessante notare che **nessuno dei rispondenti** dichiara che il ruolo di CISO non è definito e designato, ma è di fatto svolto **internamente** da **persone di strutture diverse da quella UOSI**: tipici esempi potrebbero essere quelli del CSO, del CTO, del DPO che di fatto si occupano anche della sicurezza digitale; ma questo non succede nel bacino di rispondenti al questionario OAD 2025.

Una chiara conferma che il ruolo del CISO, con una sua struttura organizzativa, è tipica delle medie grandi organizzazioni è data dalla fig. 7.1.1-2 che correla percentualmente le varie alternative sopra descritte, con le dimensioni, come numero di dipendenti, delle aziende/enti rispondenti. Si noti che l'opzione ultima descritta, che si riferisce al ruolo e funzioni del CISO espletate da altre figure quali CSO, CTO, DPO, non è rappresentata non essendo stata segnalata da alcun rispondente.
La barra azzurra del grafico della fig. 7.1.1-2 c indica che il CISO è definito, svolge il suo ruolo ed ha una sua struttura interna all'organizzazione è **crescente** al crescere delle dimensioni dell'aziende/ente. Nelle microimprese rispondenti non esiste, così come in quelle molto grandi (>5001): quest'ultima indicazione è dovuta semplicemente dalle pochissime aziende di questo tipo che hanno risposto alla parte opzionale del questionario.
La barra arancione, che indica che il ruolo del CISO è espletato dal CIO con la sua struttura, mostra percentuali relativamente alte tra le piccole e medie organizzazioni, ma non è considerata tra quelle grandi, almeno per quelle rispondenti. Analoga situazione per la barra verde, che indica che il ruolo del CISO non esiste e quando necessario le decisioni sulla sicurezza digitale sono prese dal vertice dell'organizzazione.

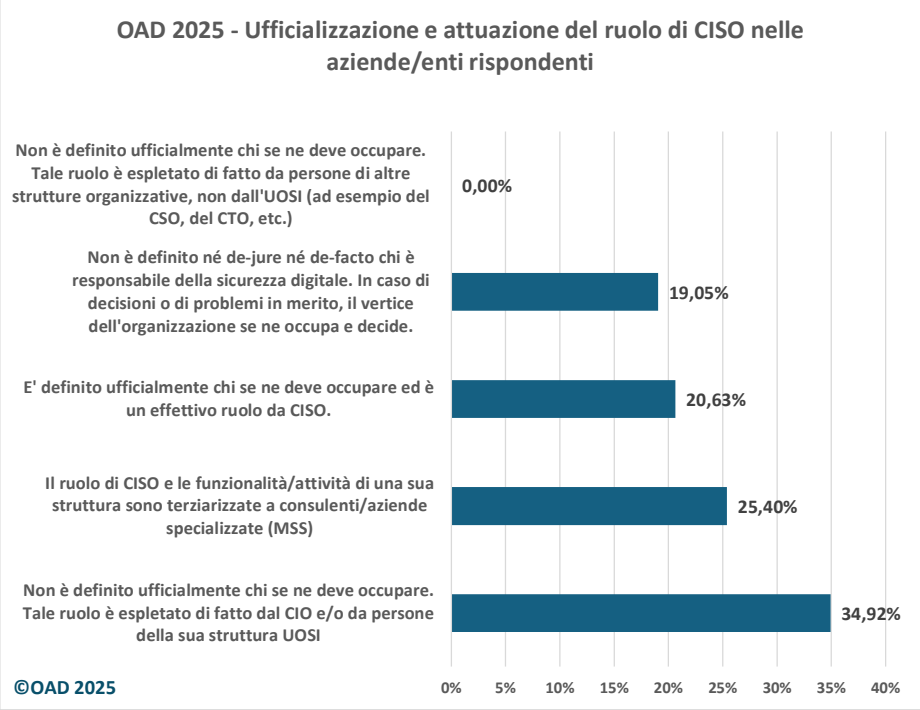


Fig. 7.1.1-1

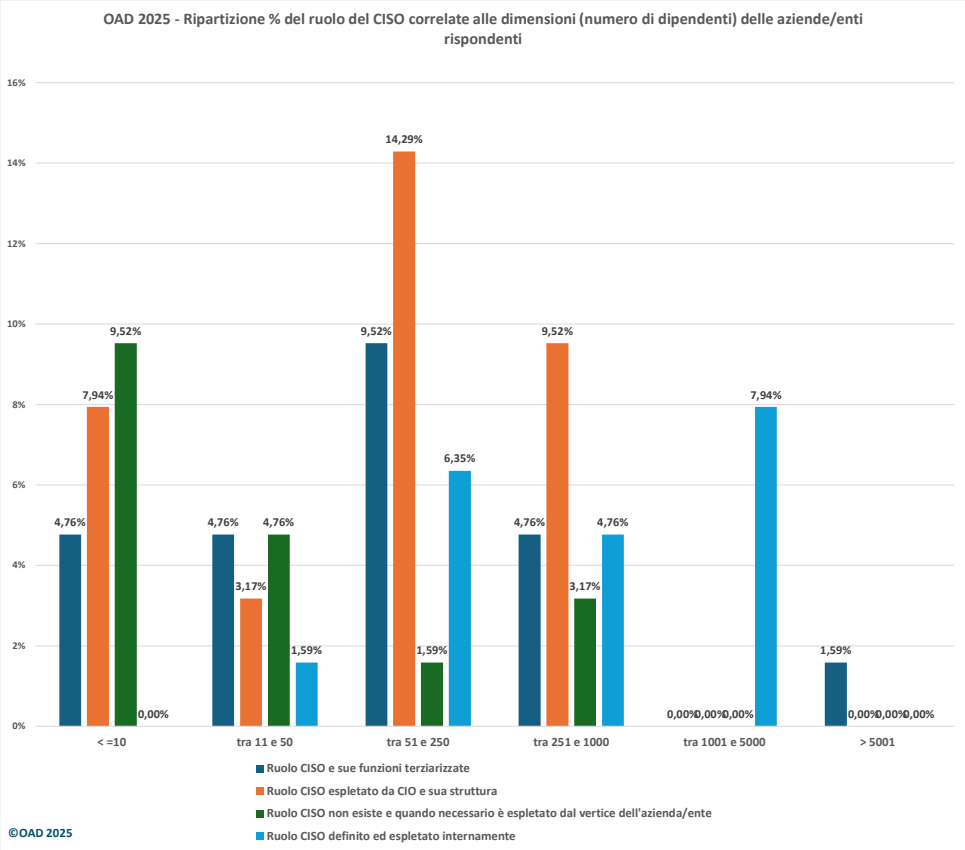


Fig. 7.1.1-2

7.1.2 Policy e procedure organizzative per la sicurezza digitale

Una policy su una determinata attività, nel contesto della sicurezza digitale, definisce le linee guida e gli indirizzi, il più delle volte con valenza pluriennale e strategica, ed è rilasciata, o comunque sottoscritta e validata, dal vertice dell'azienda/ente. Si usa di preferenza il termine inglese "policy", in quanto l'equivalente termine "politica" in italiano è poco usato in ambito informatico e può creare confusione.

Le procedure organizzative, da non confondere con le policy, forniscono dettagliate istruzioni **operative** sia organizzative sia tecniche su come comportarsi per svolgere specifiche attività e per far fronte a determinate situazioni, e sono rivolte sia alle persone che svolgono determinati ruoli, sia alle strutture organizzative che debbono espletare e/o controllare talune attività, funzioni e processi: ad esempio, dalla effettuazione dei back up ai ripristini, dalla creazione e gestione degli account degli utenti alla gestione delle emergenze e dei problemi.

Le policy e le procedure organizzative fanno spesso riferimento a normative che occorre rispettare per legge (i già citati NIS2, DORA, etc.) o per avere specifiche certificazioni, ad esempio per la sicurezza digitale o per la governance del sistema informativo con standard della famiglia ISO e best practice quali le ultime versioni di ITIL e COBIT.

Policy e procedure organizzative scritte, fatte conoscere ed aggiornate periodicamente, non sono da considerare una inutile e costosa burocrazia, e nemmeno attività solo per aziende/enti di grandi dimensioni: sono necessarie ed utili per formalizzare e divulgare come usare e gestire le risorse ICT e la loro sicurezza ad utenti finali e privilegiati, e fornire specifiche indicazioni alle terze parti che possono essere coinvolte nella

gestione e/o nel governo del sistema informativo. Sono inoltre essenziali per dimostrare l'accountability[52], così come richiesto dal GDPR e da altre normative dell'Unione Europea nell'ambito della sicurezza digitale, quali NIS2, DORA, etc.

Il questionario ha posto in merito poche domande:

- la definizione ed uso di policy e procedure organizzative per la sicurezza digitale: nel complesso quasi **l'80%** dei rispondenti l'ha fatto, ma di questi il **52,38%** lo ha fatto solo per alcune attività e funzioni di sicurezza, tipicamente per quelle più necessarie e critiche;
- la definizione ed uso di policy e procedure organizzative per la gestione di incidenti sul sistema informativo e sulla sua sicurezza (incident management): nel complesso il **90%** dei rispondenti l'ha fatto, ma di questi il **36%** dichiara che, anche se formalmente definite, esse di fatto non sono ben conosciute da tutti e non sempre correttamente seguite ed applicate;
- la definizione ed uso di procedure organizzative per l'assistenza agli utenti del SI, Sistema Informativo. Queste procedure sono fondamentale soprattutto per segnalare problemi sulla sicurezza digitale e per SI con numerosi utenti finali. Tale assistenza è realizzata da servizi per gli utenti, gestiti interamente o esternamente o in maniera mista, chiamati "help desk" o "service desk" o "contact center", che supportano gli utenti che hanno problemi nell'uso del sistema informativo e richiedono assistenza. Questi servizi forniscono assistenza con diversi livelli di approfondimento[53] e in logica multicanale, nella maggior parte dei casi anche con applicazioni di "trouble ticketing"[54]. Per la sicurezza digitale, l'help desk è la prima interfaccia del SI con l'utente finale, che può segnalare un attacco digitale o un tentativo di attacco, e tramite le sue banche dati "storiche" ed i sistemi di trouble ticketing può fornire importanti informazioni al CISO e al suo staff, oltre che all'eventuale ERT, Emergency Response Team (si veda anche il §7.2.7 sul Disaster Recovery). La 7.1.2-1 riporta percentualmente la ripartizione delle risposte avute: la quasi totalità delle aziende/enti rispondenti ha e utilizza queste procedure (solo **l'8% non le ha**, tipicamente micro organizzazioni), ma in modalità diverse. L'assistenza con supporto informatico tipo "trouble ticketing" è la più diffusa, con un **56%**, ma di questi il **26%** l'ha parzialmente terziarizzata, ed il **2%** l'ha terziarizzata totalmente. L'assistenza telefonica, senza alcun supporto informatico, è usata dal **36%** delle/dei rispondenti.

[52] Il termine "accountability" significa responsabilizzazione dei diversi ruoli che sono tenuti a dimostrare che le loro azioni ed attività sono coerenti con quanto richiesto dalla normativa, che hanno piani ed iniziative per mettere in atto le idonee misure tecniche e organizzative, che possono comprovarne l'adeguatezza anche tramite adeguati strumenti.

[53] Ad esempio: livello 1 per le domande più comuni e ripetitive, con risposte spesso già definite e automatizzate, livello 2 per richieste che richiedono la risposta e/o l'intervento di uno specialista dell'organizzazione, livello 3 per richieste che richiedono risposte e/o l'intervento dello specialista del fornitore del sistema ICT oggetto della richiesta.

[54] Il "trouble ticketing" è un'applicazione di supporto all'help/service desk (o contact center) che consente di emettere una segnalazione, il ticket, che viene inoltrato a chi può risolvere il problema posto e che a sua volta segnala tramite l'applicazione stessa l'avvenuta risoluzione o che cosa si sta facendo. Questa applicazione permette di registrare e misurare i tempi di risposta e di risoluzione dei problemi posti.

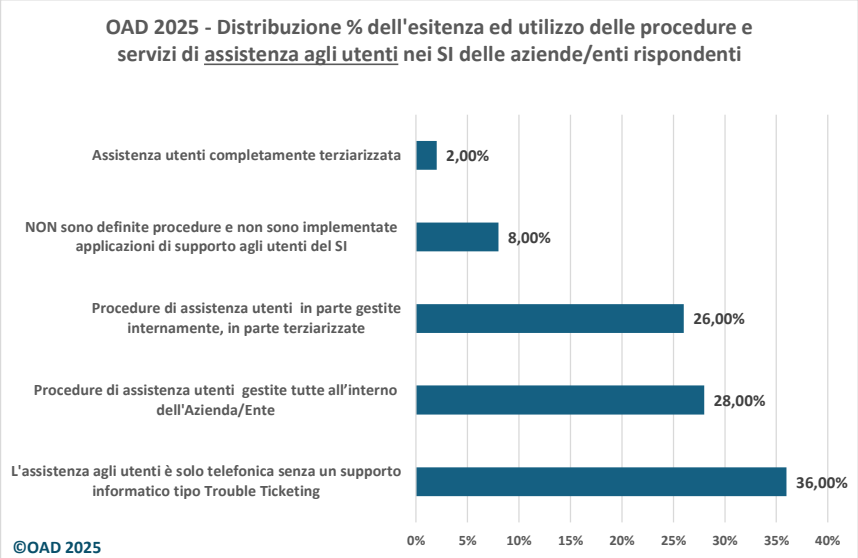


Fig. 7.1.2-1

Per la gestione degli **incidenti gravi**, e non solo riguardanti il sistema informativo, le grandi organizzazioni dedicano uno specifico team, l'ERT (Emergency Response Team o nomi simili), che tipicamente coinvolge non solo il personale dell'UOSI, Unità Organizzativa Sistemi Informativi, ma anche responsabili di altre direzioni e "business unit" dell'azienda/ente.
E' l'ERT che interviene in caso di disastri, e non solo del sistema informativo, per l'attuazione del Piano di Disaster Recovery e ripristinare al più presto la continuità operativa dell'azienda/ente che ha subito il disastro (si veda §7.2.7).
Il **44%** delle aziende/enti rispondenti dichiara di avere un ERT con definite e in uso le relative procedure organizzative, ma di questi solo il **16%** effettua periodicamente prove e simulazioni di casi di disastri: ed è quindi solo questo nucleo di aziende/enti capace realmente di attivare un Disaster Recovery del sistema informativo (SI) in caso di disastro.

7.1.3 Analisi dei rischi digitali e dei possibili impatti

L'analisi dei rischi digitali e dei lori impatti sul sistema informativo (SI), e più in generale sull'intero business e/o attività dell'azienda/ente, è basilare per la progettazione delle misure di sicurezza contestualizzate sulla specifica realtà dell'azienda/ente. L'analisi dei rischi è inoltre richiesta per la conformità a varie norme e leggi, a partire dal GDPR e dal NIS2.
Sono ormai consolidate da anni varie metodiche, best practice e framework per effettuare tali analisi, pur con differenti livelli di dettaglio: dallo standard ISO 27005 a NIST, CRAMM, Mehari, Octave-Allegro, e così via. I rischi digitali dipendono dalle vulnerabilità tecniche, organizzative e delle persone che usano e gestiscono i sistemi informatici e più in generale ogni dispositivo ICT; per una corretta individuazione dei rischi digitali occorre quindi effettuare un'analisi delle vulnerabilità digitali, di cui in §7.2.7.
Con la diffusione capillare di Internet, con la disponibilità di un enorme quantità di informazioni, molte delle quali poco attendibili o non vere, con il potenziale attaccante sconosciuto e a livello mondiale, l'analisi dei rischi si sta evolvendo in logica predittiva[55] grazie all'uso di tecniche di intelligenza artificiale. Uno strumento

[55] Si ricorda che l'analisi predittiva consiste nell'utilizzare dati, algoritmi statistici e tecniche di machine learning per individuare la probabilità di risultati futuri basandosi sui dati storici.

gratuito che aiuta nell'analisi predittiva è il **MITRE ATT&CK**, Adversarial Tactics, Techniques, and Common Knowledge (https://attack.mitre.org/), che fa riferimento alla banca dati CVE delle vulnerabilità (§3.4.1) e consente di classificare, descrivere e simulare specifici attacchi informatici e intrusioni: il suo è crescente nei team dei CISO, di pronto intervento (chiamati spesso Red Team o Emergency Team) e nei SOC.

Dall'indagine OAD 2025 emerge che quasi l'**81%** delle aziende/enti rispondenti effettua l'analisi dei rischi digitali, ma di questi solo il **28,57%** la effettua periodicamente e sistematicamente.
Un numero relativamente basso, considerando l'obbligatorietà di questa analisi richiesta da varie norme, in primis dal GDPR e dal NIS2 (si veda §3.2). Una analisi dei rischi digitali approfondita e periodicamente sistematica è la base per l'individuazione e l'implementazione delle misure di sicurezza che prevengano i rischi individuati o limitino comunque l'impatto sul business e sul SI in caso di loro occorrenza.
L'analisi dei possibili impatti sui processi e sulle attività dell'azienda/ente, analisi chiamata **BIA**, Business Impact Analysis, deve essere effettuata anche per i rischi ICT, ed è richiesta da numerose normative.
Dall'indagine 2025 emerge che la BIA è effettuata dal **68,63%** delle aziende/enti rispondenti che effettuano l'analisi dei rischi ICT. Anche questa percentuale è relativamente bassa, ancora più bassa e di più di 10 punti percentuali rispetto a quanti effettuano l'analisi dei rischi. Una delle cause dipende dal campione emerso di rispondenti, molti dei quali sono microimprese che difficilmente effettuano queste analisi.

Così come per il più generale rischio aziendale, anche per il rischio informatico (o ICT o digitale) si possono stipulare polizze assicurative per l'intero sistema informativo, o per le sue parti che trattano i dati più critici per l'azienda/ente. Occorre precisare che l'attivazione di una polizza assicurativa sui rischi digitali avviene dopo che l'azienda/ente ha implementato e messo in esercizio le necessarie misure di sicurezza, tecniche ed organizzative, per far fronte ai possibili rischi digitali. L'ente assicurativo, infatti, richiede e verifica con suoi esperti che siano in atto tutte le misure di sicurezza idonee, e allo stato dell'arte, altrimenti non stipula il contratto o chiede premi altissimi.
Per il campione emerso dall'indagine OAD 2025, il **23,81%** delle aziende/enti rispondenti ha stipulato una polizza assicurativa sul proprio sistema informativo, ma di questi il **14,29%** lo ha stipulato solo per alcune delle parti più critiche del SI.
La relativa complessità nello stipulare una polizza informatica ed il suo costo, che è fortemente aumentato negli ultimi anni con il crescere del rischio di essere attaccati, sono elementi che attualmente rendono tali polizze fruibili prevalentemente da medie e grandi organizzazioni.

7.1.4 Auditing sulla sicurezza digitale

Con il termine di "auditing" nell'ambito dei sistemi informativi e della loro sicurezza si intende il processo documentato di revisione (ossia verifica, controllo e valutazione) della efficacia delle misure in essere e della loro gestione, oltre che della conformità di tali misure alle leggi vigenti e alle normative, anche interne, che devono o dovrebbero essere seguite. Con il termine di "audit" si intende il risultato di tale valutazione, rappresentato tipicamente da un rapporto all'alta direzione. Sovente, anche tra gli addetti ai lavori, i due termini vengono usati come sinonimi.
L'auditing può essere effettuato con personale interno o con esperti e società esterne, ed alcuni grandi organizzazioni lo effettuano sia internamente che esternamente.
L'auditing della sicurezza digitale è normalmente effettuato come parte del più ampio auditing di un intero sistema informativo, o di una sua parte, volto a verificare che i dati trattati siano corretti, completi ed integri, e che siano facilmente e correttamente usati dai vari utenti.

Dalle risposte avute emerge che il **52,38%** effettua auditing per la sicurezza digitale, e di questi il **30,16%** lo effettua periodicamente in maniera regolare. Valori percentuali abbastanza alti, soprattutto considerando le numerose piccole organizzazioni rispondenti, e per le quali, se non sono del settore ICT, l'auditing della sicurezza digitale non è di forte interesse. Per chi effettua l'auditing della sicurezza digitale, la maggior parte,

il **54,55%**, lo effettua in maniera mista con personale interno e con esperti esterni. Il **27,27%** lo effettua solo con personale esterno, ossia terziarizza questa funzione, ed il **18,18%** lo gestisce solo internamente.

7.1.5 Certificazioni aziendali e individuali sulla sicurezza digitale

L'uso delle certificazioni è basilare non solo per qualificare la persona e l'azienda/ente che ne dispone, ma anche come primo indicatore credibile della effettiva specifica competenza sulla sicurezza digitale e/o sui suoi prodotti, servizi e soluzioni.
In ambito sicurezza digitale esistono numerosi tipi di certificazioni: da quelle indipendenti ed internazionali, quali ad esempio eCF (l'unica con validità legale in Europa, EN 16234-1:2016 (UNI 11506), CISSP, SSCP, CISA, CSSLP, ISO 27001 Lead Auditor, CISM, CRISC, etc., a quelle "proprietarie" rilasciate da fornitori, prevalentemente focalizzate a validare la conoscenza tecnica e sistemistica dei loro prodotti, sistemi e servizi; quasi ogni fornitore di soluzioni per la sicurezza digitale fornisce certificazioni sui suoi prodotti. Le certificazioni per la sicurezza digitale riguardano la singola persona, come quelle elencate sopra, oppure l'intera azienda/ente o solo sue parti (Divisione, Business Unit, ..), con focus sulla sicurezza realizzata per l'intero suo sistema informativo o sue parti. Esempi di queste ultime includono ISO 27001, ISO 27005.
Esistono poi certificazioni sulla sicurezza digitale per le aziende di specifici settori merceologici, ad esempio la Star del CSA (https://cloudsecurityalliance.org/star/) per i fornitori di servizi in cloud.

Il questionario OAD 2025 ha posto tre specifiche domande sulle certificazioni per la sicurezza digitale:

- quelle richieste al personale interno che si occupa di sicurezza digitale;
- quelle richieste a livello di persone e di azienda per i fornitori;
- quelle eventualmente già acquisite a livello aziendale dall'azienda/ente rispondente.

La fig. 7.1.5-1 riporta la richiesta di specifiche certificazioni individuali sulla sicurezza digitale da parte dell'azienda/ente per il suo personale interno che se ne occupa.
La maggior parte delle aziende/enti rispondenti, il **71,43%** non le richiede, ed il **22,22%** le richiede solo per i ruoli e le figure professionali più importanti e di riferimento, quali ad esempio il CISO.

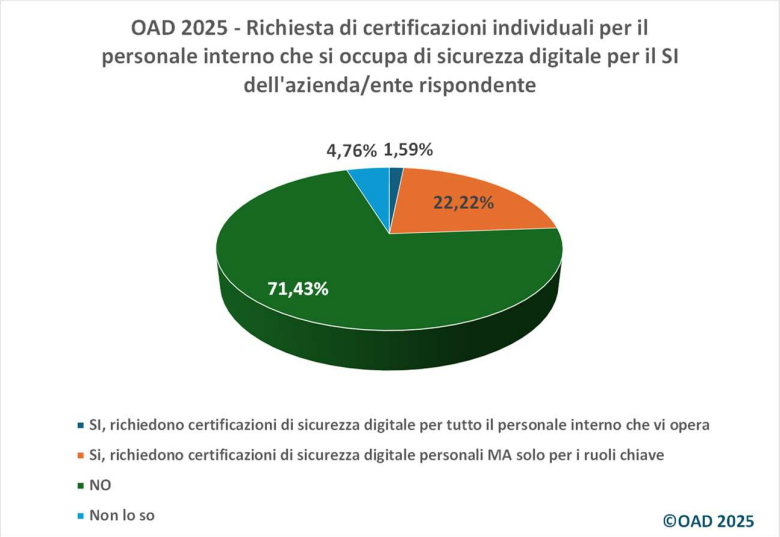


Fig. 7.1.5-1

Nei capitoli e nei paragrafi precedenti si è più volte evidenziata **la tendenza a terziarizzare, in tutto in parte, la gestione della sicurezza digitale**, talvolta, e in crescendo, con più fornitori. Questa terziarizzazione multipla, (simile al "multi cloud", ma per i servizi e sistemi di sicurezza digitale), richiede reali ed adeguate misure di sicurezza da parte dei vari fornitori, che altrimenti potrebbero diventare, con le loro vulnerabilità, i punti di ingresso per l'attacco all'azienda/ente target finale. Proprio negli ultimi anni gli attacchi di questo tipo, chiamati "supply chain attack", sono diventati frequenti e con seri impatti sull'obiettivo target, e la situazione per il bacino di rispondenti è illustrata negli attacchi subiti in §4.1.
L'avere acquisito una o più specifiche certificazioni sulla sicurezza del sistema informativo a livello aziendale per i clienti ed i fornitori collegati informaticamente all'azienda/ente nella supply è un elemento, non l'unico, per una prima garanzia che questi interlocutori dispongo di un adeguato livello di sicurezza digitale. L'azienda/ente dovrebbe chiedere queste certificazioni ai suoi interlocutori che interagiscono con il suo sistema informativo.
Con il generico termine di "Terze Parti" nei grafici sottostanti si fa riferimento a consulenti e società specializzate che intervengono nella gestione operativa della sicurezza digitale, chiamati anche **MSS**, Managed Securiry Services.

