OAD
Osservatorio
Attacchi Digitali
in Italia

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

Rapporto 2023 OAD

a cura di Marco R. A. Bozzetti

con la collaborazione della Polizia Postale e delle Comunicazioni

Sponsor Gold

QINTESI

Indagine AIPSI realizzata da

malabo
ICT Advisory

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 2021.
Un grazie particolare agli Sponsor e alle persone che hanno collaborato in vario modo alla realizzazione del questionario on line e del rapporto finale:

- per AIPSI: Massimo Chirivì
- per Malabo Srl: dott. Andrea Bozzetti, dott. Francesco Zambon
- per la Polizia Postale e delle Telecomunicazioni, che ha fornito dati e testi del Capitolo 8: il Direttore dott. Ivano Gabrielli, l'Ispettore dott. Gaetano Martucci e l'Agente dott. Antonio Micello

Dichiarazione di non responsabilità

I grafici ed i testi del presente rapporto 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 2021 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 2023.

OAD è un progetto scelto da Repubblica Digitale
https://repubblicadigitale.innovazione.gov.it/it/i-progetti/

Rapporto OAD 2023 pubblicato il 23 ottobre 2023.

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

Sommario

1. Sintesi direzionale

L'Osservatorio Attacchi Digitali in Italia, OAD, con la presente edizione 2023 giunge al sedicesimo anno di indagini consecutive sugli attacchi digitali e sulle misure di sicurezza dei sistemi informativi in Italia, avvalendosi, come negli anni precedenti, della preziosa collaborazione della Polizia Postale e delle Telecomunicazioni che ha fornito dati e testo del Capitolo 8 del presente Rapporto.
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 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 riesce a fotografare il fenomeno degli attacchi digitali intenzionali in Italia e delle misure di sicurezza in essere nei sistemi informativi delle imprese pubbliche e private italiane. OAD riesce a coinvolgere nell'indagine anche le piccole e piccolissime realtà, che costituiscono in Italia la stragrande maggioranza (per le aziende italiane: 99,91% le PMI, circa 95% quelle con meno di 10 dipendenti) e che altre indagini nazionali ed internazionali difficilmente considerano ed analizzano.

L'indagine **OAD 2023** fa riferimento **all'intero anno 2022**, quando perdurava ancora la coda della pandemia Covid-19, ed era in pieno corso l'invasione della Federazione Russa in Ucraina. Questi due eventi hanno causato, oltre al "tradizionale" crimine informatico, **un forte aumento degli attacchi digitali anche in Italia**: l'**85,1%** delle aziende/enti rispondenti ha rilevato attacchi digitali intenzionali ai loro sistemi informativi, un forte incremento, come trend, rispetto a quanto rilevato da OAD negli anni precedenti, e come evidenziato nella sottostante fig. 1-1.