La fig. 7.1.5-2 mostra che quasi il **30%** delle aziende/enti rispondenti richiede ai fornitori coinvolti certificazioni sulla sicurezza digitale sia a livello aziendale che delle singole persone che interagiscono con il personale dell'azienda/ente rispondente; il **9,38%** richiede solo certificazioni a livello individuale per il personale che interagisce con l'azienda/ente.
Una larga maggioranza di rispondenti non richiede alcuna certificazione sulla sicurezza digitale per i propri fornitori o per chi interagisce ed interopera con il proprio SI: di qui la criticità sulla supply chain.

Tale criticità è confermata dalle certificazioni aziendali sulla sicurezza digitale che l'azienda/ente rispondente ha già acquisito. Dall'indagine emerge che il **38,10%** già ne possiede almeno una, tipicamente l'ISO 27001, ma di questi il **9,52%** ha certificato solo alcune sue unità organizzative, tipicamente l'UOSI per il SI e la divisione Commerciale/e-commerce.

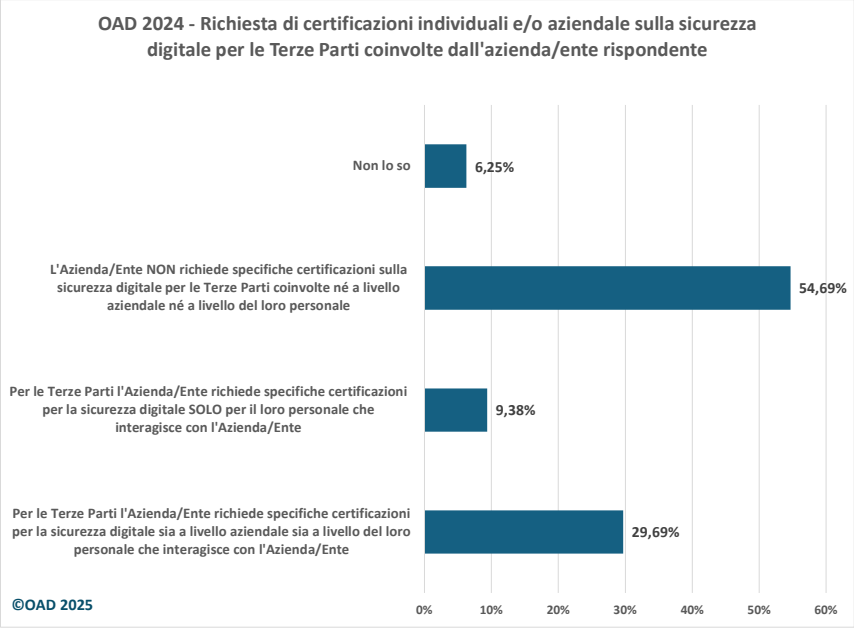


Fig. 7.1.5-2

Le aziende/enti rispondenti hanno già **certificazioni sulla sicurezza digitale a livello aziendale** per il loro SI nel **38,1%** dei casi, e di questi il **28,57%** vale per l'intera organizzazione, il rimanente solo per alcune unità organizzative, quali ad esempio l'UOSI, l'Amministrazione-finanza-controllo, le Risorse Umane.

7.2 Le misure tecniche di sicurezza digitale

Lo schema di riferimento dell'indagine OAD 2023 (e delle ultime precedenti edizioni) sulle misure tecniche di sicurezza digitali in uso nei sistemi informativi delle aziende/enti rispondenti, si articola nelle seguenti classi (chiamate anche "famiglie" di misure):

- Architettura complessiva delle misure della sicurezza digitale, integrata con l'intera architettura del sistema informatico
- Contromisure fisiche
- Misure di Identificazione, Autenticazione, Autorizzazione (IAA)
- Contromisure tecniche sicurezza digitale a livello di reti locali e geografiche
- Contromisure tecniche per la protezione (non fisica) dei singoli sistemi ICT anche terziarizzati/in cloud
- Contromisure tecniche per la protezione del software e degli applicativi dei sistemi ICT anche terziarizzati/in cloud
- Contromisure per la protezione dei dati
- Sistemi di controllo, monitoraggio e gestione della sicurezza digitale
- Piano di Disaster Recovery (DR) con l'allocazione dei relativi ambiti alternativi.

Volutamente l'indagine OAD non fa riferimento a specifiche soluzioni proprietarie, a prodotti e servizi commerciali, e le domande del questionario non sono (troppo) di dettaglio, per non richiedere a chi lo compila troppo tempo e troppe specifiche competenze tecniche.

7.2.1 Architetture per la sicurezza digitale

Dal bacino dei rispondenti emerge che il **42,25%** non fa riferimento ad alcuna architettura di sicurezza digitale nel progettare, acquisire ed implementare gli strumenti di sicurezza per il SI. Quelli che hanno una architettura di sicurezza digitale si suddividono praticamente alla pari tra chi ne fa riferimento per **l'intero SI** o solo **per le sue parti più critiche**.

La fig. 7.2.1-1 mostra la ripartizione percentuale della principale architettura di riferimento usata per l'implementazione della sicurezza digitale del SI. Si tenga presente che molti rispondenti utilizzano contemporaneamente più soluzioni architetturali, tra quelle indicate nel questionario.

Come evidenziato nella figura, le architetture più diffuse includono quelle della famiglia di standard ISO 27000, seguite dal Framework NIST , dalla architettura Zero Trust e dalla SIEM. Altre logiche architetturali hanno percentuali inferiori.

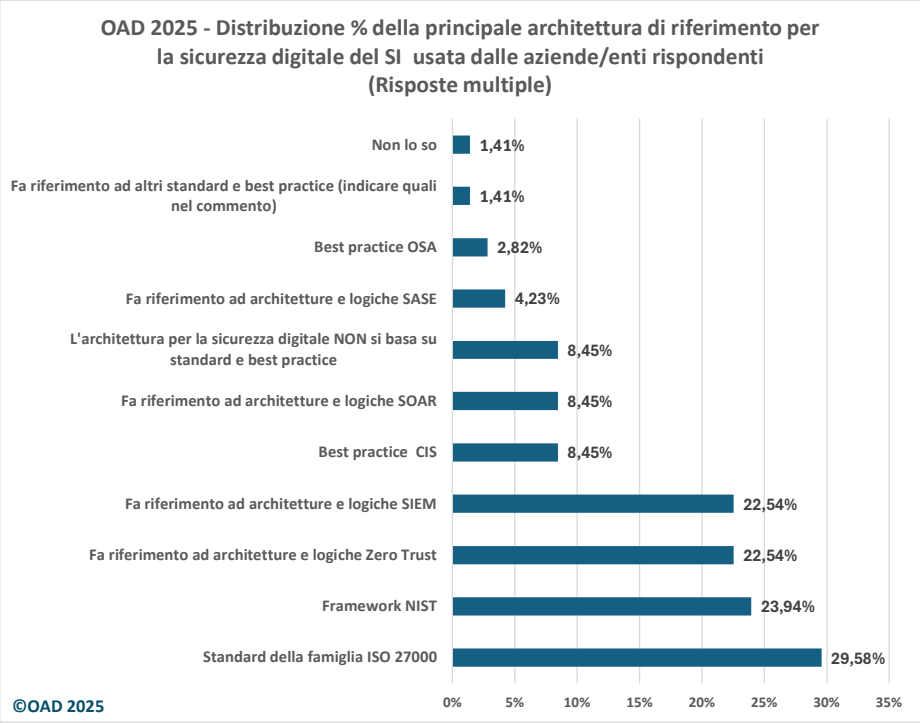


Fig. 7.2.1-1

L'architettura della sicurezza digitale consente anche di ben bilanciare le varie misure/strumenti di sicurezza da adottare, e in particolare di attuare sistemi in alta affidabilità, ad esempio con tecniche di replica in tempo reale su più sistemi.
Dal bacino di rispondenti emerge che il **35%** dispone **dell'intero SI** configurato in alta affidabilità-disponibilità, mentre il **44%** lo ha fatto solo le risorse più critiche del SI.

Alcuni dei SI dei rispondenti hanno uno o più Data Center, che possono avere diversi livelli di affidabilità come definito dallo standard ANSI/TIA 942[56] per il quale si può avere la certificazione TIA del livello implementato. La fig. 7.2.1-2 mostra i livelli di affidabilità del principale Data Center in Italia secondo lo standard ANSI/TIA 942 per i SI delle aziende rispondenti.

[56] Lo standard **ANSI/TIA 942** definisce quattro differenti livelli di affidabilità, chiamati "tier" che fanno riferimento alla misure di sicurezza fisica, in particolare:

- **Tier I**: Data Center dotato di un solo sistema di alimentazione e un solo sistema di raffreddamento con affidabilità al 99,671% l'anno, ovvero un tempo di fermo (imprevisto, non schedulato) di 28,8 ore annue.
- **Tier II**: Data Center dotato di un solo sistema di alimentazione e un solo sistema di raffreddamento ma con componenti ridondati e sistemi di backup e con affidabilità al 99,741%, ovvero circa 22 ore di fermo (imprevisto, non schedulato) nell'anno.
- **Tier III**: Data Center dotato di più sistemi di alimentazione e più sistemi di raffreddamento. Componenti ridondati e sistemi di backup e con affidabilità 99,982% ovvero 1,6 ore di fermo(imprevisto, non schedulato) all'anno.
- **Tier IV**: Data Center totalmente fault tolerant, affidabilità 99,995% e downtime (imprevisto, non schedulato) minore di 26,3 minuti all'anno.

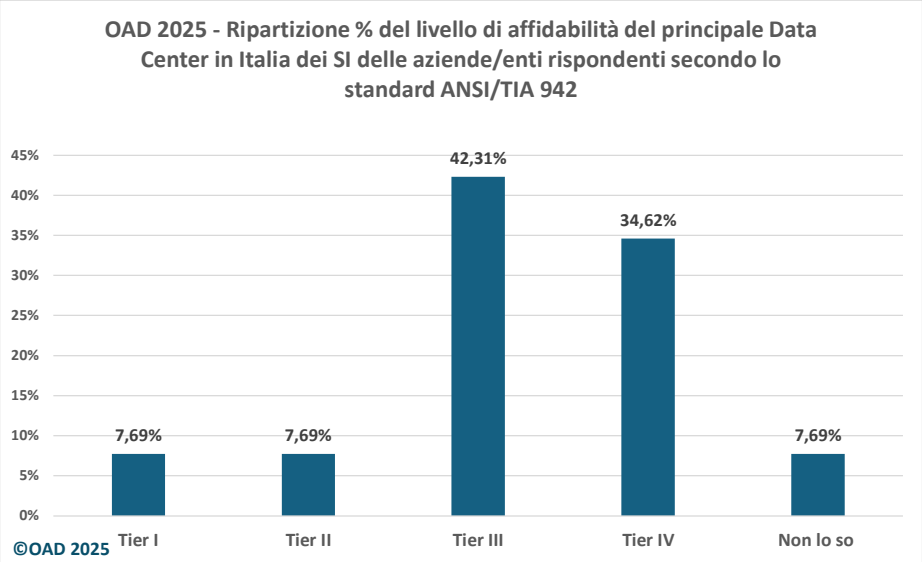


Fig. 7.2.1-2

Il **77%** delle aziende/enti rispondenti dispone di un Data Center in Italia con Tier III o IV, quindi con un buon/ elevato livello di affidabilità. Questo alto livello di affidabilità emerso dall'indagine è congruente con il settore merceologico delle aziende/enti rispondenti (si veda fig. 7-1), con le loro dimensioni come numero di dipendenti e soprattutto per il ruolo del loro SI, più o meno essenziale alle attività e processi dell'organizzazione, ed in taluni casi " risorsa critica" che rientra nelle già citate normative europee quali NIS2, DORA e le altre (si veda fig. 3.2-1).
Solo il **23%** di questi Data Center classificabili ANSI/TIA 942 ha la relativa certificazione TIA.
Questa bassa percentuale conferma ulteriormente il problema delle certificazioni, in particolare quelle aziendali e di riferimento alla sicurezza digitali, di cui anche in §7.1.5.

7.2.2 Misure tecniche di sicurezza fisica e perimetrale

Le misure tecniche per la sicurezza fisica e perimetrali includono (elenco non esaustivo) i controlli per l'accesso delle persone autorizzate nei locali ove si trovano i sistemi ICT, quali la guardiania, le bussole d'ingresso, i lettori di badge ed i sistemi di riconoscimento biometrico, etc., i sistemi per garantire la continuità elettrica (dagli UPS ai gruppi di continuità), i sistemi di climatizzazione dei locali, i sistemi rilevatori di fumo, gas, e umidità, le protezioni perimetrali passive e attive, dalle recinzioni anti-scavalcamento, inferiate alle finestre e alle porte, ai sistemi di allarme antintrusione a radar o a micro onde, i sistemi di videosorveglianza.
Nelle realtà più piccole le misure di sicurezza fisica coincidono con quelle di protezione di queste aree, ossia le porte chiudibili a chiave, le inferriate alle finestre, e così via. Le parti del sistema informativo terziarizzate, ossia in housing/hosting/cloud godono delle misure di sicurezza previste dai fornitori, che nella maggior parte dei casi sono di alto livello.
Viene dato per scontato che l'accesso del personale autorizzato ai locali di un Data Center sia adeguatamente controllato tramite specifici strumenti. Gran parte delle piccole e piccolissime organizzazioni rispondenti hanno, nelle migliori soluzioni, i dispositivi ICT principali (server, storage, unità di rete, etc.) dislocati in un'unica stanza di un ufficio, che viene chiamata da OAD computer room[57], e alla quale possono, o dovrebbero poter accedere solo un numero ristretto di persone, tipicamente l'amministratore dei sistemi ICT ed il

[57] Le computer room, nel caso di sistemi informativi distribuiti sul territorio, sono gli ambienti dipartimentali dei sistemi informativi di medie o grandi dimensioni.

personale esterno per la manutenzione dei dispositivi ICT presenti; in altri casi tali dispositivi sono "distribuiti" nelle diverse stanze degli uffici, così come lo sono i PC degli utenti, ed i controlli dell'accesso fisico sono gli stessi usati per l'accesso a questi locali; in altri casi sono terziarizzati, e l'accesso fisico non è normalmente consentito ai clienti, se non, ma con specifici e severi controlli, per l'housing.

La stragrande maggioranza dalle aziende/enti rispondenti, **l'85,71%**, dispone di misure per il controllo dell'**accesso fisico** di persone nei locali con sistemi ICT, a parte l'eventuale Data Center per il quale si da per scontato che esistano tutte le idonee misure per il controllo degli accessi fisici ai locali nei quali sono sistemati i dispositivi ICT.

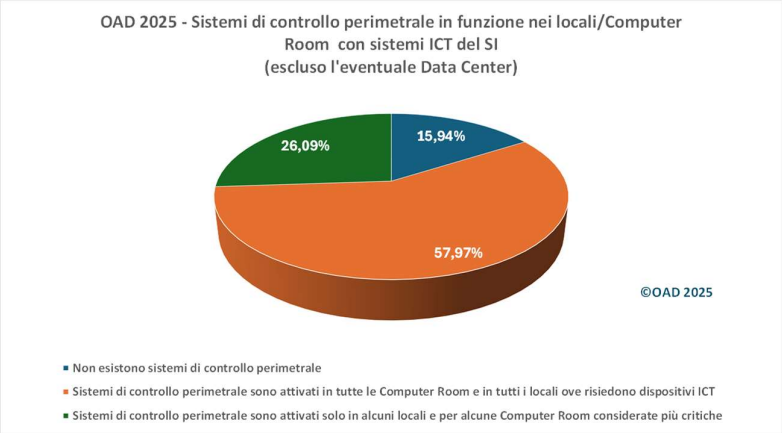


Fig. 7.2.2-1

Sempre escludendo i Data Center, la fig. 7.2.2-1 mostra che nel **84%** dei casi emersi dall'indagine sono in funzione **sistemi di controllo perimetrale**[58] nei locali/computer room ove risiedono sistemi ICT, e di questi il **26%** li ha in funzione **solo** per i locali/computer room con i sistemi ICT **più critici**, ad esempio unità di rete (ruoter, switch, access point, ..) e server-storage di applicazioni critiche, quali ad esempio gestione del personale, contabilità & finanza, ERP, etc.

Un'altra importante misura di sicurezza fisica è l'utilizzo di **sistemi di controllo e prevenzione di interruzioni dell'energia elettrica** per l'alimentazione dei sistemi ICT nelle computer room e negli altri locali in caso di black out energetico. con l'attivazione di gruppi di continuità, indicati con l'acronimo UPS, Uninterruptible Power Supply. Esistono diversi tipi di UPS, da quelli più piccoli, basati su batterie in grado di alimentare per un tempo relativamente breve i sistemi ICT in caso di black out (tipicamente consentono lo spegnimento regolare dei sistemi), a quelli di maggiori dimensioni con generatori di corrente elettrica con motori a benzina/gas, che possono alimentare i sistemi ICT per giorni e giorni (basta ricaricare il serbatoio); questi ultimi sono normalmente usati per i Data Center, mentre per computer room e locali con sistemi ICT sono normalmente usati sistemi UPS statici a batteria. Volutamente il questionario non è entrato in dettagli tecnici, e si è limitato a chiedere l'eventuale utilizzo di UPS nelle computer room.
A parte i Data Center, per il quali si dà per scontato che siano in funzione gruppi di continuità, dal bacino di rispondenti emerge che l'**79,1%**, dispone di UPS nei locali/computer room, ma di questi il **49,25%** li ha in funzione solo per i sistemi ICT più critici.

[58] I sistemi di controllo perimetrale sono simili ai sistemi anti intrusione delle abitazioni, e con diverse tecniche consentono di rilevare la presenza non autorizzata di persone e di attivare i conseguenti allarmi.

Oltre che nei Data Center, la sistemazione in rack[59] dei vari sistemi ICT (switch, router, server, storage, etc.) presenti nei vari locali dell'azienda/ente è importante non solo quale sicurezza fisica, ad esempio con la chiusura a chiave della porta anteriore/posteriore dei rack, ma anche per una loro razionale organizzazione, in particolare per la sistemazione dei cavi in uscita verso gli apparati di rete, che facilita la loro manutenzione ordinaria e straordinaria.
I **rack sono utilizzati** nelle computer room e nei locali ove funzionano dispositivi ICT del SI (non all'interno dell'eventuale Data Center) nei quali sono allocati per il **75%** delle aziende/enti rispondenti, per se in modalità diverse: per il **19,12%** sono usati per tutti i dispositivi ICT in tutte le computer room e gli altri locali ove operano, mentre per il **38,4%** sono utilizzati solo per i dispositivi ICT più critici.
Viene dato per scontato che nell'eventuale Data Center tuti i sistemi ICT siano in rack non accessibili se non da personale autorizzato.

Per ridurre la possibilità di furto di dispositivi ICT fissi, in particolare lap top e stampanti di piccole dimensioni normalmente lasciate negli uffici, possono essere attivati strumenti di fissaggio e blocco di questi dispositivi sulle scrivanie e sui ripiani dove risiedono. Questa misura di sicurezza fisica non è utilizzata dalla maggior parte delle aziende/enti rispondenti, pari al **76,12%**. Il **22,39%** utilizza questi strumenti, ma di questi il **17,91%** solo per i PC, workstation e stampanti più importanti e costosi.

7.2.3 Identificazione, autenticazione e autorizzazione degli utenti

Gli strumenti di identificazione, autenticazione e autorizzazione (IAA) per gli utenti finali e per quelli privilegiati[60] sono fondamentali per l'effettiva protezione di un sistema informativo, tenendo anche conto che gli attacchi digitali all'IAA sono nell'indagine OAD 2024 al quarto posto come diffusione, si veda fig. 4.1-1, e lo furono ai primi posti per diffusione nelle precedenti indagin OAD dal 2017 al 2021 (dal sito https://www.oadweb.it/it/rapporti-e-relativi-convegni.html si possono scaricare i Rapporti OAD di questi anni)
Le tecniche di IAA includono la consueta coppia identificatore utente e password, l'autenticazione forte a due o più fattori, ad esempio con token e con controlli via cellulare e con i certificati (in Italia forte la spinta di SPID[61], obbligatorio per gli utenti delle pubbliche amministrazioni), l'identificazione biometrica e la grafometria, gli strumenti di gestione e controllo degli accessi quali i diffusi Active Directory e l'LDAP, l'uso delle ACL, Access Control List, per la verifica dei privilegi degli utenti abilitati all'accesso alle applicazioni. Viene sempre più spesso usata per gli utenti finali l'autenticazione "**quasi forte**" che oltre ai dati dell'account utilizza una **OTP**, One Time Password, inviata o in posta elettronica o come messaggio, tipicamente SMS, sul cellulare dell'utente.
La fig. 7.2.3-1 mostra la distribuzione percentuale tra i SI delle aziende rispondenti della diffusione **dell'autenticazione forte/quasi forte** per gli **utenti privilegiati**. Solo il **22,39%** degli utenti privilegiati la usa per l'accesso a tutti i sistemi del SI, la maggior parte, il **61,19%**, la usa per i sistemi e le applicazioni più critiche.

Per **l'autenticazione degli utenti finali**, come mostrato nella fig. 7.2.3-2, la maggior parte dei SI, il **58,8%**, richiede l'utilizzo di diverse tecniche di autenticazione a seconda del tipo di applicativo, prevalentemente in funzione della sua criticità e riservatezza per le informazioni trattate, e in certi casi per lo stesso ruolo dell'utente finale. Poco meno del 30% utilizza le tradizionali tecniche di autenticazione debole e solo il 5,9% utilizza l'autenticazione forte per ogni ambiente applicativo. Interessante notare come nessuno dei SI dei

[59] Nel mondo ICT i rack sono armadi modulari , di diverse dimensioni secondo le specifiche di standard quali EIA-310 e CEI IEC-60297x, nei quali installare i dispositivi ICT, il più delle volte opportunamente strutturati per i rack.
[60] Gli utenti privilegiati sono quelli che hanno profili, privilegi e diritti d'accesso speciali per poter operare sulle risorse ICT: ad esempio gli amministratori di sistema, gli operatori ICT, i sistemisti, i manutentori, gli sviluppatori software, i fornitori dei servizi terziarizzati, il personale di supporto delle aziende fornitrici dei vari sistemi ICT, etc.
[61] SPID, Sistema Pubblico di Identità Digitale, è erogato da diversi fornitori qualificati da AgID, e fornisce tre livelli di sicurezza: il livello 1, basato sul semplice uso di un identificativo d'utente e di una password; il livello 2 che aggiunge al livello 1 una OTP, One Time Password; il livello 3 che fornisce una autenticazione forte utilizzando certificati digitali con token.

rispondenti utilizzi SPID come strumento di autenticazione al proprio interno (questo anche per il limitato numero di PA rispondenti al questionario OAD 2024).
Ancora trascurabili le percentuali di chi sta introducendo autenticazioni biometriche, quali Fido2, anche per la necessità ad oggi, nell'ambito Unione Europea (UE), di avere l'autorizzazione ad usarle da parte dei vari Garanti nazionali della privacy.

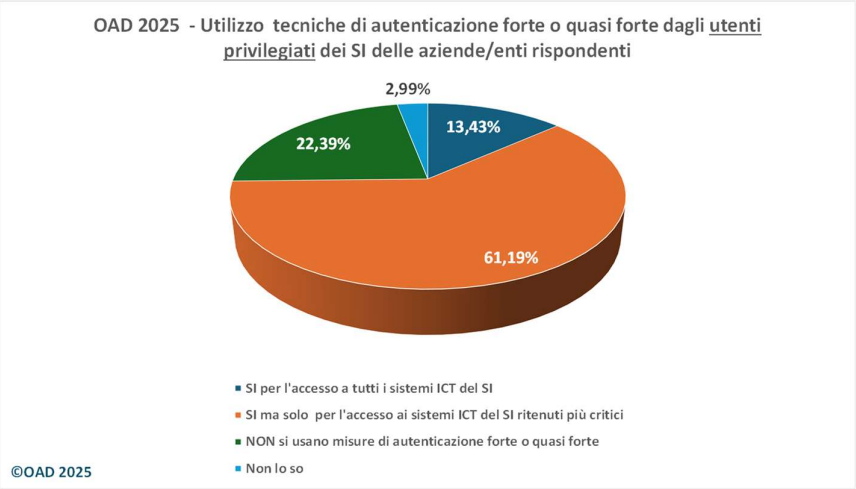


Fig. 7.2.3-1

Anche per **l'autenticazione degli utenti finali**, come mostrato nella fig. 7.2.3-2, la maggior parte dei SI, il **52,4%**, richiede l'utilizzo di diverse tecniche di autenticazione a seconda del tipo di applicativo, prevalentemente in funzione della sua criticità e riservatezza per le informazioni trattate, e in certi casi per lo stesso ruolo dell'utente finale. Il **32,4%** utilizza le tradizionali tecniche di autenticazione debole e il 5,9% utilizza l'autenticazione forte per ogni ambiente applicativo. Interessante notare come nessuno dei SI dei rispondenti utilizzi SPID come strumento di autenticazione al proprio interno (questo anche per il limitato numero di PA rispondenti al questionario OAD 2025), e lo stesso accade per gli accessi tramite servizi quali Amazon, Google e per le autenticazioni biometriche, quali Fido2[62].

L'uso delle password è ancora assai diffuso, i sistemi passwordless[63] si basano tutti su tecniche di identificazione biometriche, che richiedono (richiederebbero) l'autorizzazione all'uso da parte delle Autorità Garanti della privacy, o il cambio di alcune regole nell'attuale normativa sulla privacy.
Il tipo e la gestione delle password degli utenti finali e privilegiati è un annoso problema, di fatto per la gran parte ancora aperto. Una password dovrebbe essere lunga come minimo 12-14 caratteri, e al suo interno avere caratteri speciali[64], non tutti però usabili in varie applicazioni. Problema parzialmente rimediabile con

[62] L'autenticazione biometrica FIDO2 è uno standard di sicurezza che consente l'accesso senza password, combinando l'uso di dati biometrici (come l'impronta digitale) con la crittografia a chiave pubblica e il possesso di un dispositivo, per proteggere gli account online.
[63] Varie tecniche biometriche sono già disponibili e stanno diffondendosi nei moderni cellulari tramite riconoscimento facciale e di impronte digitali. Come già evidenziato nel capitolo, il loro uso, in particolare in ambito business, deve seguire le normative sulla privacy ed avere l'autorizzazione dell'Autorità Garante. Tra le principali tecniche e metodiche per l'autenticazione biometrica è di riferimento il Progetto open source FIDO2, https://fidoalliance.org/fido2/
[64] Il termine "caratteri speciali" è usato con definizioni diverse a seconda del contesto (lingua, caratteri stampabili, caratteri di controllo, standard ASCI-UTF-Unicode etc.). e questo porta ad una certa confusione. Senza entrare in dettagli, per l'utente finale di un SI i caratteri speciali da inserire in una password includono tipicamente caratteri non alfanumerici quali ad esempio ~!@#$ %^&*_-+=`|\(){}[]:;"'<>,.?/ .

autenticazioni forti/quasi forti e con l'uso di PIN[65], che sono codici facili e corti da ricordare da usare associate a token (smart card, chiavette USB, smartphone). In prospettiva l'eliminazione delle password avverrà tramite sistemi passwordless basati sull'identificazione biometrica.

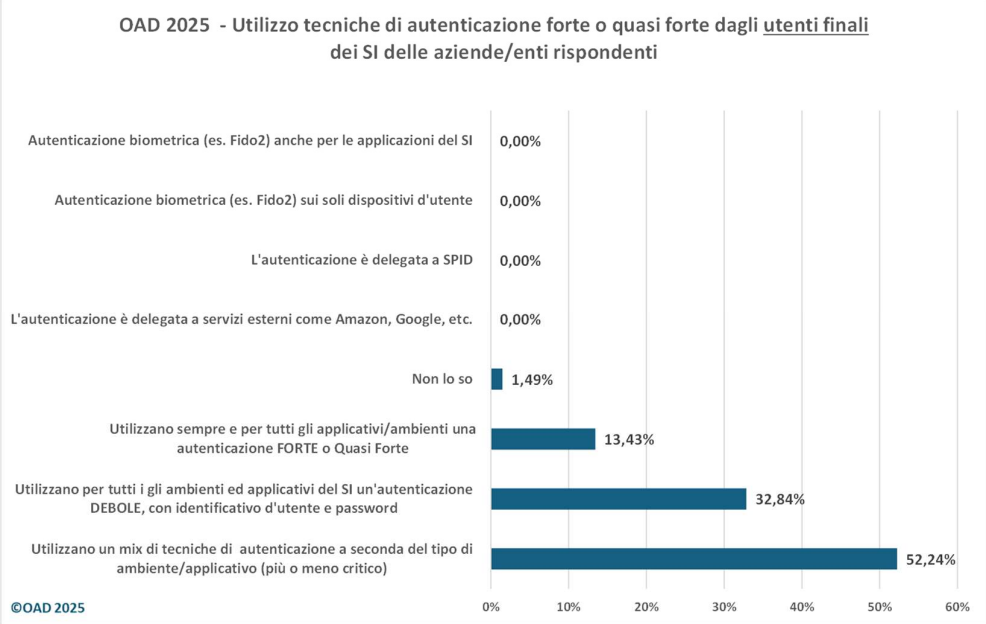


Fig. 7.2.3-2

.

Come mostrato in fig. 7.2.3-3 la **gestione delle password** per un SI è **centralizzata** per tutti gli utenti per quasi il **60%** dei SI, ed è invece lasciata alle decisioni del singolo utente, privilegiato o finale, nel **16,42%**. Nel **20,9%** dei SI è centralizzata solo la gestione delle password degli utenti privilegiati. Nessuno dei SI rispondenti sta usando tecniche passwordless.

[65] Codice PIN, *Personal Identification Number*: sequenza di caratteri numerici usata solitamente per verificare che la persona che utilizza un dispositivo, ad esempio un telefono cellulare, o un servizio, quale un prelievo con carta di debito, sia effettivamente autorizzata a compiere quella operazione (da Wikepidia).

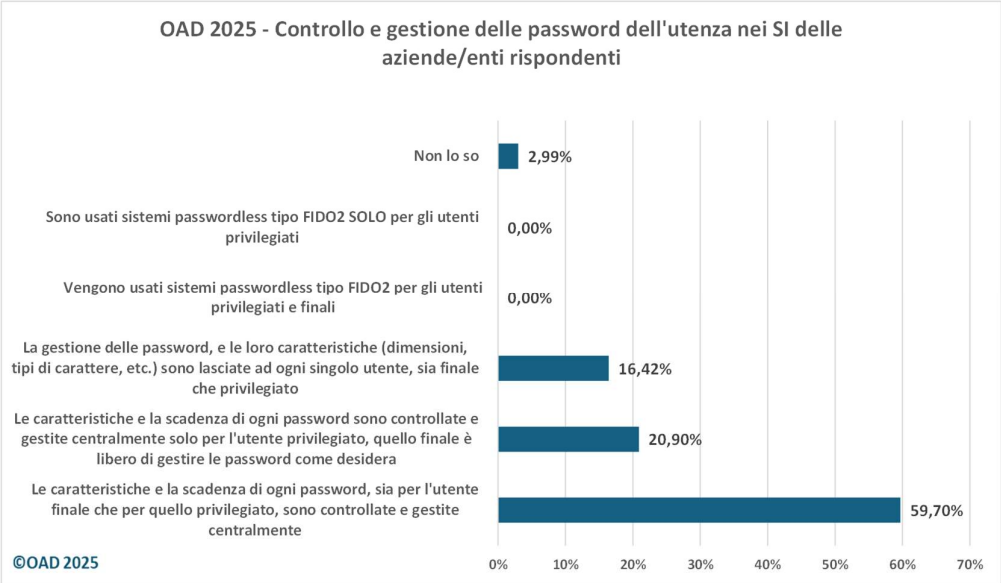


Fig. 7.2.3-3

7.2.4 Misure tecniche di sicurezza delle reti dei SI

Le reti per i sistemi informativi includono le connessioni ad Internet, le reti locali (LAN e WLAN) ed eventuali reti e connessioni dedicate per il sistema informativo, che ormai tendono ad essere dei casi eccezionali, dati anche i loro costi. Numerose le tecniche disponibili, alcune referenziate nelle domande, che includono connessioni multiple in ridondanza per garantire alta affidabilità e disponibilità, dispositivi firewall di rete e DMZ, DeMilitarized Zone (in italiano zona demilitarizzata), crittografia nelle comunicazioni (HTTPS, FTPS) e VPN, Virtual Private Network, IDS/IPS, Intrusion Detection/Prevention System, filtraggio traffico ed indirizzi, analisi comportamentali delle unità di rete intelligenti.

Più dei ¾ dei SI rispondenti, il **75,76%**, ha connessioni multiple, e di questi quasi il **40%** ha tutte le connessioni ad Internet dupplicate/ennuplicate per garantirne una alta affidabilità e disponibilità, il rimanente ha connessioni multiple solo per quelle più importanti e critiche.

Come riportato nella fig. 7.2.4-1, il **54,55%** dei SI monitora e controlla centralmente funzionalità, prestazioni e livelli di sicurezza digitale delle proprie LAN, con l'utilizzo di specifici strumenti quali DMZ, Firewall, IPS/IDS, VPN, e così via. Il **34,85%** non controlla centralmente le proprie reti, ma utilizza specifici strumenti di sicurezza digitale come quelli indicati. Le altre ipotesi considerate nel questionario e mostrate in figura hanno percentuali molto basse.

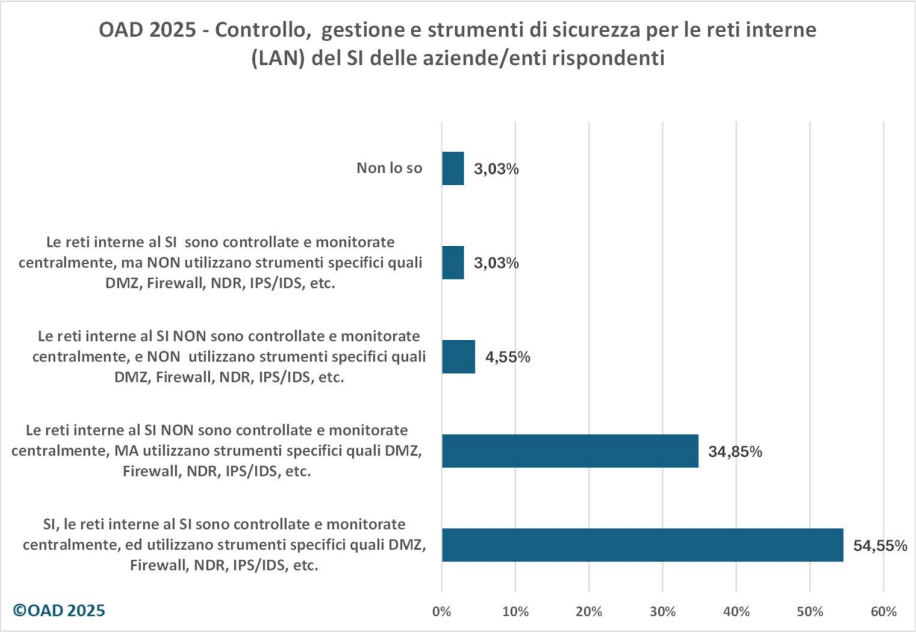


Fig. 7.2.4-1

La trasmissione dei dati nelle reti del SI, e soprattutto su Internet, deve essere protetto tramite crittografia, tipicamente coi protocolli **HTTPS** e **FTPS**.
Dal bacino di rispondenti emerge che per quasi il **90%** del traffico in rete da e per il SI è crittografato.

Per l'autore, questa alta percentuale è ragionevole dato che la maggior parte delle interazioni via Internet usata HTTPS.

Una ulteriore strumento di sicurezza a livello di rete, presente sul mercato da pochi anni, è il SASE, Secure Access Service Edge, [66] che unisce funzionalità di rete e sicurezza digitale in un'unica piattaforma cloud che consente di potenziare il livello di sicurezza delle reti e con fornitori di SASE in cloud, di far fronte ad attacchi tipo DoS/DDoS.
Il **71,21%** di SI delle aziende/enti rispondenti **non utilizza soluzioni SASE** , ma il **25,76% sì**.

7.2.5 Misure di sicurezza delle applicazioni nei SI

Le misure di sicurezza digitale a livello applicativo includono una serie di tecniche e di misure specifiche, dallo sviluppo sicuro del software al controllo della sicurezza intrinseca del codice (ad esempio con reverse engineering, con l'analisi di vulnerabilità del codice e con penetration test), dai firewall applicativi (FWA) all'isolamento da Internet di applicativi critici, dall'aggiornamento sistematico del codice alle clausole contrattuali coi fornitori, dalla sistematica profilatura dei diritti d'accesso degli utenti, sia finali che privilegiati, alla configurazione sicura e all'interoperabilità sicura con altri applicativi, e così via. La sicurezza del software di un applicativo deve, o dovrebbe, essere in primo luogo "intrinseca" e, data la grande diffusione di

[66] SASE, Secure Access Service Edge, è un soluzione architetturale (si veda fig. 7.2.1-1) basata principalmente sul cloud che potenzia la sicurezza delle reti, tipicamente WAN, Wide Area Network, connesse ad Internet e con utenti finali distribuiti ed operanti anche in "mobile" (laptop e smartphone da remote via WiFi e reti pubbliche). La logica e l'obbiettivo principale sono di fornire direttamente alla sorgente della connessione ad Internet (PC-tablet-smartphone degli utenti, dispositivi IoT, etc.) funzionalità di WAN ad alte prestazioni (**miglioramento** tempi di risposta, bassa latenza) con avanzate misure di sicurezza in rete, tipo quelle di un cloud, tra le quali fondamentale una sicura autenticazione dell'utente.

applicazioni commerciali, soprattutto per le PMI, questa dovrebbe essere garantita dal fornitore. La specifica responsabilità del fornitore di software (e più in generale di una qualsiasi prodotto ICT) nel garantire per esso gli idonei livelli di scurezza digitale rientra nel già citato Cybersecurity Act dell'UE (si veda §3.4): ogni prodotto software, o con software interno (embedded) perché possa essere venduto dovrà essere certificato da appositi enti dell'UE (anche a livello delle nazioni UE), in un logica tipo Common Criteria europeizzati.
Al di la sicurezza intrinseca del software, esso può essere corrotto anche da errate installazioni e configurazioni, e da moduli aggiunti per l'integrazione e l'interoperabilità con altre applicazioni.
Inoltre, come già riscontrato nelle precedenti indagini OAD, alcune società acquirenti di software commerciali non rinnovano poi, per motivi economici, i contratti per la loro manutenzione correttiva ed evolutiva, lasciando così in produzione nei loro SI software non aggiornati, e quindi vulnerabili e facile preda degli attaccanti.
Sul complesso ed ampio ambito della sicurezza degli applicativi software, OAD 2025 volutamente ha posto nel questionario poche domande ma tali da poter rilevare la tendenza delle aziende/enti rispondenti.

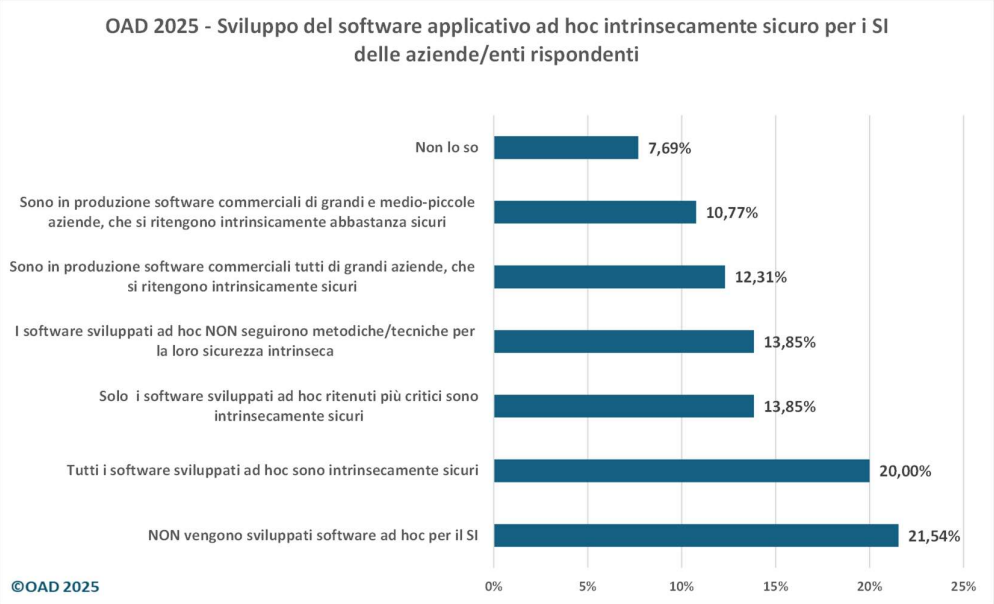


Fig. 7.2.5-1

La fig. 7.2.5-1 mostra che il **20%** dei software applicativi sviluppati ad hoc hanno seguito procedure e metodiche di sviluppo sicuro in modo da garantire una sicurezza digitale intrinseca del codice, ad esempio senza bachi, senza porte aperte (back door), e senza altre vulnerabilità; il **13,85%** dichiara che tale sviluppo sicuro è stato effettuato solo per gli applicativi più importanti e più critici per l'azienda/ente; il **23%** delle aziende/enti rispondenti ha acquisito e posto in produzione applicativi commerciali di note case produttrici, di grandi o di piccole dimensioni, che sono ritenuti intrinsecamente sicuri o abbastanza sicuri.

La seconda domanda riguarda **la verifica ed il test della sicurezza del codice software sviluppato ad hoc prima della sua messa in produzione**: le risposte avute indicano che in circa il **50%** dei SI il software sviluppato ad hoc viene verificato/testato prima della sua messa in produzione, e di questi il **33,85%** riguarda verifiche e test solo delle applicazioni considerate più importanti e critiche.

Il controllo delle autorizzazioni per l'accesso nei vari applicativi e che cosa poter fare, ossia **la profilatura degli utenti per ogni applicativo**, è un altro elemento basilare per la loro sicurezza. Nel **93,75% dei SI** delle aziende/enti rispondenti sono attivi strumenti di controllo degli accessi e delle autorizzazioni agli applicativi, ma di questi solo il **45,31%** sono attivi per tutti gli applicativi.

Uno degli strumenti più efficaci nella protezione degli applicativi in produzione è l'uso di **FWA, Firewall Applicativi**. Dal bacino di rispondenti emerge che **l'80%** dei SI li usa, ma il **20,31%** solo davanti ai server che supportano gli applicativi più importanti e/o più critici per l'azienda/ente rispondente.

Un altro aspetto fondamentale per la sicurezza digitale degli applicativi è la loro **continua e sistematica manutenzione correttiva**: tempestivo aggiornamento delle versioni rilasciate, installazione tempestiva di fix e patch, e così via. Dalle riposte avute, l'**84,7%** gestisce la manutenzione correttiva degli applicativi, e di questi il **59,38%**, ossia ben più della metà, la effettua per tutti gli applicativi operanti nel SI, dagli applicativi nei PC a quelli sui server e a quelli terziarizzati (in particolare in cloud).

7.2.6 Misure tecniche di sicurezza digitale per la protezione dei dati nei SI

I dati trattati dal sistema informativo costituiscono un reale ed importante bene (asset) per l'azienda/ente, e come tali devono essere protetti e gestiti. Numerose le tecniche e gli strumenti per la loro protezione, a partire dalla classificazione dei dati trattati in merito alle loro necessità di protezione. La classificazione è, ad esempio, necessaria per la privacy per l'individuazione dei dati personali e "sensibili. Come strumenti per la protezione dei dati seguono poi la crittografia dei dati critici e riservati, inclusi quelli personali, e le tecniche di back up e di ripristino.
La situazione della classificazioni dei dati per i sistemi informativi oggetto dell'indagine indica che il **76,56%** dichiara di aver classificato i dati, e di questi il **20,31%** dichiara di averlo fatto solo per i dati trattati da alcune applicazioni: tipicamente i dati personali e quelli confidenziali per il business e/o per le attività.

Non stupisce che per il **18,75%** dei SI non sia stato (ancora) classificato alcun dato, pur essendoci leggi, quali quelle sulla privacy, da più di 25 anni: il motivo, a giudizio dell'autore, è la significativa presenza, tra i rispondenti, di microimprese, che difficilmente effettuano (o fanno effettuare da consulenti) questo tipo di attività.

La **crittografia,** secondo algoritmi standard e consolidati, è la **tecnica più sicura per proteggere i dati trattati**, e soprattutto per quelli soggetti a leggi e normative vigenti, come ad esempio i dati personali normati dalla direttiva GPDR sulla privacy.
La fig. 7.2.6-1 riporta la situazione sul trattamento dei dati personali, in particolare di quelli "sensibili"[67]: il **37,5%** delle aziende/enti rispondenti criptano i dati personali sensibili. La maggior parte, il **40,63%** dichiara di non trattare dati personali sensibili. Questa percentuale è ragionevole, dato che quasi tutti i SI trattano dati "personali", ma molti meno quelli sensibili.

[67] Il termine di "dato sensibile" non è più citato nella direttiva GDPR, ma lo era nelle precedenti; esso è di comoda sintesi, ben conosciuto anche al di fuori degli addetti ai lavori, e si riferisce a dati personali di tipo sanitario, religioso, politico, sindacale, etc.

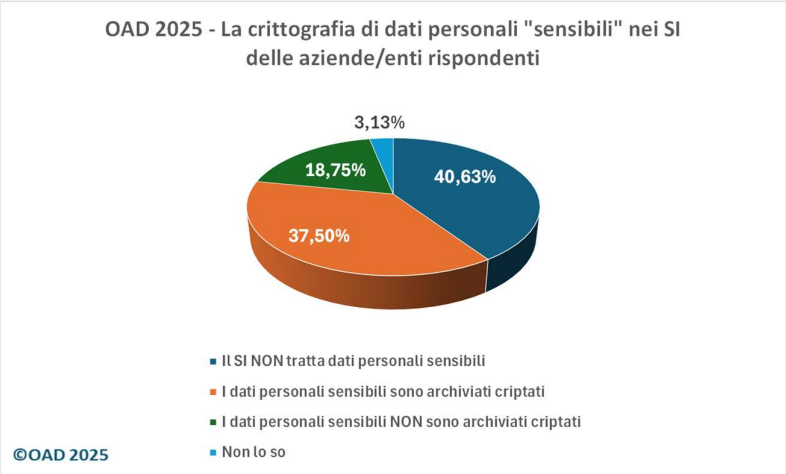


Fig. 7.2.6-1

Vengono poi criptati dati ritenuti riservati e confidenziali, non di tipo personale, dal **50%** delle aziende/enti rispondenti: questa percentuale da un lato indica come buona parte dei SI dei rispondenti abbiano un buon livello di misure di sicurezza, dall'altro come gli strumenti per criptare dati/file siano ormai diffusi e relativamente facili da usare.

Le **chiavette USB** sono un **comodo strumento per copiare file**, e date le loro attuali grandi capacità di storage, anche per copiare directory di qualche Tera Byte. Quasi tutti i dispositivi ICT, dai PC ai server, dagli storage alle unità di rete, hanno porte USB per default aperte ed utilizzabili, che dovrebbero invece essere controllate/bloccate. Le chiavette sono un utile strumento per fare delle copie dei propri file, archiviandoli in maniera sicure crittografandoli, ma anche **per rubare "fisicamente" significative quantità di dati e/o manipolare con opportuni software il sistema, ad esempio inserendo un malware**. Ulteriore rischio è che la chiavetta possa essere facilmente persa o rubata, e se non ha i dati criptati il rischio di loro improprio ed illegale utilizzo è veramente alto. Dall'indagine 2025 emerge che la maggior parte dei SI dei rispondenti, il **76,56%**, lascia le porte USB nei dispositivi ICT liberamente utilizzabili, esponendo quindi questi dispositivi a molti rischi.

Il **backup** è una essenziale misura per la protezione dei dati e dei programmi di un sistema informativo, e nelle prime indagini OAD si era rilevato come molte aziende/enti rispondenti lo effettuassero parzialmente e/o in maniera poco professionale. La fig. 7.2.6-2 riporta i dati emersi dalla presente indagine: il **43,75%** dei sistemi informativi effettua il backup "a regola d'arte": tutti i dati ed i codici software sono regolarmente e periodicamente backuppati in maniera automatica, con copie dei backup criptate su media removibili (es: hard disk removibile e off line) e allocate in sedi geograficamente diverse da quelle ove risiedono i dispositivi ICT oggetto del backup, quali i Data Center e le Computer room. Il **34,38%** effettua regolarmente i backup, ma non cripta le copie e non trasferisce questi dati su media removibili, allocandole poi in diverse sedi. Il **10,94%** non gestisce in maniera omogenea ed automatizzata il backup, ed il **4,69%** lascia la responsabilità del backup al singolo utente, tipica soluzione delle piccolissime organizzazioni.