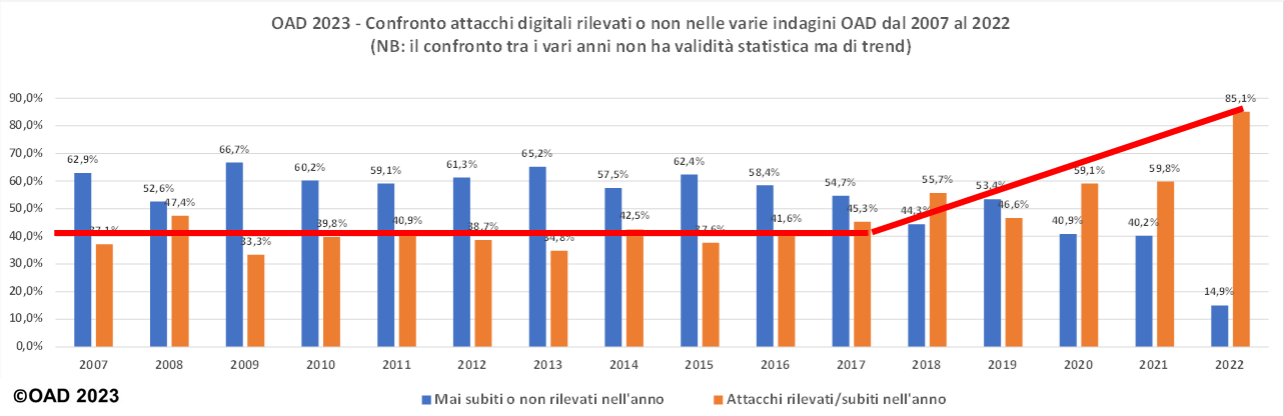


Fig. 1-1

.
La correlazione dei dati sugli attacchi rilevati con le dimensioni ed il fatturato delle aziende/enti rispondenti mostra anche per il 2022 che il maggior numero di attacchi digitali, ed i più sofisticati, sono rivolti ad organizzazioni di grandi dimensioni e fatturato. Le piccole e piccolissime organizzazioni, sia private che pubbliche, non rappresentano un obiettivo di interesse specifico per i cyber criminali negli attacchi mirati, mentre esse possono essere coinvolte in attacchi di massa, come quelli basati sul phishing e sul ransomware.
OAD distingue chiaramente che cosa si attacca, la tipologia d'attacco classificata in 14 diverse macro voci, ed il come si attacca, le tecniche usate per l'attacco e distinte in 7 macro voci. In OAD 2023 le più diffuse tipologie di attacchi digitali ad un sistema informativo dei rispondenti vedono al primo posto le **modifiche malevoli/non autorizzate ai programmi e alle loro configurazioni**, con un valore vicino al **30%** dei rispondenti, causate anche dalla larghissima diffusione di malware e di ransomware in Italia. Seguono gli attacchi **ai sistemi di controllo degli accessi** con un 23,5%, gli attacchi

DoS/DDoS, Denial of Service/Distributed DoS, per la saturazione delle risorse ICT esposte in Internet con un 19,6%, gli attacchi alle **reti** geografiche e locali con un 18,5%. Tutte le altre tipologie di attacco sono state rilevate, con percentuali decrescenti. Come **tecniche di attacco**, le più diffuse tra i rispondenti sono l'uso misto di varie tecniche, con un **35,4%**, e la raccolta malevola e non autorizzata di informazioni, ossia il social engineering, che costituisce nella maggior parte degli attacchi il loro punto di ingresso nel sistema informativo target.

L'indagine OAD 2023 è **focalizzata sugli attacchi ai siti, alle applicazioni e agli ambienti web**. Ormai la maggior parte delle applicazioni sono di tipo web, e molte di queste sono in cloud: i sistemi informativi sono quindi in parte in locale (on premise) e in parte su uno o più cloud di fornitori diversi, il multi cloud. Dal bacino delle aziende/enti rispondenti emerge che il **73,1%** dei loro sistemi informativi **hanno subito nel 2022 questo tipo di attacchi**, e di questi il **54,3% per i propri ambienti web terziarizzati**. Le vulnerabilità più sfruttate per questi attacchi sono state, per il 55,8% dei rispondenti, vulnerabilità tecniche (dell'applicazione web, della piattaforma web, del dispositivo d'utente) e per il 25,8% vulnerabilità degli utenti, sia finali sia soprattutto privilegiati (amministratori di sistemi, sistemisti, fornitori, etc.). Con riferimento alle 10 più diffuse vulnerabilità per web evidenziate da OWASP nel 2022, quelle individuate negli attacchi **più gravi** rilevati dalle aziende/enti rispondenti ad OAD 2023 sono sono al primo posto i componenti software obsoleti e vulnerabili, con il 19,6%. Seguono con il 10,8% il progetto non sicuro del software e con il 10.4% la cattiva configurazione della sicurezza digitale nei web, cui seguono, al di sotto del 10%, le altre principali vulnerabilità indicate da OWASP. Per l'11,2% dei rispondenti nessuna delle 10 vulnerabilità considerate è la causa dell'attacco più grave subito in ambito web. Un esempio di questo tipo è un attacco DoS/DDoS, in cui l'oggetto dell'attacco, un sito o un'applicazione web, non ha vulnerabilità interne, e subisce la saturazione delle connessioni ad Internet non essendo stati attivati opportuni strumenti di rete per dirottare il traffico malevolo di saturazione.
Gli impatti dell'attacco più grave agli ambiti web sono suddivisi tra impatti tecnici, in termini di durata del disservizio, ed impatti economici, come ulteriori costi sul budget del sistema informativo ed il loro più o meno forte ripercuotersi sul bilancio complessivo dell'azienda/ente rispondente. **L'impatto tecnico** è stato **alto e significativo** per il **73,6%** delle aziende/enti rispondenti, con un disservizio durato più di 2 giorni, in ambito informatico un tempo veramente lungo. Una così alta percentuale è ancor più preoccupante in quanto emerge da aziende ed enti mediamente con misure di sicurezza digitali di alto livello e allo stato dell'arte, come più avanti approfondito. L'impatto economico ha visto un significativo aumento dei costi a livello di budget del sistema informativo (utilizzo di nuovi strumenti e servizi di sicurezza, formazione utenti e specialisti, consulenze tecniche e legali, comunicazioni coi media, etc.). **L'impatto economico** è stato **elevato e significativo** per il **24%** delle aziende/enti rispondenti, i cui ulteriori costi tecnici si sono ripercossi fortemente sul bilancio dell'intera azienda/ente. Queste alte percentuali confermano la pericolosità e la criticità crescente degli attacchi digitali subiti.
Le probabili **motivazioni per l'attacco più grave** vedono al primo posto tra i rispondenti la **frode** (25%), cui segue il **sabotaggio** (23,1%) ed il **ricatto** (22,7%). Seguono la **guerra digitale** (11,5%) e l'**hacktivism** (10,8%), pur con le difficoltà di distinguere questi attacchi da quelli della "tradizionale" criminalità informatica. Le motivazioni nel loro insieme, come negli anni precedenti, sono in gran parte di tipo economico.
I probabili **attaccanti per l'attacco più grave** vedono al primo posto, **32,7%**, attori "esterni" all'azienda/ente colpita, coi quali sovente collaborano utenti interni, volontariamente o involontariamente: ad esempio l'apertura di email di phishing, l'accesso a siti malevoli, il fornire il proprio account ad un collega o a un interlocutore.