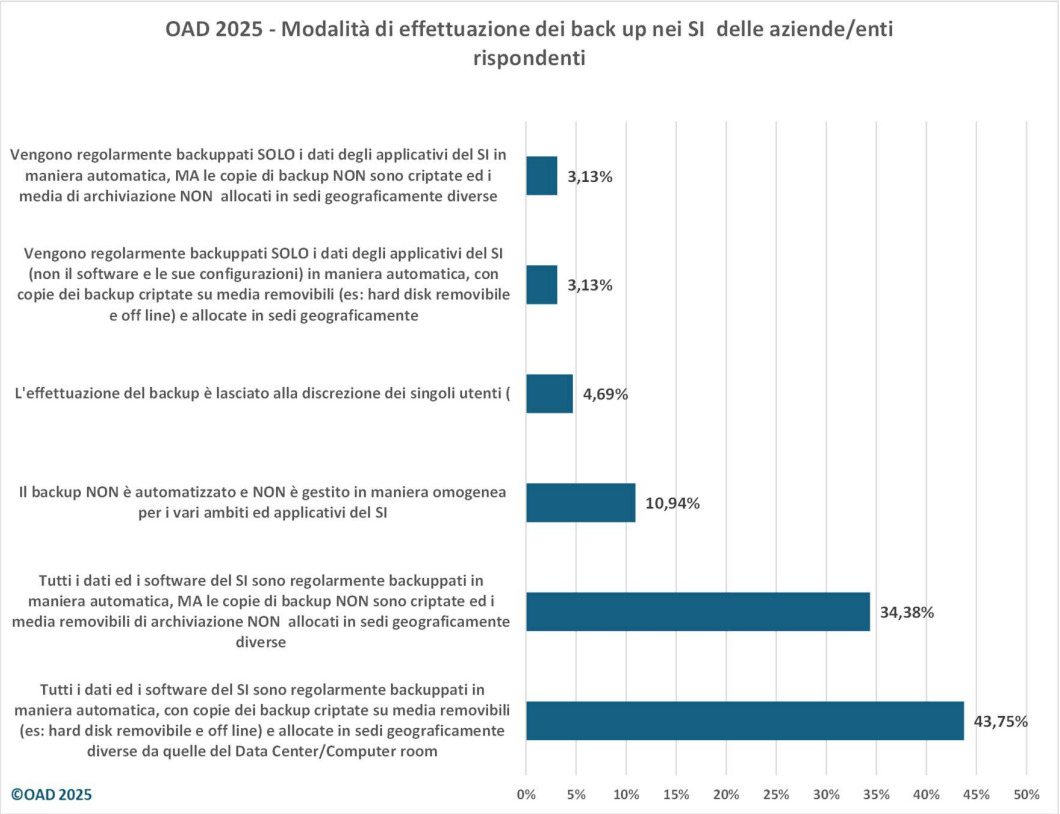


Fig. 7.2.6-2

Per una effettiva disponibilità dei dati del sistema informativo non solo occorre effettuare frequenti, periodici e sistematici backup, ma anche **saper ripristinare uno o più sistemi ICT, in caso di loro malfunzionamento o blocco o rottura, tramite i dati di backup**. Dall'indagine emerge che il **76,56%** delle aziende/enti rispondenti ha definito, ufficializzato ed utilizza procedure per come ripristinare i vari sistemi dai dati dei backup, e di questi il **40,63%** periodicamente le verifica e prova con test, rendendosi quindi in grado di usarle correttamente e tempestivamente quando necessario. Il **17,19 %** non ha definito procedure di ripristino.

7.2.7 Misure e strumenti per la gestione ed il controllo della sicurezza digitale

Le misure e gli strumenti per la gestione della sicurezza digitale di un sistema informativo nel suo complesso sono un insieme di strumenti tecnici ed organizzativi, ed alcuni possono essere considerati anche come misure e strumenti di contrasto.

L'autore ha preferito evidenziare in un paragrafo a sé stante gli strumenti di solito usati per la gestione operativa della sicurezza digitale, che in molti casi è integrata con la gestione del sistema informativo e dei suoi componenti.

Le misure e gli strumenti che sono stati fatti rientrare nell'ambito della gestione della sicurezza digitale, e che sono un di cui della più generale gestione dell'intero sistema informativo, includono i sistemi di directory di tutte le risorse digitali e delle loro configurazioni e licenze (**ICT Asset Management**), i sistemi di **monitoraggio e controllo delle funzionalità e delle prestazioni dei sistemi ICT**, i sistemi di raccolta, correlazione e gestione di tutti gli eventi (**SIEM**) rilevati dai sistemi ICT, ed in particolare i sistemi per la **raccolta e la gestione dei log** dei sistemi ICT e degli utenti (che sono sovente inclusi nei sistemi SIEM), i sistemi di "orchestrazione" **SOAR**

(Security Orchestration, Automation and Response), che consentono di automatizzare e di velocizzare la gestione della sicurezza digitale, in particolare degli incidenti/attacchi digitali, i sistemi **SASE** (Secure Access Service Edge), i sistemi di **analisi comportamentale di utenti e risorse ICT**. Oltre a queste misure e strumenti, che per lo più operano in maniera continua e in tempo reale o quasi, sono considerati alcuni strumenti e logiche già citate o trattate nei paragrafi precedenti, quali gli strumenti di **analisi e di gestione dei rischi** ed il **Disaster Recovery (DR)**.
Tra gli strumenti e le tecniche che in maniera crescente sono utilizzate per una efficace ed efficiente gestione della sicurezza digitale, e più in generale dell'intero sistema informatico, sono quelle di Intelligenza Artificiale, che includono i sistemi esperti ed il machine learning.

Lo strumento basilare per poter effettuare l'analisi dei rischi ICT e gestire la sicurezza digitale è avere, aggiornato, **l'inventario di tutte le risorse ICT del SI**, hardware, software e terziarizzate.

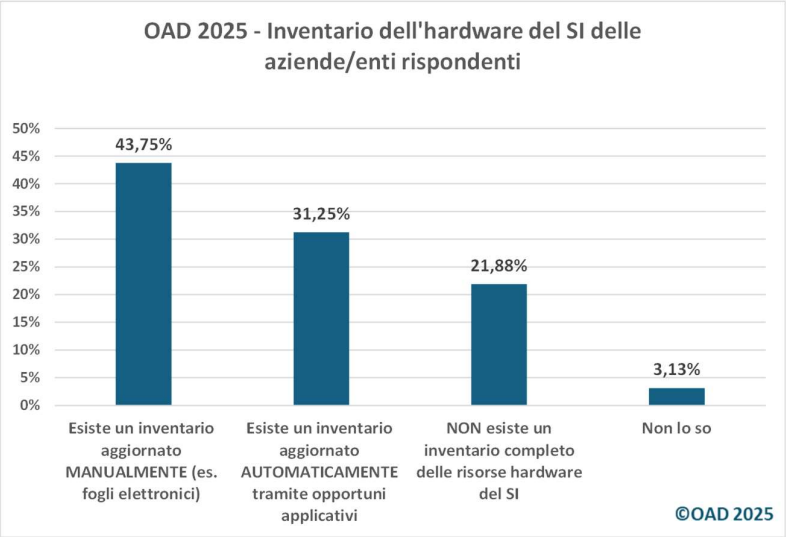


Fig. 7.2.7-1

La fig. 7.2.7-1 mostra la situazione per **l'inventario delle risorse hardware** del SI dell'azienda/ente rispondente: il **21,88%** non ha un inventario delle risorse hardware, mentre il **75%** ha un inventario, ma realizzato in differenti maniere: il **43,75%** di questi realizza una raccolta manuale delle informazioni sull'hardware esistente in fogli elettronici o in altri tipi di documenti; il **31,25%** ha un inventario centralizzato, aggiornato automaticamente con appositi software.
Le **licenze per l'hardware del SI**, necessarie in particolare per la sua manutenzione, dovrebbero essere associate all'inventario, per una loro più efficace gestione. Dall'indagine emerge che dispongono di un inventario dell'hardware con le relative licenze associate **il 54,17%,** ma di questi solo il **25%** riguarda tutte le risorse hardware. Nel **45,83%** dei casi tale associazione tra inventario hardware e relative licenze non esiste.

Per quanto riguarda l'**inventario del software** del sistema informativo, sia di base sia applicativo, la fig. 7.2.7-2 evidenzia che il **28,13%** delle aziende/enti rispondenti non ha un inventario del software, il **65,63%** ha un inventario, ma realizzato in differenti maniere: il **40,63%** realizza una raccolta manuale delle informazioni sul software esistente in fogli elettronici o in altri tipi di documenti, probabilmente gestito e conservato nelle diverse sedi periferiche dove si trovano i dispositivi ICT; il **25%** ha un inventario centralizzato, aggiornato automaticamente con appositi software.

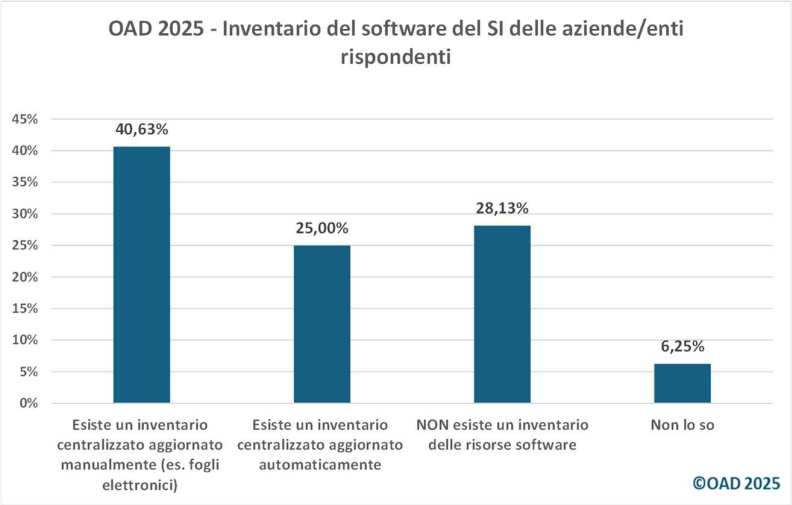


Fig. 7.2.7-2

Soprattutto per il software, le **licenze di manutenzione** dovrebbero essere associate all'inventario software. Come per l'inventario hardware, a questa domanda potevano rispondere solo quelli che avevano dichiarato di avere un inverntario del software. Dalle risposte avute emerge che il **52,38%** delle aziende/enti che hanno l'inventario software non lo correlano con le relative licenze. Per quelli che hanno effettuato e gestiscono tale correlazione, il **33,33%** l'ha per tutti i software inventariati, mentre il **14,29%** ha correlato le licenze solo per alcuni software.

Gli inventari dell'hardware e del software dovrebbero poi essere tra loro correlati ed integrati, per poter saper su quale hardware sono in funzione determinati programmi. La situazione su tale integrazione, limitata alle sole aziende/enti che hanno dichiarato nelle precedenti risposte di avere inventari dell'hardware e del software, evidenzia che il **61,9%** ha i due inventari dell'hardware e del software correlati/integrati tra loro.

Nell'ambito della **gestione operativa della sicurezza digitale**, lo strumento di base è il sistema di monitoraggio e controllo della sicurezza digitale nei vari dispositivi ICT del SI; in alcune implementazioni questo monitoraggio è integrato con quello dell'intero SI, in altri casi è un sistema indipendente, sempre centralizzato, che controlla solo le risorse, hardware e software, che espletano le funzioni di sicurezza digitale. Questi sistemi specializzati talvolta si articolano per specifiche funzionalità di sicurezza, e sovente sono di fornitori diversi. La diffusione di soluzioni in cloud ed il crescere della terziarizzazione della gestione operativa della sicurezza digitale, grazie alla crescita di servizi in rete quali CSaaS, CyberSecurity as a Service, e MSS, Managed Security Services, consente o la totale o la parziale terziarizzazione della gestione operativa della sicurezza digitale.

Nel questionario OAD 2025 si è cercato di semplificare e ridurre le domande su questo argomento, e la fig. 7.2.7-3 mostra i risultati emersi. A parte chi non ha saputo rispondere a questa domanda, solo il **17,19%** dei SI delle aziende/enti rispondenti non ha in funzione alcun sistema di controllo e monitoraggio della sicurezza digitale.

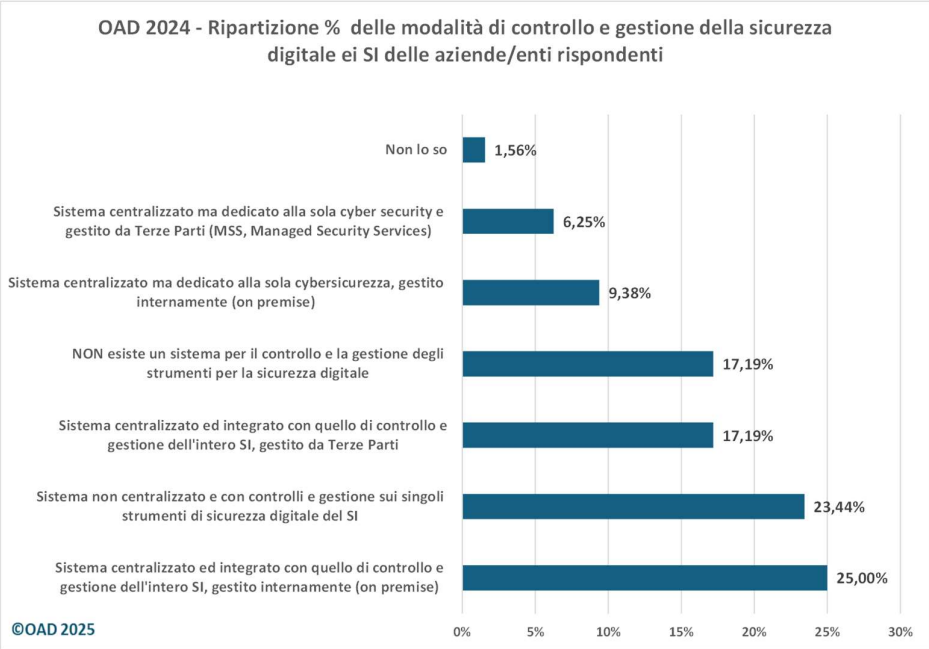


Fig. 7.2.7-3

Tutti gli altri SI hanno sistema di controllo e monitoraggio per la sicurezza digitale: le due tipologie più diffuse riguardano, con il **25%**, i sistemi centralizzati, integrati con quelli di controllo e monitoraggio dell'intero SI e gestiti on premise, soluzione tipica per SI di grandi dimensioni, e con il **23,44%** il controllo non centralizzato ma di ogni singolo sistema ICT in locale, soluzione diffusa nei SI di piccole e piccolissime dimensioni. Il **17,19%** ha terziarizzato la gestione operativa della sicurezza digitale, e sono quindi di Terze Parti i sistemi di controllo e monitoraggio, e da questi ultimi gestiti.

Un altro aspetto importante per la gestione della sicurezza digitale è il settaggio e la **configurazione corretta** delle funzionalità di sicurezza nei sistemi ICT, in particolare per tutte le opzioni inerenti la sicurezza, che troppo spesso non vengono correttamente settate. Dalle risposte avute emerge che nel **47,7%** dei SI delle aziende/enti rispondenti le configurazioni inerenti la sicurezza digitale sono sistematicamente aggiornate, manualmente o in maniera automatica, ma per il **23,1%**, non sono definite metodiche/procedure per correttamente configurare le opzioni di sicurezza all'installazione o successivamente. Per un altro **23,1%** il settaggio/configurazione è effettuato solo alla prima installazione.

Altro aspetto fondamentale nella gestione della sicurezza digitale di un SI è il **sistematico e tempestivo aggiornamento di ogni software in produzione**, da quello di base a quello applicativo. Come più volte evidenziato nei capitoli precedenti, la larga diffusione di ransomware in Italia è causata soprattutto dal non aggiornamento del software, e quindi dalla correzione/eliminazione di vulnerabilità che i ransomware (e più in generale i malware) sfruttano per attaccare il SI. Dalle risposte avute al questionario, emerge che **l'82,54%** aggiorna centralmente e in maniera automatica i software quando segnalato dal/dai Fornitori, ma di questi il **28,57%** lo effettua solo per alcuni software, e non per tutti.

Nell'ambito della gestione operativa della sicurezza digitale rientrano anche **le periodiche analisi di vulnerabilità ed i penetration test (**pentest).

*Si tenga conto che nel questionario OAD **l'analisi dei rischi** è considerata una **misura organizzativa**, mentre **l'analisi delle vulnerabilità** ed i **pentest** sono considerate **misure tecniche**, ivi inclusa l'analisi delle vulnerabilità organizzative e degli utenti.*

Come mostrato nella fig. 7.2.7-4, solo il **15,63%** delle aziende/enti rispondenti non effettua l'analisi di vulnerabilità. E' un dato sostanzialmente positivo, relativo prevalentemente alle piccole e piccolissime organizzazioni rispondenti, controbilanciato da un ampio **42,19%**, poco meno della metà del totale, che effettua l'analisi delle vulnerabilità in maniera sistematica e periodica, e da un **37,5**% che la effettua o quando richiesto dal vertice dell'azienda/ente o in caso di eventi o necessità specifiche, ad esempio dopo un attacco, per verifiche in caso di specifiche certificazioni, e così via. Quindi quasi **l'80%** delle aziende/enti rispondenti effettua l'analisi delle vulnerabilità, analisi che costituisce il primo basilare passo per una corretta implementazione delle misure di sicurezza idonee per uno specifico SI.

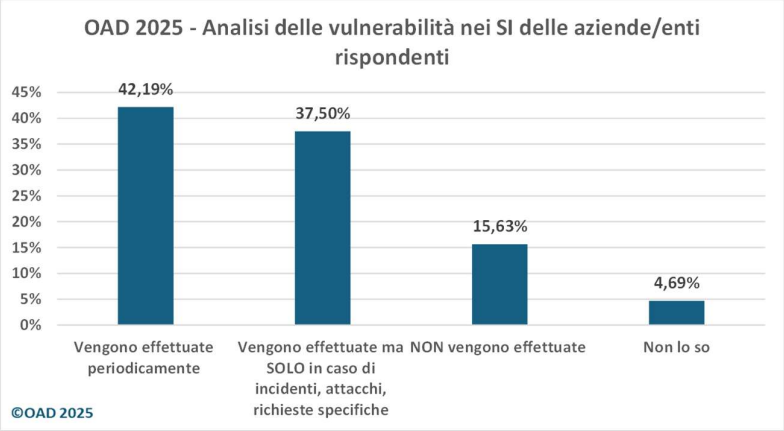


Fig. 7.2.7-4

A fianco dell'analisi delle vulnerabilità, e in particolare dopo aver effettuato opportuni aggiornamenti dei software in uso, è talvolta opportuno effettuare dei **pentest** per verificare che le vulnerabilità individuate siano state soppresse e che le misure di prevenzione e protezione della sicurezza digitale siano correttamente in grado di reagire ai possibili attacchi, verificando con tentativi di penetrazione di prova e non distruttivi.
La fig. 7.2.7-5 mostra che il **47,62%** delle aziende/enti rispondenti effettua pentest, e di queste il **31,75%** li effettua periodicamente e con regolarità, il resto li effettua solo quando richiesto, ad esempio per contribuire ad una certificazione aziendale, dopo l'installazione di un nuovo strumento di sicurezza digitale, etc. Il **52,38%** non effettua pentest.

Si deve tener presente che con l'ampia adozione di applicazioni e servizi in cloud, che nella maggior parte dei casi bloccano i pentest, l'utilizzo di questi ultimi è iniziato a ridursi.

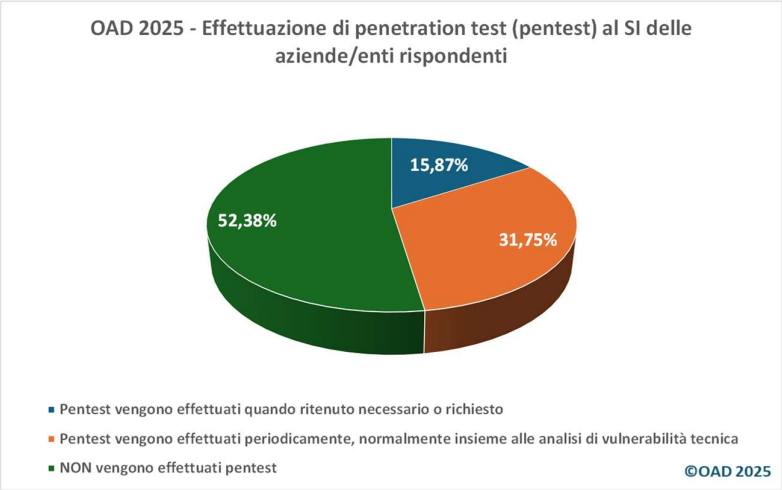


Fig. 7.2.7-5

La **raccolta e la gestione dei log** è un'altra misura utile nella gestione operativa del SI e della sua sicurezza, e che è anche richiesta in alcune normative (tra cui l'obbligo in Italia di archiviazione dei log degli amministratori di sistema dal provvedimento del Garante italiano della privacy del 27/11/2008). Il questionario OAD 2025 ha richiesto solo se viene effettuata la raccolta e la gestione dei log degli utenti, sia quelli privilegiati sia quelli finali.
La fig. 7.2.7-6 riassume le risposte raccolte: a parte un **13,43%** che non raccoglie ed analizza i log, tutti gli altri lo fanno, seppure con varie modalità. Il **32,84%** raccoglie e gestisce i log di tutti gli utenti, mentre il **13,43%** lo fa solo per gli utenti privilegiati, così come è obbligatorio per gli amministratori di sistema.

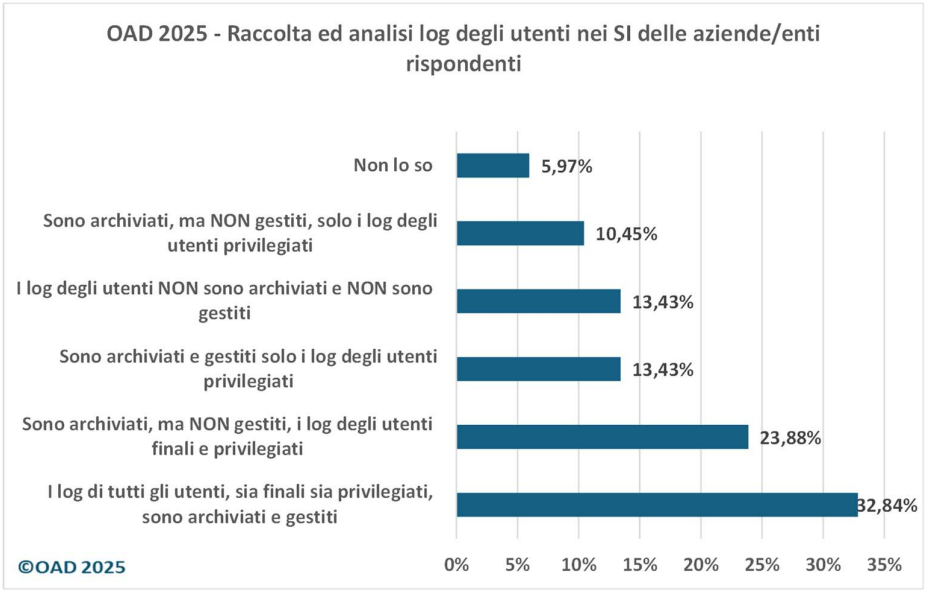


Fig. 7.2.7-6

Nel controllo e nella gestione della sicurezza digitale di un SI va assumendo un'importanza crescente il controllo della sicurezza nella **supply chain con fornitori e clienti** che direttamente interoperano con i loro SI

con quello dell'azienda/ente rispondente. Come evidenziato nei capitoli 3 e 4, stanno crescendo gli attacchi al SI target tramite le vulnerabilità dei suoi interlocutori nella catena informatica della supply chain.

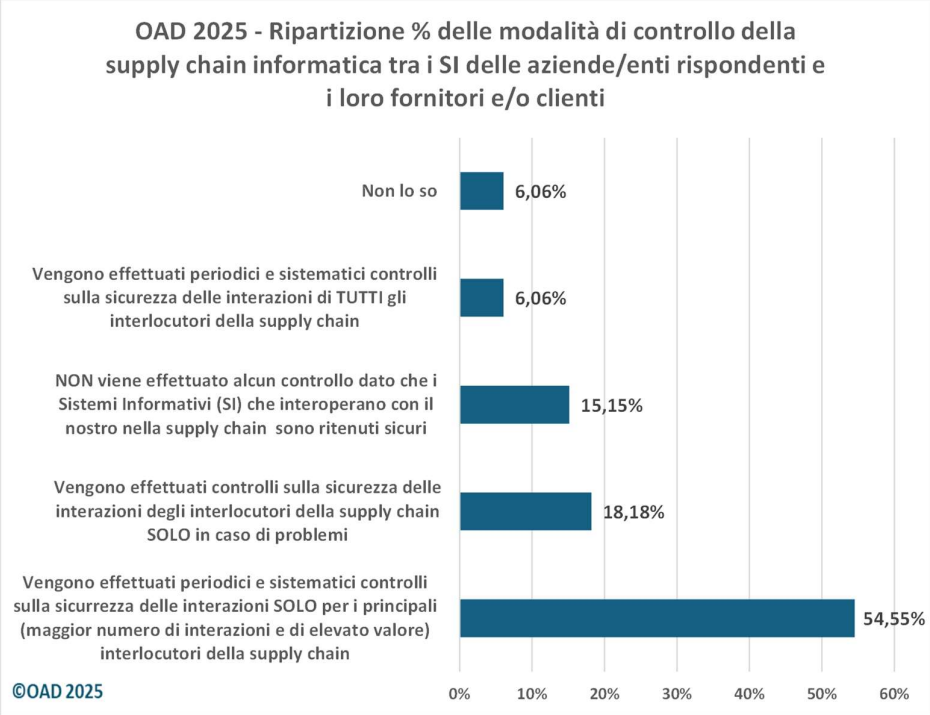


Fig. 7.2.7-7

La fig. 7.2.7-7 mostra che gran parte dei SI dei rispondenti, il **78,79%** effettua un controllo sulle supply chain, e di questi il **54,55%** la effettua solo con i fornitori/clienti più importanti.

Ulteriori strumenti e servizi di significativo ausilio nella gestione operativa della sicurezza digitale sono l'help desk, di cui a §7.1.2, ed il SOC, Security Operation Center. Il primo è un servizio di ausilio per gli utenti dell'intero sistema informativo, e può raccogliere e soddisfare richieste e segnalazioni anche in merito alla sicurezza digitale. Queste ultime sono passate al SOC, se esiste, perché le analizzi e le contestualizzi alla locale realtà, prendendo per le più gravi le opportune decisioni in accordo con il CISO, il CIO e talvolta con il vertice dell'azienda/ente. Dalle risposte avute al questionario si evince che un SOC è usato dal **23,81%** delle aziende/enti rispondenti, e di queste il **14,29%** usa un SOC fornito da Terze Parti, che il **7,94%** usa un SOC "misto" tra suo personale interno ed aziende/specialisti esterni, e solo il **1,59%** gestisce internamente (on premise) il proprio SOC.

E' bene sottolineare che un SOC è tipico di grande organizzazioni e di grandi fornitori di networking/cloud/hosting.

Nell'ambito della gestione della sicurezza digitale un aspetto importante è la definizione di un **Piano di Disaster Recovery (DR) del SI**, che consenta all'azienda/ente, in caso di "disastro", di poter ripristinare in tempi brevi almeno le principali risorse ICT e poter garantire così la (minima) continuità operativa dei processi e delle attività che non possono e che non dovrebbero fermarsi nemmeno in caso di disastro. Per questo motivo il Piano DR fa parte (dovrebbe) del più generale Piano di Continuità Operativa **(Business Continuity Plan**) per

l'intera azienda/ente. I frequenti terremoti ed altri disastri naturali in Italia, oltre alla pandemia Covid-19, le guerre, gli attacchi terroristici, costituiscono un ambito tale da richiedere effettivi piani di DR e di BC anche per medie e piccole organizzazioni, non solo per quelle grandi e grandissime. È necessario inoltre evidenziare la differenza tra avere un piano di DR e disporre delle risorse ICT per poterlo attuare: il piano di DR è un documento, che specifica come e quando attuare un DR con quali misure tecniche ed organizzative. La disponibilità delle risorse ICT per attivare il DR in siti remoti ed alternativi significa aver attivato, e quindi pagare, la disponibilità di tali risorse ICT alternative a quelle del sistema informativo. Ma senza la disponibilità di tali risorse alternative, qualsiasi piano di DR è totalmente inefficace e quindi inutile. Molte aziende/enti hanno un Piano di DR, ma non hanno in parallelo già "riservato" le risorse ICT alternative, anche virtuali in cloud, necessarie per poter riattivare almeno le parti essenziali del sistema informativo su queste risorse alternative. In aggiunta, occorre provare periodicamente le procedure relative al DR con tutto il personale predefinito da coinvolgere, che OAD chiama ERT, Emergency Response Team.

Dall'indagine OAD 2025 emerge che il **70%** dei SI delle aziende/enti rispondenti ha un Piano di DR, e di questi il **46%** l'ha attuato considerando solo le parti del SI fondamentali per garantire la continuità operativa minima per le sue attività/business.
La percentuale emersa è veramente alta, considerando la composizione delle aziende/enti emerse dal sondaggio. Questo da un lato dipende che i rispondenti appartengono, come più volte sottolineato, alla fascia medio-alta in termini di livello di sicurezza digitale, dall'altro che la diffusione di attacchi digitali sempre più "cattivi" ed impattanti l'attività ed il business sta portando imprese di ogni dimensione e settore merceologico a munirsi di adeguati strumenti non solo di prevenzione e difesa, ma anche di **resilienza**.

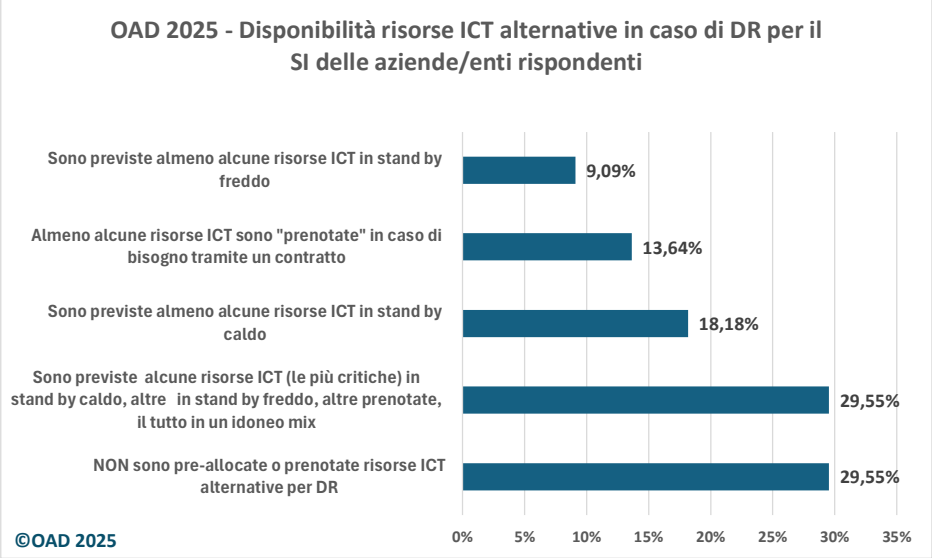


Fig. 7.2.7-8

Tale tendenza è confermata da quanto emerge dalla fig. 7.2.7-8, cui hanno risposto solo chi aveva dichiarato di avere un Piano di DR, e che mostra la disponibilità di risorse ICT "alternative" da utilizzare in caso di DR del SI. Quasi il **30%** delle aziende/enti rispondenti **non** ha previsto o allocato risorse ICT alternative, pur avendo un piano di DR; è un DR solo sulla carta, di fatto difficilmente attuabile in breve tempo nel momento di un disastro, senza poter disporre di risorse ICT alternative. Questa percentuale è abbastanza alta, ma sicuramente influenzata dalle microimprese che hanno risposto alle domande opzionali sulle misure di sicurezza. D'altro canto quasi un **70%** delle aziende/enti rispondenti hanno previsto risorse alternative in caso

di DR, e questo è una dato positivo: finalmente le organizzazioni rispondenti stanno seriamente considerando l'evenienza di un DR: prima il COVID poi le guerre in atto, con tutti gli attacchi digitali ad esse correlate, hanno sicuramente fatto comprendere anche alle piccole organizzazioni **l'importanza della resilienza**. Il **30%** circa delle organizzazioni rispondenti dichiara di aver previsto un intelligente mix di soluzioni tra risorse ICT alternative in stand by caldo, freddo e prenotate con i fornitori, tipicamente ora in ambito cloud. A scendere, il disporre di soluzioni in stand by freddo e caldo, ossia disponibilità risorse ICT in tempo reale e probabilmente in replica su risorse remote in una architettura ad alta affidabilità, e la prenotazione di risorse presso fornitori, tipicamente di cloud.

La gestione efficace di una gravissima emergenza come il recovery di un SI richiede non solo la disponibilità di risorse alternative, come sopra descritto, ma anche una struttura e procedure organizzative che possano mettere in atto il piano di DR. OAD chiama tale struttura **ERT, Emergency Response Team**, e in §7.1.2 è riportata quale sia la situazione in merito tra le aziende/enti rispondenti.
Aver definito un ERT e le relative procedure da seguire in caso di disastro non basta; occorre che le persone dell'ERT, sulla base del Piano di DR, effettuino periodicamente delle **esercitazioni** (normalmente a tavolino, chiamate **DTE, Desk Top Exercise**), ad esempio su base semestrale, o annuale, così da verificare la corretta impostazione delle procedure organizzative e la preparazione del personale da coinvolgere in un DR. In un DTE vengono simulati diversi possibili casi di disastri (considerando quanto analizzato nell'ultima analisi dei rischi ICT effettuata) e provate le procedure previste nel piano, attivando le persone e le risorse ICT da coinvolgere.
Senza periodiche sperimentazioni e senza la pre-allocazione delle risorse ICT alternative, un piano di DR ben difficilmente potrà essere attivato nei tempi necessari ed a costi ragionevoli.
La fig. 7.2.7-9 mostra che il **43,18%** delle organizzazioni rispondenti che hanno un Piano di DR non effettuano simulazioni e prove. Tutte le altre le effettuano, ma in modalità e tempi diversi, come evidenziato nella figura. Si noti che la percentuale più alta di questi, il **36,36%,** riguarda l'effettuare periodiche simulazioni solo sulle parte del SI più importanti e che supportano le attività primarie che non possono essere totalmente bloccate in caso di disastro
.

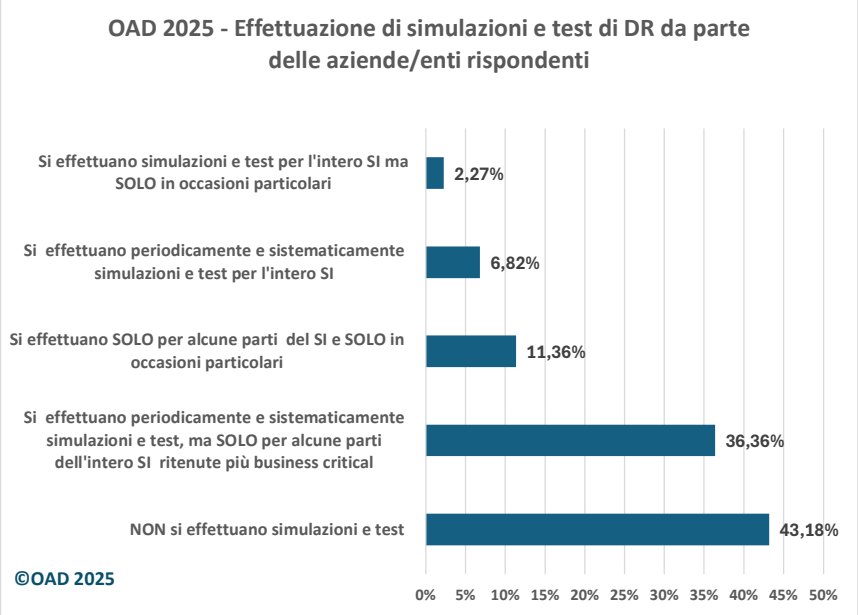


Fig. 7.2.7-9

7.3 Le misure di sicurezza per gli ambienti OT nei SI delle aziende/enti rispondenti

Si è dedicato un sottocapitolo specifico alle misure di cybersicurezza negli ambienti OT, avendo effettuato anche in questa indagine OAD 2025 un'analisi verticale sugli attacchi ai sistemi OT, presentata in §4.3.
Negli anni passati OAD aveva considerato gli attacchi a quelli che ora si chiamano sistemi OT, prevalentemente focalizzati sui sistemi di automazione e di controllo dei processi industriali, e aveva posto specifiche domande anche sulle misure di sicurezza in atto per questi sistemi. Nelle ultime edizioni di OAD queste domande erano state eliminate per semplificare e rendere più veloce la compilazione del questionario online.
Si sono di introdotte domande sulle misure di sicurezza per i sistemi OT in questa edizione 2025, ma lasciandole opzionali, e "riservate" a chi aveva dichiarato di avere e gestire sistemi OT.

Le risposte al questionario raccolte sono quindi delle aziende/enti rispondenti che hanno e gestiscono sistemi OT, che sono il **40,58%** del totale (si veda fig. 4.3-3), e tra queste di quelle che hanno deciso di rispondere alle domande sulle misure di sicurezza, il **40,8%** dei rispondenti complessivi (si veda fig. 7-1): complessivamente circa il **16,56% del totale** delle aziende/enti rispondenti.

A livello di rete, una prima misura di sicurezza per i dispositivi OT è di collegarli su reti locali a loro dedicate, e non sulle stesse reti locali dove sono connessi i PC ed altri sistemi non OT (quali server, storage, router) collegati al SI. Le risposte avute dai rispondenti evidenziano che per il **32,26%** tutti i sistemi OT operano su reti locali loro dedicate, e per il **42,94%** solo alcuni sistemi OT operano su reti locali loro dedicate.
Solo il **25,81%** dei rispondenti collega sistemi OT e altri sistemi informatici sulla stessa rete locale.
Questi dati sono molto positivi, ed indicano che quasi i ¾ delle aziende/enti rispondenti sta implementando correttamente, in termi di sicurezza di rete, i sistemi OT che utilizza.

Inizialmente i sistemi OT operavano in maniera totalmente isolata, e nell'ambito dell'industria manifatturiera (ma anche in ambito sanitario, nelle PA, Pubbliche Amministrazioni, e in quasi tutti gli altri settori merceologici) non rientravano come sistemi ICT , e quindi nell'ambito del SI, ma come sistemi di produzione: il responsabile di riferimento non era il CIO, ma il capo dello stabilimento, o della direzione medica, e così via. Con il divenire sempre più digitali dei sistemi OT (inizialmente prevalentemente analogici) e con il parallelo crescere e potenziarsi delle reti di comunicazione, con la necessità di registrare, trattare ed archiviare le informazioni digitali da essi generati, il collegamento e l'interoperabilità dei sistemi OT con il mondo IT è andato fortemente crescendo.

La fig. 7.3-1 mostra che la stragrande maggioranza dei sistemi OT delle aziende/enti rispondenti, il **83,87%** ha controlli e monitoraggi effettuabili sia in locale che da remoto, e di questi il **29%** ha il doppio controllo per tutti i sistemi OT.

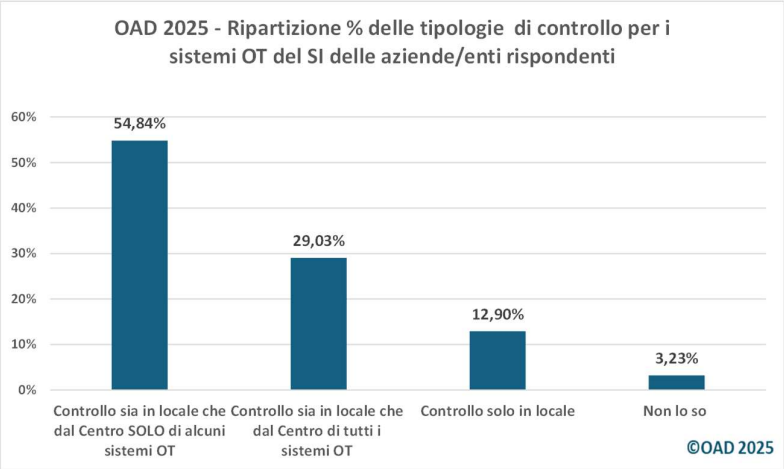


Fig. 7.3-1

Il livello di affidabilità e disponibilità di un sistema ICT, in caso di suo malfunzionamento, è dato anche dalla sua configurazione in replica in tempo "quasi" reale oppure dalla disponibilità di una sua copia "di scorta" che possa facilmente e tempestivamente sostituire il dispositivo malfunzionante. Queste logiche di repliche on line e di pezzi di scorta dipendono fortemente dal tipo di sistema OT, in termini di dimensione, costo, complessità. Si possono avere repliche on line o pezzi di scorta per sistemi relativamente piccoli, non per grandi dispositivi come quelli medici per la TAC.
La fig. 7.3-2 fornisce comunque una indicazione di massima significativa: Il **35,48%** dei sistemi OT dei rispondenti ha parti di scorta, il **32,26%** non è in replica e non ha scorte di alcun tipo. ed il **22,58**% è in replica: di questi il **19,35%** (la stragrande maggioranza) ha una replica solo per gli OT più critici, il **3,23%** ha una replica per tutti i sistemi OT.

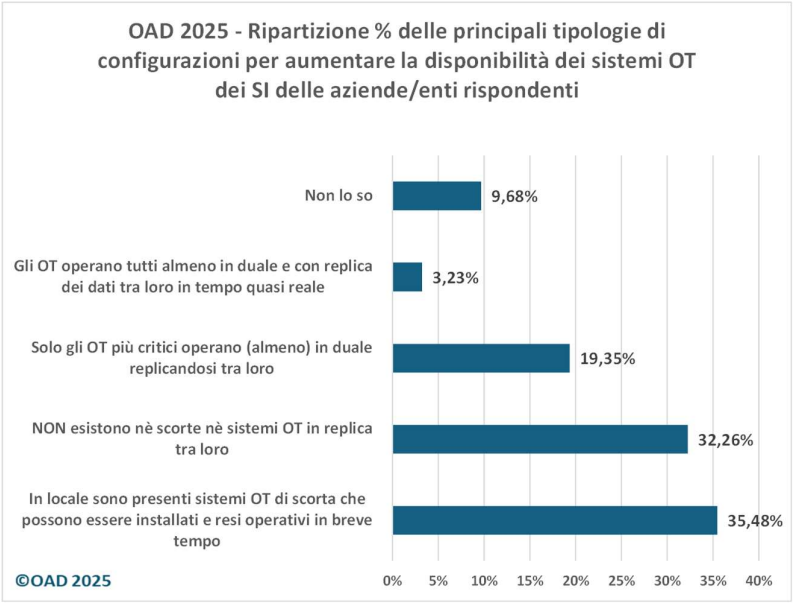


Fig. 7.3-2

Come già evidenziato nei paragrafi precedenti, **la rilevazione e la gestione degli incidenti ICT** è basilare per poter garantire un idoneo livello di sicurezza digitale. Gli incidenti digitali, nel cui ambito sono inclusi gli attacchi, occorrono ovviamente anche in ambito OT, e come già evidenziato in §4.3, possono anche coinvolgere persone, non solo sistemi ICT, con possibili seri problemi nel connubio security-safety. La gestione di ogni incidente o attacco digitale richiede soprattutto chiare ed efficaci procedure organizzative, perché sia chiaro chi deve fare che cosa e come.
Dall'indagine emerge che per il **58%** dei rispondenti nel caso di incidenti in ambito OT si usano le stesse procedure in uso per gli altri ambiti del SI. Solo per **l'6,45%** sono definite e seguite specifiche procedure, e per il **29%** delle aziende/enti rispondenti non esistono procedure cui far riferimento per gestire gli incidenti digitali sui sistemi OT.
Quest'ultima percentuale , a giudizio dell'autore, è ancora troppo alta, e costituisce un indicatore di come siano sottostimati gli aspetti organizzativi anche per la sicurezza digitale dei sistemi OT.

E' crescente nell'ambito OT il riferimento a specifiche best practice e standard internazionali, tra questi i più diffusi includono:

- la serie di standard ISA/IEC 52443
- NIST IR 8200 per IOT
- NIST SP 800-82r3 - Guide to Operational Technology (OT) Security
- le linee guida per la sicurezza IoT della IoT Security Foundation
- OPC UA, Open Platform Communication Unified Architecture della OPC Foundation

L'indagine evidenzia che il **48,29%** delle aziende/enti rispondenti li segue in riferimento soprattutto ai dispositivi OT più recenti e moderni, mentre un ben più esiguo **3,7%** ne fa riferimento per tutti i sistemi OT che deve acquisire e gestire.

7.4 La valutazione del livello di sicurezza dei SI delle aziende/enti rispondenti

Il questionario OAD 2025 conteneva due sezioni con domande e risposte preimpostate sulle **misure di sicurezza digitale** in essere nel SI oggetto delle risposte sugli attacchi. La compilazione di queste due sezioni era opzionale: il **40%** dei rispondenti ha compilato queste due sezioni, ed ha così potuto ottenere, alla fine della compilazione dell'intero questionario, una macro valutazione, contestualizzata alle macro necessità di sicurezza dell'azienda/ente, del livello di sicurezza digitale del SI oggetto della compilazione.

La fig. 7.4-1 mostra i risultati della valutazione ottenuta.

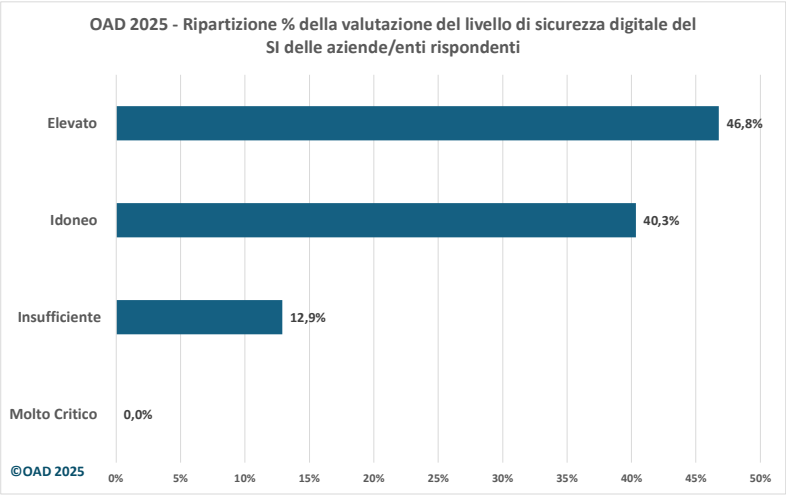


Fig. 7.4-1

Questo 40% di rispondenti è di vari settori merceologici, siveda fig. 7-1, ed è di varie dimensioni, si veda fig. 7-2, mala stragrande maggioranza, il **87,1%**, ha avuto un risultato positivo o molto positivo. Solo il **12,9%** è risultato insufficiente, e **nessuno** è risultato "molto critico".

8. Contributo della Polizia Postale e per la Sicurezza Cibernetica

OAD riporta in questo capitolo l'intero contributo del "Servizio Polizia Postale e per la Sicurezza Cibernetica[68]", 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 ed AIPSI **ringraziano vivamente** insieme al **Direttore** del Servizio Polizia Postale Polizia Postale e delle Telecomunicazioni **Ivano Gabrielli**.

La Polizia Postale da anni collabora con AIPSI per 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 nell'obiettivo degli attacchi digitali in ambito business di 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[69], 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 nazionale.

Nella fig. 8-1 sono messe a confronto le informazioni ricevute da OAD negli anni dalla Polizia Postale **sugli attacchi alle infrastrutture critiche e ai servizi essenziali**. La tabella evidenzia che il **numero di attacchi rilevati** è molto simile nel 2023 e nel 2024, ed entrambi sono inferiori rispetto al 2022, che costituisce il picco degli attacchi nell'arco temporale considerato, dal 2016 al 1° semestre 2025. Il numero di attacchi nell'anno 2021 e in quelli precedenti sono di un ordine di grandezza inferiori. I dati emersi per il 1° semestre 2025 confermano sostanzialmente la tendenza per l'intero 2025 sul medesimo ordine di grandezza del 2024. Per gli "alert diramati" il 2022 è l'anno del picco, e coincide con il picco di attacchi rilevati nelle indagini OAD, come mostrato nella fig. 4-2.

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 Infoinvestigative". Emerge chiaramente come:

- siano **fortemente aumentati i siti web esaminati** dalla Polizia Postale, indicatore della sempre più ampia informazione e mal/disinformazione inerente anche i temi caldi geopolitici, trattatati in §3;
- gli **spazi virtuali oscurati**, che includono anche i siti web, sono una piccola percentuale, tra l'1 e il 2%, di quelli esaminati, con un picco nel 2023.

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.

[68] Per un inquadramento delle attività si veda: https://www.interno.gov.it/sites/default/files/2025-01/2024-report-def.-sppsc.pdf.
NB: nel testo il "Servizio Polizia Postale e per la Sicurezza Cibernetica" per brevità viene indicato come "Polizia Postale"
[69] https://www.commissariatodips.it/profilo/cnaipic/index.html

E' 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 crescente aumento delle somme sottratte

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

Comparando le due figure, emerge chiaramente che le frodi informatiche sono più complesse e difficili da realizzare, richiedendo elevate competenze tecniche; pertanto per esse i casi trattati e le persone indagate sono inferiori, e in certi anni di molto, rispetto alle truffe online. Ma sono soprattutto le somme sottratte assai inferiori: in tutti gli anni considerate, quelle delle truffe hanno un fattore moltiplicativo di più di 3.

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" è purtroppo molto vera e ancor più preoccupante, ed è un fronte sul quale le democrazie liberali, e in primis l'Italia, devono combattere contrastando sistematicamente e continuamente tale disinformazione, come già considerato nel §3.

Tutti i dati forniti dalla Polizia Postale, con le considerazioni iniziali del suo contributo riportato nel seguito e che l'autore condivide pienamente, ***evidenziano la criticità in Italia della criminalità cyber e degli attacchi****, considerando che questi ultimi sono stati rivolti a SI con elevate misure di sicurezza digitale (tipiche per infrastrutture critiche e servizi essenziali, o almeno così dovrebbe essere). Questi dati confermano ulteriormente che l'Italia si trova, da anni, in una situazione di* ***insicurezza digitale sistemica*** *anche per i SI critici e/o che forniscono servizi essenziali per il funzionamento del Paese.*

Protezione strutture critiche/essenziali	1 gen - 30 giugno 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 (*)	4.911 **	12.058 **	12.101 **	13.099	282	509	1181	459	1.032	844
Alert diramati	22.990	59.875	77.012	113.420	24.824	83.416	82.484	80.777	31.524	6.721
Indagini avviate	n.d.	n.d.	96	110	34	103	155	74	72	70
Persone denunciate/indagate (*)	49 **	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)	21	63	79	77	17	69	79	108	83	85

* 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.).

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

Cyber Terrorismo	1 gen -30 giugno 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	101.683	295.493	182.209	175.572	11.962	37.081	36.377	36.000
Spazi Virtuali con contenuti illeciti rilevati	983	4.642	2.037	1.598				
Spazi oscurati per attiv. infoinvestigative	275	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 gen -30 giugno 2025	1 gen - 31 dic 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022
Casi trattati	4.116	8.602	10.755	5.908
Persone indagate	379	923	927	725
Somme sottratte (€)	28.466.633	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 gen -30 giugno 2025	1 gen - 31 dic 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022
Casi trattati	9.261	18.967	16.637	15.699
Persone indagate	1.950	3.627	3.610	3.570
Somme sottratte (€)	109.235.401	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)

OAD
Osservatorio
Attacchi Digitali
in Italia

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 (indagine AIPSI)

ANNO 2024

e

Primo Semestre 2025

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

Dati aggiornati al 30 giugno 2025

Roma, 24 luglio 2025

Isp. della Polizia di Stato
Gaetano Martucci

Ass. C. della Polizia di Stato
Luigi Ummaro

Agt. della Polizia di Stato
Valeria Pettirossi

Sommario

PREMESSA

La rivoluzione digitale ha inciso nel profondo il tessuto socioeconomico, trasformando radicalmente il modo in cui cittadini, imprese e pubbliche amministrazioni interagiscono e creano valore. L'automazione dei processi, l'accesso istantaneo ai dati e la pervasività delle piattaforme *online* hanno aperto spazi di innovazione straordinari, ma hanno anche esteso oltre ogni previsione il perimetro vulnerabile dell'intera collettività. Oggi l'"officina" della nostra quotidianità si regge su infrastrutture digitali fragili, ogni nodo connesso rappresenta un possibile punto di ingresso per attacchi sempre più sofisticati e mirati. È in questo contesto che le sfide legate alla sicurezza cibernetica assumono un rilievo centrale, rendendo necessario, per istituzioni e aziende, un continuo adattamento dei processi, delle competenze e delle strutture operative.

Negli ultimi anni abbiamo assistito a un'escalation di minacce inedite per tecniche e portata. Le attività criminali basate su *ransomware* hanno continuato a manifestare una forte capacità di penetrazione e di impatto, con gravi conseguenze per realtà strategiche e operative. Tali attacchi hanno spesso comportato significativi rallentamenti dei sistemi informatici coinvolti e avanzate richieste estorsive da parte dei gruppi autori, generando situazioni critiche sotto il profilo operativo, economico e reputazionale. Al contempo, le frodi finanziarie si sono evolute in schemi sempre più ingegnosi, capaci di aggirare controlli *legacy* grazie a tecniche di ingegneria sociale sempre più evolute. Parallelamente, 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.

Nell'ambito di un ampio progetto volto all'innovazione tecnologica e al rafforzamento delle competenze specialistiche, la Polizia di Stato ha introdotto la figura dell'Ispettore Cibernetico, una professionalità che unisce competenze giuridiche, *mastery* tecnologica e abilità investigative. Selezionati con criteri stringenti, i candidati affrontano un percorso residenziale di nove mesi nel quale studio teorico e pratica operativa si fondono: dal diritto processuale alle tecniche forensi, dalla simulazione di *incident response* alla gestione diretta dei rapporti con l'Autorità Giudiziaria. Questo

approccio ha abbattuto la tradizionale dicotomia tra "tecnico" e "investigatore", creando specialisti in grado di custodire la catena probatoria senza interruzioni e di accelerare i tempi di indagine. Quando, a settembre 2026, i primi 210 ispettori saranno pienamente operativi, l'Italia disporrà di un modello che sarà un unicum a livello internazionale.

Lo stato di salute del Paese, fotografato dai dati della Polizia Postale nel 2024, mostra numeri eloquenti: 12.058 attacchi informatici rilevati, di cui 1.568 diretti contro infrastrutture critiche; quasi 19.000 truffe online con perdite per 183 milioni di euro; frodi informatiche che hanno generato danni per oltre 48,6 milioni di euro e la costanza con cui vengono perpetrati i reati digitali contro la persona, con un'incidenza particolarmente elevata tra gli adolescenti, rappresenta un fenomeno di estrema gravità che richiede interventi rapidi ed efficaci per tutelare le vittime.

Sul fronte della lotta al terrorismo, il monitoraggio ha intercettato 4.642 spazi virtuali illeciti, con 2.369 oscuramenti a supporto delle attività investigative.

Questi numeri non sono semplici statistiche: raccontano di cittadini esposti, strutture messe a rischio e di un impegno incessante per tutelare la sicurezza nazionale in un contesto di conflitto asimmetrico con attori statali e non.

La portata transnazionale delle minacce impone un livello di cooperazione giuridica e operativa senza precedenti. Strumenti come *l'European Investigation Order* e i *Joint Investigation Team* di Europol hanno consentito interventi coordinati in moltissimi casi. Particolarmente significative le indagini denominate "*Taken Down*" e "*NoName*", condotte con il coordinamento di Eurojust ed Europol: la prima ha rappresentato l'operazione più estesa mai realizzata contro la pirateria audiovisiva in ambito italiano e internazionale; la seconda ha riguardato un gruppo di hacker responsabile di migliaia di attacchi informatici a infrastrutture critiche di diversi Paesi europei. Permangono tuttavia ostacoli rilevanti derivanti da divergenze normative, soprattutto nei Paesi caratterizzati da quadri giuridici non allineati, dove il tracciamento delle criptovalute e la validazione delle evidenze digitali continuano a rappresentare ambiti di forte criticità. Allo stesso tempo, l'intelligenza artificiale sta ridefinendo i confini del conflitto cibernetico: se da un lato, ad esempio, gli algoritmi potenziano l'efficacia di attacchi *ransomware* e la capacità di generare *deepfake* su scala industriale, dall'altro offrono alle forze di polizia strumenti per assolvere in modo ancora più efficace la loro missione.

In Italia la *Cyber Threat Intelligence* si è fatta cuore operativo della prevenzione, grazie ad accordi con gestori di reti critiche e *partnership* con il mondo accademico per l'elaborazione di modelli di analisi avanzata. Allo stesso tempo, campagne di sensibilizzazione come "Una Vita da Social" e "Cuori Connessi" hanno coinvolto nel 2024 oltre quattrocentomila studenti, promuovendo consapevolezza sui rischi digitali e comportamenti più sicuri.

Con quasi tre milioni di visite al portale www.commissariatodips.it nel 2024, il Commissariato di P.S. Online si è fatto promotore di una sicurezza partecipata, coinvolgendo i cittadini non solo come fruitori ma come veri e propri alleati nell'*intelligence* civica, segnalando tempestivamente anomalie e potenziali minacce a difesa del bene comune.

Un ulteriore aspetto riguarda le vulnerabilità di genere: nella diffusione di immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate *(revenge porn)*, le donne rappresentano il 73% delle vittime, un dato che mette in luce come la dimensione emotiva e psicologica si intrecci strettamente con quella tecnologica. Affrontare queste dinamiche richiede non solo strumenti investigativi e misure di tutela legale, ma anche reti di supporto psicologico e iniziative di sensibilizzazione mirate a trasmettere soprattutto ai più giovani il valore dell'empatia digitale.

La "mappa" dei 55.278 fascicoli aperti nel 2024 dalla Polizia Postale e i *trend* rilevati nel primo semestre del 2025 tracciano la rotta per il prossimo futuro: è indispensabile potenziare la formazione tecnica, aggiornare i *framework* normativi in chiave cyber-resiliente e rafforzare le alleanze internazionali. Solo così il progresso digitale potrà rimanere sinonimo di libertà e innovazione, anziché trasformarsi in un terreno di scontro e vulnerabilità.

Nel cuore operativo della Polizia di Stato, la Polizia Postale e per la sicurezza cibernetica è costantemente impegnata a evolvere i suoi modelli, convinta che la sicurezza cibernetica sia una sfida culturale, prima ancora che tecnologica, dove ogni cittadino è chiamato a concorrere presidiando il proprio spazio digitale.

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 2024
Attacchi rilevati totali (*)	12.058 **
Alert diramati	59.875
Persone indagate (*)	178 **
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	63
Attacchi solo I.C. – OSE – PAL	***1.568***
Persone indagate solo I.C. – OSE – PAL	***60***

* 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.).

	Primo Semestre 2025
Attacchi rilevati totali (*)	4.911 **
Alert diramati	22.990
Persone indagate (*)	49 **
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	21
Attacchi solo I.C. – OSE – PAL	***526***
Persone indagate solo I.C. – OSE – PAL	***12***

* 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 2024
Casi trattati pedopornografia e adescamento online	2.828
Persone indagate	1.184
Perquisizioni	986
Monitoraggi rete	42.231
Siti presenti in black list al 31/12/2023	2.775

	Primo Semestre 2025
Casi trattati pedopornografia e adescamento online	1.383
Persone indagate	796
Perquisizioni	604
Monitoraggi rete	7.826
Siti presenti in black list al 30/06/2024	2.821

-=oOOo=-

IL COMMISSARIATO DI P.S. ONLINE

	1 gen – 31 dic 2024
Segnalazioni	84.286
Informazioni	23.490
Visite	2.925.314
Accessi	53.816.209
Alert Diramati	31
Interventi finalizzati alla prevenzione di intenti suicidari	253

	Primo Semestre 2025
Segnalazioni	45.762
Informazioni	12.954
Visite	1.992.028
Accessi	32.882.132
Alert Diramati	15
Interventi finalizzati alla prevenzione di intenti suicidari	196

-=oOOo=-

PREVENZIONE CYBERTERRORISMO

• *Eversione Internazionale Estremismo religioso e politico* • *Eversione nazionale estrema destra, area antagonista, attività in circostanze di emergenza*	1 gen – 31 dic 2024
Spazi web monitorati	295.493
Spazi Virtuali con contenuti illeciti rilevati	4.642
Spazi oscurati per attiv. infoinvestigative	2.369

• *Eversione Internazionale Estremismo religioso e politico* • *Eversione nazionale estrema destra, area antagonista, attività in circostanze di emergenza*	Primo Semestre 2025
Spazi web monitorati	101.683
Spazi Virtuali con contenuti illeciti rilevati	983
Spazi oscurati per attiv. infoinvestigative	275

-=oOOo=-

LE FRODI INFORMATICHE

	1 gen – 31 dic 2024
Casi trattati	8.602
Persone indagate	923
Somme sottratte	48.674.917 €

	Primo Semestre 2025
Casi trattati	4.116
Persone indagate	379
Somme sottratte	28.466.633 €

-=oOOo=-

LE TRUFFE ONLINE

	1 gen – 31 dic 2024
Casi trattati	18.967
Persone indagate	3.627
Somme sottratte	183.377.101 €

	Primo Semestre 2025
Casi trattati	9.261
Persone indagate	1.950
Somme sottratte	109.235.401 €

=oOOo=-

REATI CONTRO LA PERSONA

	1 gen – 31 dic 2024
Casi trattati	9.300
Persone indagate	1.393

	Primo Semestre 2025
Casi trattati	4.590
Persone indagate	619

ALLEGATI

Allegato A Aspetti metodologici dell'indagine OAD 2025

L'indagine OAD 2025, 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 l'unica 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.
Grazie al numero di risposte raccolte e alla loro distribuzione tra aziende ed enti pubblici di varie dimensioni e appartenenti a diversi settori merceologici, l'indagine OAD cerca e puntualmente riesce a fotografare il fenomeno degli attacchi digitali intenzionali in Italia, riuscendo a coinvolgere nell'indagine anche le piccole e piccolissime realtà, che costituiscono in Italia la stragrande maggioranza e che altre indagini nazionali ed internazionali ben difficilmente considerano.

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.
Per garantire un ulteriore livello di protezione ed evitare l'inoltro di più questionari compilati dalla stessa persona, il questionario, una volta completato e salvato, non può più essere modificato, e dallo stesso posto di lavoro non è più possibile compilare una seconda volta il questionario.
L'autore, AIPSI e Malabo garantiscono comunque la totale riservatezza sulle risposte raccolte.

Per acquisire il maggior numero possibile di rispondenti, AIPSI, Malabo 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 da AIPSI.

Quando termina il periodo previsto per la compilazione del questionario, Malabo 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 e su quello AIPSI per poter essere scaricato gratuitamente da tutti gli interessati.
Come già indicato, il bacino dei rispondenti all'indagine non è predefinito e bilanciato statisticamente. L'indagine OAD non ha pertanto valore strettamente statistico, ma dato il numero e l'eterogeneità delle aziende/enti dei rispondenti, sia per settore merceologico sia per dimensione, è comunque significativa e sufficiente per fornire attendibili indicazioni sul fenomeno degli attacchi digitali in Italia e sulle loro tendenze.

L'elaborazione dai 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 molti casi delle 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 dal 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.

L'indagine OAD è stata scelta tra i progetti di Repubblica Digitale, si veda https://repubblicadigitale.gov.it/servizi/coalizione/iniziative/oad-extended, per la sua importanza in termini di comunicazione, sensibilizzazione e formazione sulla cybersecurity.

A.1 L'indagine OAD 2025

L'indagine effettuata tramite un questionario on line via web ha posto due sole domande sugli attacchi digitali **subiti nel 2024** 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, ed ha approfondito gli attacchi digitali rilevati nel 2023 **alle applicazioni ed agli ambienti web** ed ai **sistemi OT, Operation Technology**.

Il **questionario on line OAD 2024** è stato operativo sulla piattaforma LimeSurvey installata sul sito web www.oadweb.it da febbraio 2025 a fine agosto 2025.

Il **questionario online OAD 2025**, con risposte predefinite da selezionare, è strutturato con **110 domande raccolte in 10 sezioni**, molte delle quali opzionali e "saltabili" nel corso della compilazione. In alcune sezioni sono presenti delle sottosezioni per meglio articolare e contestualizzare le varie domande. Inoltre in alcune sezioni ci sono delle "domande" non visibili che effettuano calcoli sulle risposte selezionate per la valutazione del livello di sicurezza del SI oggetto delle risposte.
Le sezioni considerate nel questionario 2025:

- S1 - Brevi informazioni sulla Azienda/Ente della/del rispondente (10 domande)
- S2 - Attacchi digitali di ogni tipo al Sistema Informativo rilevati nell'intero 2024 (2 domande)
- S3 - Approfondimento attacchi ai siti e alle applicazioni web del Sistema Informativo (11 domande)
- S3B - Approfondimento sugli attacchi a servizi ed applicazioni informatiche basate su Intelligenza Artificiale (1 domanda)
- S3C - Approfondimento sugli attacchi a sistemi ed apparati OT del Sistema Informativo (8 domande)
- S4 - Attacchi più temuti nel prossimo futuro (3 domande)
- S5 - Macro caratteristiche del Sistema Informativo cui la/il rispondente fa riferimento, sia per aziende Provider hosting/cloud che per le altre aziende/enti (8 domande + 1 se continuare con le domande sulle misure di sicurezza adottate)

- S6 - Misure tecniche in atto per la sicurezza digitale dell'intero Sistema Informativo (6 domande)
  - S6.1 - Misure fisiche di sicurezza digitale (5 domande)
  - S6.2 - Misure di Identificazione, Autenticazione e Autorizzazione (4 domande)
  - S6.3 - Misure per la sicurezza delle reti, locali e geografiche, incluse le connessioni ad Internet (4 domande)
  - S6.4 - Misure di sicurezza delle applicazioni del Sistema Informativo (4 domande)
  - S6.5 - Misure tecniche di sicurezza digitale per la protezione dei dati (6 domande)
  - S6.6 - Strumenti tecnici per il controllo e la gestione della sicurezza digitale del SI (10 domande)
  - S6.7 - La sicurezza nei sistemi OT in uso (5 domande)
- S7 - Misure organizzative di sicurezza digitale nell'Azienda/Ente della/del rispondente (17 domande)
- S8 - Ruolo della/del rispondente (1 domanda)
- S10 – Calcoli (non visibili) e presentazione finale in tempo reale della macro valutazione del livello di sicurezza del SI a chi completa le risposte incluse quelle delle Sezioni 6 e 7.

Gruppi di domande relative ad un argomento vengono automaticamente saltate se quel tipo di argomento non è stato selezionato. Questa logica implementativa del questionario online riduce significativamente i tempi per completarlo.

Gli approfondimenti sugli attacchi erano richiesti per **3 indagini verticali**: ambienti **web**, **OT**, **basati su IA.**
Per l'indagine verticale sul web, si è fatto anche riferimento alle 10 top vulnerabilità in ambito web individuate da OWASP. Anche per gli attacchi agli ambienti applicativi basati su tecniche di IA si è fatto riferimento alle recenti 10 top vulnerabilità individuate da OWASP per l'IA.
Per le indagini verticali sugli attacchi digitali agli ambienti web e a quelli OT sono state poste le seguenti domande di approfondimento:

- il principale impatto tecnico subito a seguito dall'attacco più grave, con risposte multiple, in termini di non disponibilità dei servizi ICT erogati dal sistema informativo;
- il principale impatto subito in termini di costi sia per budget del sistema informativo sia per il bilancio dell'intera azienda/ente a seguito dall'attacco più grave, con risposte multiple;
- le possibili motivazioni dell'attacco più grave, nel periodo considerato, secondo la stima del compilatore, con risposte multiple;
- il tempo massimo richiesto per il ripristino ex ante dei sistemi ICT, nel caso del più grave attacco subito nel periodo considerato.

Queste domande non sono state poste per gli attacchi agli ambienti basati su IA.

Le domande sulle **misure di sicurezza digitale in essere** sui SI oggetto delle risposte delle organizzazioni rispondenti **non erano obbligatorie,** ma compilandole, alla fine si poteva avere una macro valutazione del livello di sicurezza del sistema informativo oggetto delle risposte fornite, come descritto in A.3.

A.2 La tassonomia degli attacchi digitali per OAD 2025

L'edizione 2025 ha aggiunto alle 14 tipologie di attacco della precedente edizione una nuova tipologia che fa riferimento agli attacchi alle applicazioni ed ai sevizi informatici basati su tecniche di IA, Intelligenza Artificiale.
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 nel corso del 2022
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, ..) 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 2024 **non è stato rilevato alcun attacco digitale** intenzionale al Sistema Informativo
- Nel corso dell'intero 2024 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 infatti, 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 7 voci, descritte nel prossimo paragrafo §A.2.1.

A.2.1 Le classi di tecniche di attacco considerate (come si attacca)

Facendo riferimento principalmente alle tassonomie sviluppate da CERT[70] e da Sandia[71], si sono categorizzate le tecniche di attacco sotto riportate per poter descrivere e richiedere nel questionario OAD 2025 quali sono (o quali si pensa possano essere state) le tecniche usate dall'attaccante per

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

portare l'attacco rilevato.
E' 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, inclusi gli APT, Advanced Persistent Threat.

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

A.2.1.1 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.2.1.2 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.2.1.3 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** includono XSS[72], attacchi drive by[73], script "fileless"[74]
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 troian horse, ransonware, 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.2.1.4 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.2.1.5 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

[72] 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.
[73] Sfruttano vulnerabilità del browser per scaricare ed eseguire codice maligno non appena l'utente visita un sito web infetto.
[74] Eseguono codice dannoso direttamente nella memoria RAM senza scriverlo su disco, rendendo più difficile il rilevamento da parte degli antivirus tradizionali.

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 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.2.1.6 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.2.1.7 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.2.1.8 Utilizzo di due o più tecniche di attacco (es. APT)

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

A3 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 2024, 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)**.

Una di queste valutazioni appare 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.

ALLEGATO B Glossario

2C	Command & Control, indica un sistema centralizzato per coordinare e gestire bootnet e sferrare attacchi soprattutto di tipo DoS/DDoS.
Account	Insieme di informazioni di identificazione ed autenticazione di un utente di un sistema informativo. Tipicamente è costituito da un identificativo d'utente e da una password, ma può estendersi a certificati digitali, riconoscimenti biometrici e richiedere l'uso di token quali smart card, chiavette USB, ecc.
Accountability	significa responsabilizzazione di un ruolo, che è tenuto a dimostrare che le azioni ed attività svolte sono coerenti con quanto richiesto/stabilito dal suo ruolo.
ACL	Access Control List: elenco di regole per il controllo degli accessi a risorse ICT.
ACN	Agenzia Cibernetica Nazionale.
Active Directory	Sistema di directory della Microsoft, integrato nei sistemi operativi Windows dal 2000 in avanti. Utilizza SSO, LDAP, Kerberos, DNS, DHCP, etc.
Active X Control	File che contengono controlli e funzioni in Active X che “estendono” (eXtension) ed espletano specifiche funzionalità; facilitano lo sviluppo di software di un modulo software dell’ambiente Windows in maniera distribuita su Internet.
Address spoofing	Generazione di traffico (pacchetti IP) contenenti l’indicazione di un falso mittente (indirizzo sorgente IP).
Adware	Codice maligno 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.
AET	Advanced Elusion Techniques: tecniche avanzate di elusione degli strumenti di sicurezza in uso.
AI	Artificial Intelligence, che individua l’ampio campo delle tecniche e delle teorie di intelligenza artificiale.
AIPSI	Associazione Italiana Professionisti Sicurezza Informatica.
AISE	Agenzia Informazioni e Sicurezza Esterna.
AISI	Agenzia Informazioni e Sicurezza Interna.
Alert	Viene spesso usato il termine inglese di “allarme” per indicare segnalazione di eventi e problemi inerenti la sicurezza informatica; la segnalazione può essere generata sia da dispositivi di monitoraggio e controllo sia dalle persone addette.
API	Application Programming Interface
App	Neologismo ed abbreviazione di "application" (applicazione) per indicare, anche in italiano, le applicazioni operanti localmente sui sistemi mobili, tipicamente su smartphone.
ASAT	Arma anti satellite
ATECO	ATtività ECOnomiche: classificazione delle attività economiche.
ATP	Advanced Persistent Threat: attacco persistente e sofisticato, basato su diverse tecniche operanti contemporaneamente e capaci di scoprire e sfruttare diverse vulnerabilità. Usato da organizzazioni con grandi capacità e risorse.
Attacco mirato	O specifico, indicato sovente con il termine inglese targeted attack: attacco portato ad uno specifico sistema obiettivo, o a un gruppo similare di obiettivi, con tecniche sofisticate e specifiche per il sistema target. Viene incluso sovente tra gli ATP.
Attacco massivo	Attacco rivolto ad una grande massa di obiettivi simili, anche dell’ordine di milioni: può essere semplice e non sofisticato, ma nella massa qualche attacco va quasi sempre a buon fine. Tipici esempi i phishing ed i ransomware.
Audit	Per la sicurezza digitale, il risultato di un auditing.
Auditing	Per la sicurezza digitale, il processo documentato di revisione (ossia verifica, controllo e valutazione) della efficacia delle misure in essere e della loro gestione, oltre che della

	conformità di tali misure alle leggi vigenti e alle normative, anche interne, che devono essere seguite.
Backdoor	Interfaccia e/o meccanismo nascosto che permette di accedere ad un programma superando le normali procedure e barriere d'accesso.
BAS	Building Automation Systems: sistemi di controllo, gestione e automazione di dispositivi hardware e software all'interno di un edificio. In Italia si usa più sovente il termine di "domotica".
BIA	Business Impact Analysis.
Blade server	"Lama", ossia scheda omnicomprensiva di elaborazione di un sistema ad alta affidabilità costituito da più lame interconnesse ed interoperanti.
Blended Threats	Attacco portato con l'uso contemporaneo di più strumenti, tipo virus, worm e trojan horse.
Bluetooth	Protocollo, standard de facto, di collegamento senza fili a brevi distanze. Opera in radio frequenza in campi attorno ai 2,45 GHz.
Bots	Programmi, chiamati anche Drones o Zombies, usati originariamente per automatizzare talune funzioni nei programmi ICR, ma che ora sono usati per attacchi distribuiti.
Botnet	Insieme di computer in rete, chiamati "zombi", che a loro insaputa hanno agenti (programmi) malevoli dai quali partono attacchi distribuiti, tipicamente DDOS.
Buffer overflow	Consiste nel sovra-scrivere in un buffer o in uno stack del programma dati o istruzioni con i quali il programma stesso può comportarsi in maniera diversa dal previsto, fornire dati errati, bloccare il sistema operativo, ecc.
BYOD	Bring Your Own Device: policy aziendale che consente l'utilizzo di dispositivi mobili di proprietà dell'utente anche nell'ambito dei sistemi dell'azienda/ente. Il fenomeno è chiamato anche "consumerizzazione".
CAaaS	Cyber Attack as a Service.
CAPTCHA	Completely Automated PublicTuring test to tell Computers and Humans Apart: l'acronimo indica una famiglia di test costituita da una o più domande e risposte per assicurarsi che l'utente sia un essere umano e non un programma software.
CASB	Cloud Access Security Brokers.
C&C	Command&Control: Sistema centrale di commando e controllo di una botnet.
CED	Centro Elaborazione Dati: centro di calcolo ove risiedono tutti i sistemi centralizzati di elaborazione, archiviazione e trasmissione dei dati.
CER	Direttiva EU per la resilienza delle infrastrutture critiche.
CERT	Computer Emergency Response Team.
Chatbot	Programma software realizzato per interagire con gli umani via voce e/o scambi di testi. Hanno numerose applicazioni, tipicamente l'assistente virtuale digitale, ma possono essere programmati per agire in maniera malevola e costituire un componente di un attacco digitale.
Cybersquatting	Acquisto e/o registrazione di un nome di dominio web identico o simile a un dominio esistente, con l'intento illegale e truffaldino di trarre profitto illegalmente da un marchio, da un nome di azienda o da un nome di persona famosa cui il dominio fa di fatto riferimento.
Churn rate	Tasso di abbandono a favore della concorrenza, tipicamente dopo un attacco.
CIO	Chief Information Officer: il responsabile dell'intero sistema informatico.
CIS CISA	Center for Internet Security: definisce e fornisce linee guide, checklist (CIS Controls e benchmark) e una architettura di sicurezza digitale, la CIS SecureSuite Cybersecurity and Infrastructure Security Agency negli US
CISA	Certified Information Systems Auditor di ISACA.

CISO	Chief Information Security Officer: il responsabile della sicurezza digitale dell'intero sistema informativo.
CISR	Comitato interministeriale per la sicurezza della Repubblica
CISSP	Certified Information Systems Security Professional.
Cyber warfare	Guerra cibernetica, chiamata anche guerra informatica, guerra elettronica, guerra digitale
Cluster	Insieme di computer e/o di schede (es lame di un sistema blade) cooperanti per aumentare l'affidabilità complessiva del sistema; il termine è anche usato per identificare un insieme contiguo di settori in un disco rigido.
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, all'interno della Polizia Postale e delle Telecomunicazioni.
COBIT	Control Objectives for Information and related Technology: consolidata best practice per il governo (governance) di un SI ed il suo audit.
Consumerizzazione	Si veda BYOD.
Container	Istanza di un ambito virtualizzato di applicazioni, che isola le risorse hardware e software in uso da ognuna di esse, pur sempre all'interno di un solo e unico sistema operativo.
COPASIR	Comitato parlamentare per la sicurezza della Repubblica: è l'organo di controllo parlamentare sulle agenzie italiane di intelligence.
COR	Comando Operazioni in Rete (Ministero Difesa).
CPS	Cyber-Physical System (in ambiti OT).
CRAMM	CCTA Risk Analysis and Management Method
Cryptojacking	Utilizzo di capacità elaborativa di un inconsapevole sistema ICT target da parte di un cybercriminale per creare criptovaluta.
Crowdturfing	Combinazione di "crowdsourcing" e "astroturfing", indica un attacco basato su recensioni scorrette e false per danneggiare la reputazione di un prodotto o di una azienda/ente.
CRRT	Cyber Rapid Response Teams: a livello UE -ENISA
CSaaS	Cyber Security as a Service
CSIRT	Computer Security Incident Response Team: fa parte di ACN
CSO	Chief Security Officer; responsabile della sicurezza dell'intera azienda/ente, prevalentemente per la sicurezza fisica di edifici e del personale. In alcune organizzazioni il CISO riporta a questa figura.
CSSLP	Certified Secure Software Lifecycle Professional.
CTO	Chief Technology Officer: è il direttore tecnico di più alto livello, tipicamente per aziende che producono prodotti e servizi ICT. In talune organizzazioni il CIO riporta a questa figura.
CTTA	Central Computer and Telecommunications Agency del Governo UK, ora chiamato Cabinet Office.
CVCN	Centro di Valutazione e Certificazione Nazionale: fa parte di ACN
CVE	Common Vulnerabilities and Exposures: l'acronimo indica sia il programma di identificazione e classificazione delle vulnerabilità tecniche di ogni sistema e servizio ICT, sia l'elenco di record delle vulnerabilità identificate.
CVSS	Common Vulnerability Scoring System: metrica internazionale di valutazione della gravità di una vulnerabilità di un sistema ICT.
DAC	Discretionary Access Control.
Darknet	Rete virtuale privata nella quale gli utenti si connettono solamente con persone di cui si fidano.
Dark web	Siti web che si raggiungono via Internet ma attraverso specifici software, configurazioni e accessi autorizzativi, e non sono indicizzati, e quindi ritrovabili, dai motori di ricerca. Molti

	dark web contengono informazioni criminali, dalla pedopornografia a strumenti informatici di attacco e da account e identità digitali rubate che sono poste in vendita.
Data Breach	Letteralmente "violazione dei dati", spesso è usato come sinonimo di furto di dati. Tecnicamente è usato per indicare l'accesso a banche dati o a file system contenenti identità digitali ed informazioni personali.
Data Center	Centro Dati: si veda CED.
DB	Data Base: banca dati.
DBMS	Data Base Management System.
DCS	Distributed Control System (ambiti OT).
Deadlock	Condizione in cui due o più processi non sono più in grado di proseguire perché ciascuno aspetta il risultato di una operazione che dovrebbe essere eseguita dall'altro.
Deamon:	Software di base operante in back-ground in un ambiente multi-tasking.
Defacement o Defacing	In inglese significa deturpare, e nel gergo della sicurezza digitale indica un attacco ad un sito web per modificarlo o distruggerlo; spesso con tale attacco viene modificata solo la home-page a scopo dimostrativo.
DES	Data Encryption Standard
DoS/ DDoS	Denial of Service e Distributed Denial of Service: attacco per saturare sistemi e servizi ed impedire la loro disponibilità.
Dialer	Programma software che connette il sistema ad Internet, ad una rete o ad un computer remoto tramite linea telefonica (PSTN o ISDN); può essere utilizzato per attacchi e frodi.
DKIM	Domain Keys Identified Mail: in ambito DMARC, chiavi di crittografia asimmetrica per l'autenticazione di ogni messaggio di posta elettronica. Il messaggio viene firmato dal server e il destinatario controlla i messaggi con la chiave pubblica DKIM, che viene fornita nel DNS del dominio.
DMARC	Domain-based Message Authentication, Reporting, and Conformance: sistema standard di autenticazione dei messaggi di posta elettronica, che aiuta gli amministratori della posta a impedire che hacker e altri malintenzionati eseguano lo spoofing dell'organizzazione e del dominio
DNS	Domain Name System.
Docker	Software per la creazione di container.
DORA DLP	Digital Operational Resilience Act: regolamento europeo che stabilisce un quadro unificato per la gestione dei rischi informatici nel settore dei servizi finanziari dell'Unione Europea. Data Loss Prevention: sistemi e tecniche per prevenire la perdita e/o il furto di dati nel corso del loro trattamento, archiviazione inclusa.
DMZ	DeMilitarized Zone: isola del sistema informatico costituita da sottoreti locali, fisiche o virtuali, ove sono allocati i server esposti ad Internet.
DNS	Domain Name System: sistema gerarchico di nomi (naming) di host su Internet che vengono associati al loro indirizzo IP di identificazione nella rete.
Download	Azione di scaricare file o informazioni, tipicamente via Internet.
DR	Disaster Recovery.
Drive-by Downloads	Attacchi digitali causati dallo scaricare (anche inconsapevolmente) codici maligni o programmi malevoli.
Drones, Droni	Si veda bots.
ECCC	European Cybersecurity Competence Centre and Network
ECDL	European Computer Driving Licence: ideata, realizzata e gestita da AICA, ora al 20° anno di vita, è il patentino europeo di conoscenza di vari aspetti dell'ICT soprattutto nell'ottica dell'utente finale.
eCF	European Competence Framework: quadro europeo standardizzato sulle competenze digitali e sui ruoli ICT che espletano professionalmente tali competenze.

ECSF	European Cybersecurity Skills Framework, emanato a fine 2022 da ENISA: considera 10 ruoli per la sicurezza digitale, tra cui il CISO.
EDGE	Enhanced Data rates for GSM Evolution.
EDR	Endpoint Detection and Response.
eIDAS	electronic IDentification Authentication and Signature: regolamento UE n. 910/2014 sull'identità digitale - mira a fornire una normativa di base a livello UE per i servizi fiduciari e l'identificazione elettronica degli Stati membri.
ENISA	European Union Agency for Cybersecurity.
ERT	Emergency Response Team.
ETACS	Extended TACS.
FIRST	Forum of Incident Response and Security Teams, che attualmente ha incarico la gestione della metrica CVSS.
FTP	File Transfer Protocol: protocollo per il trasferimento di file.
Exploit	Attacco ad una risorsa ICT utilizzando sue vulnerabilità.
Extranet	Intranet accessibile anche da utenti esterni all'azienda/ente.
Ethical hacking	Attività di provare attacchi ai fini di scoprire bachi e vulnerabilità dei programmi, e porvi rimedio con opportune patch/fix.
EUCIP	European Certification of Informatics Professionals: ora sostituito da eCF.
FIDO2	Standard per l'autenticazione biometrica
Fix	correzione di un programma software, usato spesso come sinonimo di patch.
Flash threats	Tipi di virus in grado di diffondersi molto velocemente.
Flooding	Letteralmente significa "allagamento" ed è un termini associato a varie tecniche per attacchi DoS/DDoS.
Form	In informatica indica il campo generato da una applicazione visibile su una schermata, nel quale l'utente deve inserire dei caratteri per interagire con l'applicazione stessa; è l'elemento base per l'interfaccia tra utente e applicazione per l'inserimento dei dati (data entry).
FSD	Fornitori di Servizi Digitali, così come definiti da NIS.
FTPS	File Transfer Protocol Secure: per il trasferimento di file crittati
FW	FireWall generico, normalmente di rete.
FWA	FireWall Applicativo.
GDPR	General Data Protection Regulation: Regolamento 2016/679 UE per la protezione dei dati personali delle persone fisiche (privacy).
GenAI	Generative AI: un tipo di AI.
GPRS	General Packet Radio Service.
GSM	Global System for Mobile communications.
Hactivism	Termine derivato dalla combinazione di hack e di activism, indica un uso sovversivo dell'ICT per promuovere un'ideologia politica/religiosa e la sua agenda o un cambiamento sociale.
Hijacking	Tipico attacco in rete "dell'uomo in mezzo" tra due interlocutori, che si maschera per uno dei due e prende il controllo della comunicazione. In ambito web, questo termine è usato per indicare un attacco ove: le richieste di pagine a un web vengo dirottate su un web falso (via DNS), sono intercettati validi account di e-mail e poi attaccati questi ultimi (flooding).
Hoax	In italiano "bufala" o burla, indica la segnalazione di falsi virus; rientra tra le tecniche di social engineering.
Honeynet	Rete di honeypot.
Honeypot	Sistema "trappola" su Internet per farvi accedere con opportune esche possibili attaccanti e poterli individuare.

Hosting	Servizio che “ospita” risorse logiche ICT del Cliente su hardware del fornitore del servizio.
Housing	Concessione in locazione di uno spazio fisico, normalmente in un Data Center già attrezzato, ove riporre, funzionanti, le risorse ICT di proprietà del Cliente.
HSDPA	High Speed Downlink Packet Access.
HTTPS	HyperText Transfer Protocol Secure: protocollo sicuro per le transazioni crittate tra browser e sito web, e viceversa.
Hypervisor	Elemento di base di un sistema virtualizzato, che crea e gestisce sistemi virtuali.
IA IAA	Intelligenza Artificiale Identificazione - Autenticazione – Autorizzazione: per il controllo degli accessi ai sistemi ICT.
IaaS	Infrastructure as a Service.
IAM	Identity & Access Management.
ICS	Industrial Control System (in ambienti OT)
IDS	Intrusion Detection System.
Information Leakage	Diffusione-dispersione non autorizzata di informazioni.
Info stealer (anche infostealer)	Malware progettati per carpire informazioni, tipicamente quelle di un utente mentre effettua un login
Intranet	Rete e server operanti in http/https ed accessibili solo ad utenti interni ad una data azienda/ente.
IoT	Internet of Things (Internet delle Cose): componenti/sistemi intelligenti ed interoperanti su Internet, tipici di ambienti OT.
IIoT	Industrial IoT.
IPS	Intrusion Prevention System.
ISACA	Information Systems Audit and Control Association.
ISSA	Information Systems Security Association: AIPSI è il suo capitolo italiano
ISTAT	Istituto Nazionale di Statistica
ITIL	Information Technology Infrastructure Library: consolidata best practice per la gestione operativa (management) di un SI.
JWC	Joint Warfare Centre in ambito NATO
Kerberos	Metodo sicuro per autenticare la richiesta di un servizio, basato su crittografia simmetrica. Utilizzato da Active Directory.
KEV	Known Exploited Vulnerabilities, catalogo basato su CVE e gestito dalla agenzia statunitense CISA.
Kubernetes	Sistemi per la gestione di carichi di lavoro e servizi containerizzati in ambito cloud, in grado di facilitare sia la configurazione dichiarativa che l'automazione.
LDAP	*Lightweight Directory Access Protocol: protocollo standard per la gestione e l'interrogazione dei servizi di directory che organizzano e regolano in maniera gerarchica le risorse ICT ed il loro utilizzo da parte degli utenti. Il termine LDAP indica anche il sistema di directory nel suo complesso.*
LLM	Large Language Model: tipo di IA
Log bashing	Operazioni tramite le quali un attaccante cancella le tracce del proprio passaggio e attività sul sistema attaccato. Vengono ricercate e distrutte le voci di registri, log, contrassegni e file temporanei, ecc. Possono operare sia a livello di sistema operativo (es. deamon sui server Unix/Linux), sui registri dei browser, ecc. Esistono innumerevoli programmi per gestire le registrazioni, ma sono tecnicamente complessi.
LTE	Long Term Evolution.
MAC	Mandatory Access Control.
MAC	Codice indirizzo assegnato in modo univoco ad ogni scheda di rete.
MAC	Media Access Control: sub strato del livello datalink del modello ISO/OSI.

MAC flooding	Tecnica di attacco tipo DoS/DDoS ad un dispositivo con indirizzo MAC per saturarlo e bloccarne il corretto funzionamento.
Malicious insider	Attaccante interno all'organizzazione cui viene portato l'attacco.
Malvertising	Contrazione di "malicious advertisements": pubblicità malevola, con pagine web che nascondono un codice maligno o altre tecniche di attacco, come il dirottamento su siti web mascherati e fraudolenti.
Malware	Termine generico che indica qualsiasi tipo di programma software di attacco.
MaaS	Malware as a Service: fornitura in cloud di malware (a pagamento).
MEHARI	MEthod for Harmonized Analysis of Risk.
MFA	Multi-Factor Authentication: autenticazione con più fattore, ad esempio con certificati, token diversi e identificazioni biometriche.
Microservizi	Approccio allo sviluppo ed all'organizzazione dell'architettura dei software, evoluzione dell'architettura SOA e dell'object orientation. I microservizi sono moduli software autonomi, specializzati, indipendenti di piccole dimensioni che comunicano tra loro tramite API ben definite. Le architetture dei microservizi permettono di scalare e sviluppare le applicazioni in modo rapido e semplice.
Mirroring	termine inglese per indicare la replica e la sincronizzazione di dati su due o più dischi.
MSS	Managed Security Service.
MSSP	Managed Security Service Provider: fornitore di servizi per la sicurezza digitale.
NAC	Network Access Control: termine usato con più significati, che complessivamente indica un approccio architetturale ed un insieme di soluzioni per unificare e potenziare le misure di sicurezza a livello del punto di accesso dell'utente al sistema informativo.
NATO	Organizzazione del Trattato dell'Atlantico del Nord.
NCC-IT	Centro Nazionale di Coordinamento Italiano: fa parte di ACN.
NCS	Nucleo per la cybersicurezza ora operante in ambito ACN.
NFT	Non Fungible Token: è un gettone non riproducibile nell'ambito di una blockchain. Gli NFT sono associati a beni virtuali, da un documento a un'opera d'arte, e come tali hanno un mercato mondiale.
NIS	Network and Information Security: direttiva UE 2016/1148, recepita in Italia con il D. Lgs. n. 65 del 18/5/2018, che definisce le misure di sicurezza digitale necessarie a livello di ogni paese membro per le infrastrutture ICT critiche, chiamate anche "servizi essenziali".
NIS2	Aggiornamento ed ampliamento della NIS
NIST	National Institute of Standards and Technology
NSTPFT	Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza contrastare le frodi telematiche ed informatiche, nonché tutelare la privacy.
NVD	National Vulnerability Database statunitense, gestito da NIST
OASIS	Consorzio di aziende ICT no profit che fornisce norme implementative per alcuni standard, tra i quali la SOA e la sua sicurezza (SALM SPML, XACML).
OCSI	Organismo di Certificazione della Sicurezza Informatica: ora fa parte di ACN
OLE	Object Linking and Embedding.
OPC	OLE for Process Control (ambito OT).
OPS	Open Platform Communications. Standard de facto per la comunicazione tra sistemi OT
OPS UA	Open Platform Communications Unified Architecture.
OSA	Open Security Architecture.
OT	Operational Technology.
OTP	One Time Password: logica e/o dispositivo che genera password da usarsi una sola volta per sessione/transazione.
Outsourcer	Fornitore di servizi digitali terziarizzati.
OWASP	Open Web Application Security Project.

PaaS	Platform as a Service.
PAC	Pubblica Amministrazione Centrale.
PAC	Programmable Automation Controller (ambiti OT).
PAL	Pubblica Amministrazione Locale.
PAM	Privileged Access Management.
Payload	"Carico utile" di informazioni all'interno di un programma, di un protocollo, ecc.; tipicamente è il codice maligno da attivare sul sistema attaccato dopo esservi penetrati.
PEC	Posta Elettronica Certificata.
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 digitale di social engineering per carpire informazioni riservate di un utente, basato sull'invio di un falso messaggio in posta elettronica che fa riferimento ad un ente primario, che richiede di collegarsi ad un server (trappola) per controllo ed aggiornamento dei dati.
PID	Proportional-Integral-Derivative (in ambito OT)
PIN	Personal Identification Number
Ping of death	Invio di pacchetti di ping di grandi dimensioni (ICMP echo request), che blocca la pila di protocolli TCP/IP: è un tipo di attacco DoS/DDoS.
PLC	Programmable Logic Controller (ambiti OT).
PMI	Piccole e Medie Imprese: sotto i 250 dipendenti.
PNRR	Piano Nazionale di Ripresa e di Resilienza.
Port scanner	Programma software che esplora una fascia di indirizzi IP sulla rete per verificare quali porte, a livello superiore, sono accessibili e quali vulnerabilità eventualmente presentano. È uno strumento di controllo della sicurezza, ma è anche uno strumento propedeutico ad un attacco.
Provisioning	Attività grazie alle quale vengono fornite le opportune risorse ICT e la loro configurazione, in particolare i diritti d'accesso, ad utenti di un SI
PUP	Potentially Unwanted Programs: programma che l'utente consente di installare sui suoi sistemi ma che, a sua insaputa, contengono codici maligni o modificano il livello di sicurezza del sistema. Tipici esempi: adware, dialer, sniffer, port scanner.
QR	Quick Response: è un codice a barre bidimensionale, ossia a matrice, che è impiegato per memorizzare informazioni generalmente destinate a essere lette tramite uno smartphone.
Race condition	Termine che indica le situazioni derivanti da condivisione di una risorsa comune, ad esempio un file o un dato, ed in cui il risultato viene a dipendere dall'ordine in cui vengono effettuate le operazioni.
Ransomware	Codice maligno che restringe e/o blocca i diritti d'accesso e tramite il quale viene chiesto un riscatto (ransom) per far funzionare correttamente il sistema.
RBAC	Request Based Access Control.
RBAC	Role Based Access Control.
RFID	Radio-Frequency Identification: tecnologia per l'identificazione e/o memorizzazione automatica di informazioni inerenti oggetti, animali o persone, basata su un tag intelligente identificativo dell'entità oggetto dell'identificazione ed un dispositivo in grado di riconoscere l'entità se in sua prossimità, scambiando in radio frequenza delle informazioni.
Ricatto	L'attacco digitale perpetrato viene poi usato per ricattare l'attaccato perché paghi per non subirne di altri, magari più perniciosi. Il malware ransomware ha come tipica motivazione il ricatto, che è un tipo della più generale frode informatica.
Ritorsione	L'attacco digitale è stato portato come "vendetta" verso torti subiti, o come tali ritenuti: tipico il caso di un dipendente cui è stata negata una sua richiesta, o di ex dipendente

	licenziato. L'attaccante intende "colpire" con un attacco digitale l'Azienda/Ente che ritiene "colpevole" dei (presunti) torti subiti.
Robot	Un sistema in grado di svolgere, più o meno indipendentemente, un lavoro al posto dell'uomo
Robotica	La disciplina dell'ingegneria che studia e sviluppa metodi che permettano a un robot di eseguire dei compiti specifici riproducendo in modo automatico il lavoro umano.
Rogueware	Falso antivirus che a sua volta è un codice maligno che infetta il sistema.
Rootkit	Programma software di attacco che consente di prendere il completo controllo di un sistema, alla radice come indica il termine.
RPU	Remote Processor Unit (in ambiti OT).
SaaS	Software as a Service.
SALM	Security Assertion Markup Language.
SASE	Secure Access Service Edge.
SCADA	Supervisory Control And Data Acquisition: sistema informatico distribuito per il controllo ed il monitoraggio di processi, ed in parte per la loro automazione, in ambiti 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.
Scammer	Chi effettua uno scam.
SCAP	Security Content Automation Protocol.
SCC	Security Command Centre.
Scareware	Software d'attacco che finge di prevenire falsi allarmi, e diffonde notizie su falsi malware o attacchi.
Scraping	Letteralmente significa "raschiando", è il termine usato per indicare l'attività di ricerca e raccolta, in maniera automatica, di determinate informazioni dai sistemi connessi in Internet.
SD-WAN	Software Defined WAN (Wide Area Network)
SGSI	Sistema Gestione Sicurezza Informatica.
SIEM	Security Information and Event Management: sistemi e servizi per la gestione in tempo reale di informazioni ed allarmi generati dalle risorse ICT di un sistema informativo, inclusi i log.
Sinkhole	metodo per reindirizzare specifico traffico Internet per motivi di sicurezza, tipicamente per analizzarlo, per individuare attività anomale o per sventare attacchi. Può essere realizzato tramite darknet o honeynet.
Sistema Informatico	Insieme dei sistemi e dei servizi ICT, dalle reti ai server ed agli applicativi, anche terziarizzati e in cloud, organizzato in una specifica architettura e che una azienda/ente usa a supporto delle proprie attività. Il sistema informatico può includere anche i dispositivi d'utente fissi e mobili (PC, smartphone, tablet, etc.), i sistemi di automazione e controllo industriale (DCS, PLC, robot, ecc.) ed i dispositivi IoT. Il termine indica quindi l'insieme dei sistemi ICT che lo costituiscono
Sistema Informativo	Indica il Sistema Informatico con tutte le informazioni che vi sono trattate.
Sniffing-snooping	Tecniche mirate a leggere il contenuto (pay load) dei pacchetti in rete, sia LAN che WAN.
Slack	Servizio di messaggistica per le aziende che collega le persone alle informazioni di cui hanno bisogno, creando e gestendo gruppi di lavoro.
Smart city	Città "intelligente" largamente dotata di infrastrutture e soluzioni ICT sia per i suoi abitanti e per interagire con loro, sia per migliorare il controllo del territorio, della sua sicurezza, dell'ambiente, della viabilità, ecc.
Smart grid	Grid è la rete elettrica di distribuzione di energia, che affiancata da una rete informatica che la gestisce diviene "smart".

Smishing	Attacco di social engineering per carpire informazioni riservate di un utente, basato sull'invio di SMS. E' l'analogo del phishing con la posta elettronica.
SMS	Short Message Service.
Smurf	Tipo di attacco per la saturazione di una risorsa, avendo una banda trasmissiva limitata. Si usano tipicamente pacchetti ICMP Echo Request in broadcast, che fanno generare a loro volta ICMP Echo Replay.
SOA	Service Oriented Architetture.
SOAR	Security Orchestration, Automation and Response: sistemi di automazione ed integrazione dei vari strumenti e processi di sicurezza digitale.
SOC	Security Operation Centre.
Social Engineering	Ingegneria sociale: con questo termine vengono considerate tutte le modalità di carpire informazioni, quali l'user-id e la password, per accedere illegalmente ad una risorsa informatica.
Spamming	Invio di posta elettronica "indesiderata" all'utente.
SPF	Sender Policy Framework: in DMARC, un record di testo DNS nel dominio considerato, che indica ai servizi di posta e ai ricevitori di ricevere l'e-mail dall'IP del server fornito nel record SPF.
SPID	Sistema Pubblico di Identità Digitale: è attualmente obbligatorio per accedere on line ai servizi digitali delle Pubbliche Amministrazioni.
SPML	Service Provisioning Markup Language.
Spoofing	Attacco digitale che falsifica l'indirizzo nell'intestazione Da: di un messaggio email. Un messaggio contraffatto mediante lo spoofing sembra provenire dall'organizzazione o dal dominio la cui identità è stata rubata.
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.
SQL	Structured Query Language: linguaggio per interazione con un DB relazionale.
SQL injection	Tecnica di inserimento di codice in un programma che sfrutta delle vulnerabilità sul database con interfaccia SQL che viene usata dall'applicazione.
SSCP	Systems Security Certified Practitioner.
SSO	Single Sign On: autenticazione unica per avere accesso a diversi sistemi e programmi.
Stealth	Registrazione invisibile.
Stuxnet	Uno dei primi e più noti attacchi ATP, portato ai sistemi di controllo delle centrifughe delle centrali nucleari iraniane.
SYN Flooding	Invio di un gran numero di pacchetti SYN a un sistema per intasarlo (DoS/DDoS).
TA	Targeted Attacks: attacchi mirati, talvolta persistenti, effettuati con più strumenti anche contemporaneamente; rientrano in questa categoria APT e Watering Hole.
TACS	Total Access Communication System.
Telegram	Servizio di messaggistica istantanea e di broadcasting criptato e gratuito.
TLC	Telecomunicazioni.
Troll Troll net Trojan Horse	Utenti di Internet, e in particolare di social net, che pubblicano messaggi Gruppo organizzato di troll Cavallo di Troia: codice maligno che realizza azioni indesiderate o non note all'utente. I virus fanno parte di questa categoria.
TOR	The Onion Router: sistema di comunicazione anonima in Internet basato sul protocollo onion router e su tecniche di crittografia.
Trouble ticketing	Processo e sistema informatico di supporto per la gestione delle richieste e delle segnalazioni da parte degli utenti; tipicamente in uso per help-desk e contact center.
UE	Unione Europea.

UEBA	User and Entity Behavioral Analytics.
UOSI	Unità Organizzativa Sistemi Informativi.
UMTS	Universal Mobile Telephone System.
URL	Uniform Resource Locator: sequenza di carattere che identifica in maniera nome univoca una risorsa ICT in rete; esempio: www.oadweb.it.
Utente finale	Utente di un sistema d'utente e/o di una o più applicazioni con i diritti di accesso relativi al suo ruolo, ma non di tipo privilegiato.
Utente privilegiato	Utenti con diritti d'accesso privilegiati: includono operatori, manutentori ed amministratori di sistema di un sistema informativo, che hanno i più elevati diritti per poter accedere e gestire le risorse ICT del sistema informatico sulle quali debbono operare. Rientrano in questa categoria anche gli sviluppatori di software. Gli attuali trend di forte terziarizzazione di queste funzioni portano a personale esterno dei fornitori dell'azienda/ente cliente tali diritti, con la necessità di maggiori controlli su di loro per assicurarsi l'adeguate livello di sicurezza digitale.
Vishing	Attacco di social engineering per carpire informazioni riservate di un utente, basato su chiamate telefoniche. E' l'analogo del phishing con la posta elettronica.
VoIP	Voice over IP.
VPN	Virtual Private Network: rete virtuale creata tramite Internet per realizzare una rete "privata" e sicura per i soli utenti abilitati.
XACML	eXstensible Access Control Markup Language.
XSS	Cross - site scripting: una vulnerabilità di un sito web attendibile che consente di inserire a livello "client" dei codici maligni via "script", ad esempio JavaScript, ed HTML per modificare le pagine web che l'utente vede.
Watering Hole	Famiglia di attacchi che rientrano nella categoria dei Targeted Attack. Il termine, traducibile in" attacco alla pozza d'acqua", fa riferimento agli agguati di animali carnivori alle prede che si dissetano in una pozza d'acqua. La metafora è usata per attacchi mirati a siti web specialistici, ad esempio di finanza, di politica, di strategie, ecc., cui una persona o un'azienda target accede periodicamente.
Wiper	Malware distruttivo che manipola e/o cancella il driver di un hard disk, eliminando tutti i dati archiviati e non consentendo più il suo utilizzo.
Worm	Tipo di virus che non necessita di un file eseguibile per attivarsi e diffondersi, dato che modifica il sistema operativo del sistema attaccato in modo da essere eseguito automaticamente e tentare di replicarsi sfruttando per lo più Internet.
Zero-day attack	Attacchi basati su vulnerabilità ancora non note e/o a cui non è ancora stato trovato rimedio.
Zero Trust	Modello di sicurezza informatica che elimina la fiducia implicita all'interno di una rete.
Zombies, zombi	Si veda bots.
ZTA	Zero Trust Architecture: framework-architettura per la sicurezza digitale basato sul principio "never trust, always verify".

ALLEGATO C Profili SPONSOR SILVER

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 è **Google Cloud Partner** e 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 inoltre 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.

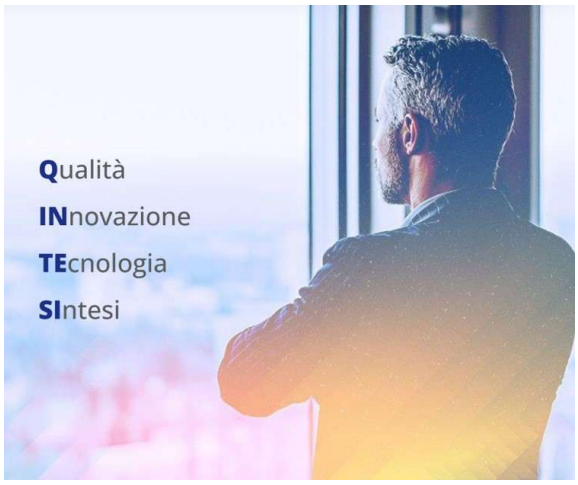
Qintesi ha stretto una partnership con SAP **Fioneer**, leader globale nelle soluzioni software per l'industria dei servizi finanziari al fine di fornire alle istituzioni finanziarie soluzioni all'avanguardia e supportarle nell'implementazione di progetti complessi.

Infine, Qintesi ha stretto una partnership 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.

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 D Profilo Patrocinatori

AICA

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 digitali. Tra le varie sue iniziative, ha realizzato a livello europeo l' ECDL e l'eCF (UNI EN 16234-1:2016): per quest'ultimo è accreditata come ente certificatore.

https://www.aicanet.it/

AIP-ITCS

L'Associazione Informatici Professionisti vuole rappresentare unicamente il capitale umano del settore ICT, per consentire agli associati di operare nel mercato dei servizi e del lavoro con autorevolezza, competenza e professionalità, in modo da contribuire positivamente allo sviluppo socio-economico del Paese e della "società della conoscenza e della comunicazione", con soddisfazione del cliente e del consumatore.

https://web.aipitcs.it/

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/

Anitec-Assinform

Operante nell'ambito confindustriale, è l'associazione di settore delle imprese che operano in Italia nella produzione di software, sistemi e apparecchiature elettroniche e nella fornitura di soluzioni applicative e di reti, di servizi a valore aggiunto e contenuti connessi all'uso dell'ICT e allo sviluppo dell'innovazione digitale.

https://www.anitec-assinform.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/

ASSI-Bologna

Associazione Specialisti Sistemi Informativi, è l'associazione senza fine di lucro di professionisti dell'ICT che favorisce e stimola l'incontro fra colleghi, in maniera del tutto informale, e realizza un piano di informazione periodico attraverso incontri e seminari scelti e finanziati dai Soci. Aderisce a FIDAInform.

www.assi-bo.it

ASSO-DPO

L'Associazione Data Protection Officer è un significativo punto di riferimento dei propri associati per discutere ed approfondire le tematiche relative all'applicazione della normativa europea ed italiana in materia di privacy e data protection.

https://www.assodpo.it/

AUSED

Associazione tra Utenti di Sistemi e Tecnologie dell'Informazione, è una associazione indipendente e senza scopi di lucro che raggruppa aziende e professionisti del lato domanda ICT, che operano in diversi settori, tra cui quello industriale, manifatturiero, dei servizi, nonché alcuni enti pubblici.

www.aused.org

Club del Digitale e dell'Innovazione di Torino

Libera associazione privata, apolitica senza scopi di lucro dell'area torinese-piemontese, che si propone come punto di riferimento e di incontro per i professionisti della comunità IT. Aderisce a FIDAInform.

http://www.clubdi.org/

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/

CIOClub Italia

Libera associazione tra professionisti dell'IT per condividere conoscenza e confrontarsi per lavoro o per passione, nella gestione dei dipartimenti IT. Obiettivi: sviluppare idee comuni, realizzare grandi progetti, condividere iniziative di successo.

https://cioclubitalia.it/

Club per le Tecnologie dell'Informazione dell'Emilia-Romagna

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT dell'area regionale, i cui membri sono consulenti e professionisti manageriali del settore informatico. Primari obiettivi lo sviluppo sociale, economico e industriale del Paese attraverso la promozione di un corretto uso delle Tecnologie dell'Informazione. Aderisce a FIDAInform

Club per le Tecnologie dell'Informazione di Milano

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT dell'area milanese-lombarda per la promozione delle discipline digitali attraverso la crescita professionale e lo scambio di competenze tra i soci. Aderisce a FIDAInform.

http://www.clubtimilano.net/

Club per le Tecnologie dell'Informazione della Liguria

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT dell'area genovese-ligure, per promuovere l'innovazione ICT e lo scambio di conoscenze tra i propri soci, che operano nel campo dell'ICT sia come utilizzatori che come fornitori. Aderisce a FIDAInform.

http://www.ctiliguria.it/

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/

CSA, Cyber Security Angels

Associazione di persone d'impresa, tipicamente CISO e CIO, costituito per creare una rete di conoscenze dirette al fine di far fronte comune alle problematiche nascenti sul fronte della Cyber Security.

https://www.cybersecurityangels.it/

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/

FIDAInform

Federazione Nazionale delle Associazioni Professionali di Information Management: è la federazione a livello nazionale dei vari Club della tecnologia dell'informazione operanti a livello regionale. Si propone come "nodo" attivo del Sistema-Paese per lo sviluppo del settore delle tecnologie dell'informazione e della comunicazione, promuovendo la professionalità dei Soci.
http://www.fidainform.it/

Inforav

Istituto per lo sviluppo e la gestione avanzata dell'informazione, è una libera associazione senza scopi di lucro, a cui aderiscono Amministrazioni ed Enti pubblici, Associazioni, Fondazioni, Società Finanziarie, Commerciali ed Industriali di primaria rilevanza nazionale; promuove e sviluppa iniziative di interesse generale o della Pubblica Amministrazione, con la collaborazione dei propri Soci e anche di esperti di conclamata competenza, in diversi settori dell'ICT e dell'Organizzazione. Aderisce a FIDAInform.

http://www.inforav.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/

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 E Principali fonti e riferimenti

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

- FTI: "Osservatorio sulla criminalità informatica – Rapporto 1997", 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", publicato su Linea EDP, 31 Luglio 2025: https://www.lineaedp.it/featured/il-fattore-umano-nella-sicurezza-digitale/

E.2 Le principali fonti sugli attacchi e sulle vulnerabilità

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://cve.mitre.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/
- 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/
- SANS Institute fornisce sistematicamente segnalazioni su vari tipi di attacchi e di vulnerabilità, oltre all'aggiornato elenco 20 prioritari controlli di sicurezza per le norme Federali US FISMA: www.sans.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/
- WASC, Web Application Security Consortium, effettua vari progetti indipendenti sulla sicurezza digitale per le applicazioni web, e fornisce il WASC Threat Classification Online, simile a OSWAP: http://www.webappsec.org/,
- World Economic Forum, realizza un annuale rapporto sui rischi globali, che includono anche i rischi ICT e le cyberwar: https://www.weforum.org/reports/global-risks-report-2023/

Allegato F AIPSI

AIPSI – Associazione Italiana Professionisti Sicurezza Informatica

AIPSI è una associazione italiana di sole persone fisiche, no profit e indipendente, capitolo italiano della mondiale ISSA® – Information Systems Security Association (più di 13000 Soci in 100 Capitoli nel mondo)

AIPSI è rivolta ai professionisti che si occupano a vario titolo di cybersicurezza e di cyber resilience.

Aiuta concretamente i soci nella loro crescita professionale e promuove la cultura della sicurezza digitale in ambito pubblico, privato e accademico, rappresentando un punto di riferimento per esperti, aziende, enti e istituzioni.

AIPSI si propone di:

- Diffondere la **consapevolezza e la cultura della cybersecurity**
- Promuovere la **formazione continua** e la **certificazione delle competenze**
- Favorire il **dialogo tra professionisti**, imprese, PA e mondo accademico
- Contribuire allo sviluppo di normative, best practice e standard internazionali
- Collaborare attivamente con varie associazioni nazionali, e con la federazione FIDAInform di cui è componente

Principali attività

- **Eventi e convegni**: seminari, webinar, workshop aperti a professionisti, aziende e istituzioni, ed alcuni riservati ai Soci.
- **Osservatori e ricerche**: il principale è **OAD,** Osservatorio Attacchi Digitali in Italia, indagine annuale su attacchi e minacce cyber a livello nazionale.
- **Mentorship** gratuita ai Soci di AIPSI e delle associazioni federate in FIDAInform sull'indirizzo e la crescita professionale.
- **Tavoli di lavoro e gruppi tematici**: per lo sviluppo di linee guida operative e confronti su casi concreti
    - **AIPSI School:** iniziativa educativa per sensibilizzare e formare studenti/studentesse delle scuole medie e delle superiori sui temi della sicurezza digitale, dell'uso consapevole degli strumenti informatici e della cittadinanza digitale.
- **Collaborazioni internazionali**: partecipazione a progetti e iniziative globali nel campo della cybersecurity

A chi ci rivolgiamo

- Professionisti ICT e della sicurezza informatica
- CISO, CIO, DPO, CTO, amministratori di sistema e responsabili IT, di imprese pubbliche e private
- Manager, consulenti e auditor in ambito sicurezza, compliance e risk management
- Università e studenti interessati ad avvicinarsi al mondo della cybersecurity
- Istituzioni pubbliche, enti normativi e organismi di vigilanza

Perché aderire ad AIPSI

- Entrare in un **network autorevole** e qualificato a livello mondiale
- Partecipare attivamente a eventi, osservatori e tavoli tecnici

- Accedere a contenuti e aggiornamenti esclusivi
- Avere **visibilità professionale** nel panorama italiano della sicurezza informatica
- Contribuire allo **sviluppo della cultura cyber** in Italia

Diverse modalità di iscrizione ad AIPSI

- Socio AIPSI-ISSA: prezzo US$ 160,00 per anno (12 mesi)
- Socio SOLO AIPSI: prezzo € 50,00 per annuo 12 mesi)
- Socio AIPSI-GIOVANE: fino a 27 anni, a tutti i servizi del Socio SOLO AIPSI:
  - Primo annuo di iscrizione GRATUITO
  - Dal secondo fino ai 27 anni € 25,00 per anno (12 mesi)
- La Tabella sottostante confronta i vari servizi disponibili ai Soci

Servizio-Iniziativa AIPSI/ISSA	Socio AIPSI-ISSA	Socio SOLO AIPSI	Socio GIOVANE	Non Socio
Webinar/evento pubblico AIPSI (richiede registrazione)	√	√	√	√
Newsletter AIPSI mensile (richiede registrazione)	√	√	√	√
OAD, Osservatorio Attacchi Digitali in Italia	√	√	√	√
SIG CSWI, Cyber Security Women Italy	√	√	√	√
Accesso sito web e social net AIPSI pubblici	√	√	√	√
Webinar/evento riservato Soci AIPSI	√	√	√	
Possibilità di essere oratore in eventi/webinar AIPSI	√	√	√	
Mentorship di indirizzamento e crescita professionale	√	√	√	
SIG Competenze, crescita e percorsi professionali	√	√	√	
SIG Architetture Sicurezza Digitale	√	√	√	
SIG Intelligenza Artificiale e sicurezza digitale	√	√	√	
Supporto e sconto certificazione eCFPlus (UNI EN 16234-1:2016) per le figure di Security Manager e Security Specialist con AICA	√	√	√	
Sconti con altre Associazioni ed Aziende da accordi AIPSI	√	√	√	
Possibilità di scrivere articoli in nome e per conto di AIPSI	√	√	√	
Networking nazionale tra Soci AIPSI	√	√	√	
Possibilità di essere eletto/nominato Consigliere o in altri ruoli decisionali di AIPSI	√			
Rappresentanza AIPSI in altre Associazioni o in tavoli istituzionali	√			
Essere oratori in un convegno all'estero in nome e per conto di AIPSI	√			
Rivista mensile ISSA Journal	√			
Indagine ESG ISSA "The Life and Times of Cyber Security Professionals"	√			
Seguire convegni, workshop, webinar ISSA (n inglese)	√			
Seguire corsi online in inglese	√			
Partecipare a vari SIG, Special Interest Group, ISSA	√			
Sconti su corsi e certificazioni individuali all'estero per accordi ISSA	√			
Possibilità di scrivere articoli su riviste/eventi all'estero in nome e per conto di AIPSI	√			
Network soci AIPSI ed ISSA a livello mondiale	√			

Per associarsi si veda: https://www.aipsi.org/associazione/come-associarsi.html

Per contatti e per avere ulteriori informazioni scrivere a: aipsi@aipsi.org

Allegato G Malabo srl

Malabo Srl, https://www.malaboadvisoring.it/, opera dal 2001 nell'ambito della consulenza direzionale sull'ICT e sulla trasformazione digitale per clienti lato sia offerta sia domanda ICT, basandosi su una rete consolidata di esperti "senior" e di società ultra-specializzate su specifici temi dell'ICT e della sicurezza digitale.

Malabo opera professionalmente sulle seguenti settori:

- interventi consulenziali
  - presso il responsabile del sistema informativo (CIO) e/o del responsabile sicurezza digitale (CISO) e dei loro staff: riorganizzazione della struttura, rapporti con l'alta direzione e con le altre direzioni, miglioramento della gestione operativa e della "governance" del Sistema Informativo (SI) e della sua sicurezza, ruolo di supervisore o di capo progetto in progetti critici, potenziamento misiure di sicurezza tecniche ed organizzative, Piano di Disaster Recovery e suo periodico test, etc.;
  - presso l'Alta Direzione ed i suoi componenti operativi (Board of Director, Consiglio di Amministrazione, Amministratore, Direttore Generale, CEO, COO, CTO, etc.) per la valutazione dell'efficacia e dell'efficienza dell'attuale struttura organizzativa (e delle sue competenze e capacità) del SI, per migliorare ed accelerare la trasformazione digitale, per la compliance alle diverse normative europee ed italiane (GDPR, NIS2, CER, DORA, etc.), per migliorare la governance del SI, per il Piano di Business Continuity e suo periodico test, per l'analisi del valore dell'ICT, per la valutazione delle competenze ICT secondo gli standard europei;
  - presso il responsabile commerciale e/o di marketing (ma sovente anche con l'AD/DG) delle aziende dell'offerta, individuazione di tecnologie e soluzioni innovative su cui investire e/o da acquisire, indicazioni e supporto per riposizionamento sul mercato, etc.;
- interventi di formazione e di sensibilizzazione sia in aula che da remoto con webinar/web live/e-learning;
- l'attivazione e la gestione di specifici strumenti informatici di supporto, sviluppati e personalizzati da Malabo nel corso della consulenza, o acquisiti dal Cliente (come uno dei risultati della consulenza stessa) o preesistenti presso il Cliente.

Il denominatore comune di ogni intervento è aiutare il cliente in modo che l'ICT crei un effettivo e misurabile **valore** per il suo business e per le sue attività.

Le principali aree di eccellenza e competenza di Malabo includono le tecnologie e le architetture ICT, la sicurezza digitale (cybersecurity), il governo e la gestione del SI, la conformità a normative e standard (compliance), le competenze, profili e ruoli ICT nell'organizzazione.

I vantaggi competitivi di Malabo, percepibili dai clienti, includono l'effettiva, consolidata esperienza e l'aggiornata competenza dei suoi professionisti, da cui deriva la semplicità, la velocità e l'economicità dell'intervento, la contestualizzazione dell'intervento sulla realtà del Cliente con la realizzazione di soluzioni su misura e con un effettivo trasferimento di conoscenza, il riferimento agli standard e alle best practice internazionali, l'utilizzo di strumenti informatici di supporto.

Per maggiori informazioni: www.malaboadvisoring.it e/o inviare una e-mail a info@malaboadvisoring.it

Allegato H 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 fondatore e CEO di **Malabo S.r.l.** (https://www.malaboadvisoring.it/), attiva dal 2001, specializzata in progetti di innovazione, sicurezza digitale e strategie ICT per aziende ed enti pubblici.

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: 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**: Architetture ICT, cloud e microservizi, 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, compliance.
- Tutti i corsi includono casi reali tratti dall'esperienza diretta.

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 **240 pubblicazioni**, tra cui **50 libri e rapporti internazionali**.

AIPSI c/o Malabo srl Via Savona, 26 20144 Milano - tel. 02 72191512 aipsi@aipsi.org

Malabo Srl Via Savona 26 20144 Milano - tel. 02 72191512 info@malaboadvisoring.it

OAD Osservatorio Attacchi Digitali in Italia

aipsi ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

ASSOCIAZIONI PATROCINANTI OAD 2025

AICA

AIP Associazione Informatici Professionisti — ITCS Italian Computer Society

AISIS Associazione Italiana Sistemi Informativi in Sanità — CHIME International Italy Chapter

AITASIT Associazione Italiana Amministratori di Sistema e Telemedicina

ANIPA

Anitec-Assinform

ANORC

ASSOCIAZIONE SPECIALISTI SISTEMI INFORMATIVI

ASSO DPO Associazione Data Protection Officer

ASE BE THE CHANGE 1976

Club Digitale Innovazione Torino

CDTI

CIO club — CIOCLUB ITALIA

CTI Club

CTI Liguria

ClubTI Club per le tecnologie dell'informazione

CONFASSOCIAZIONI Digital

CSA Cyber Security @ngels — Security by Sharing

CSIG Ivrea - Torino

FIDA INFORM

Inforav Istituto per lo sviluppo e la gestione avanzata dell'informazione

OWASP ITALY

SESAMO Associazione Amministratori Immobiliari