Il drammatico incremento di attacchi digitali rilevato dai rispondenti a OAD 2023 è confermato dai dati forniti dalla Polizia Postale e delle Comunicazioni. Per le sole infrastrutture critiche italiane, lo specifico gruppo della Polizia Postale C.N.A.I.P.I.C. ha rilevato un moltiplicarsi degli attacchi rispetto agli anni precedenti, come evidenziato dalla fig. 1-2 (n.d., non disponibile: il dato non è stato fornito). La Polizia Postale evidenzia forti incrementi anche nelle frodi informatiche, nelle truffe online e nella prevenzione del cyberterrorismo, come dettagliato nel Capitolo 8.

Protezione strutture critiche	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	13.099	282	509	1181	459	1.032	844
Alert diramati	113.420	24.824	83.416	82.484	80.777	31.524	6.721
Indagini avviate	110	34	103	155	74	72	70
Persone arrestate	n.d	n.d.	n.d.	3	1	3	3
Persone denunciate/indagate	334	n.d.	105	117	14	1.316	1.226
Perquisizioni	n.d.	n.d.	n.d.	n.d.	n.d.	73	58
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	77	17	69	79	108	83	85

Fig. 1-2 (Fonte: elaborazione OAD su dati Polizia Postale)

Per meglio comprendere il fenomeno degli attacchi digitali, OAD analizza a grandi linee il tipo ed il ruolo del sistema informativo, e quali sono le misure di sicurezza digitali che ha implementato.
Il ruolo del sistema informativo per supportare le attività ed i processi dell'impresa pubblica o privata è essenziale per i 2/3 delle aziende/enti rispondenti e per questo motivo la sua sicurezza digitale deve essere di alto livello, efficace ed efficiente.
Il **53,8%** dei sistemi informativi considerati nell'indagine è di piccole-medie dimensioni, non ha un Data Center, ed è gestito in Italia: le caratteristiche tipiche per una piccola o media organizzazione, le più diffuse in Italia. Il **42,6%** è di grandi dimensioni, con uno più Data Center, in Italia e/o in altri paesi. Sul totale dei sistemi informativi dei rispondenti, l'86,2% sono controllati e gestiti in Italia. Il 95% utilizza servizi ICT terziarizzati, soprattutto in cloud, indipendentemente dalle dimensioni dell'azienda/ente: anche le piccole organizzazioni ora utilizzano largamente servizi in cloud, mentre nelle precedenti edizioni OAD il loro numero era molto inferiore. Il 13,1% dei sistemi informativi fornisce servizi essenziali per l'Italia, soggetti quindi al NIS e nel prossimo futuro alle nuove normative europee NIS2, DORA, etc. Considerando i settori merceologici delle aziende/enti rispondenti, per OAD tale percentuale è probabilmente più bassa di quello che avrebbe dovuto essere, forse perché chi ha compilato il questionario non conosceva le nuove direttive.
Nel questionario OAD 2023, le domande sulle misure tecniche ed organizzative presenti nei sistemi informativi erano lasciate opzionali: ad esse ha risposto il **42,2%** delle/dei rispondenti, con prevalenza percentuale delle aziende del settore ICT, inclusi i provider di servizi in cloud. Le PAC, Pubbliche Amministrazioni Centrali, è l'unico settore i cui rispondenti non hanno compilato le misure tecniche.
Gli aspetti organizzativi della sicurezza digitale sono determinanti per la sua attuazione e gestione effettiva ed efficace, dato che le maggiori vulnerabilità, e le più difficili da eliminare o ridurre, sono proprio quelle delle persone utenti dei sistemi informativi e delle organizzazioni nelle quali operano.
Le misure organizzative per la sicurezza digitale, storicamente carenti e trascurate rispetto a quelle tecniche, sono migliorate, confrontandole come trend con quelle degli anni scorsi. Una unità organizzativa per la sicurezza digitale è presente nel **74,1%** delle aziende/enti, il cui responsabile è il CISO, Chief Information Security Officer: nel 52,4% dei casi all'interno dell'UOSI, Unità Organizzativa Sistemi Informativi, rispondendo quindi al CIO, Chief Information Officer; negli altri casi è in altre strutture organizzative, un ulteriore indicatore del buon livello di sicurezza digitale in atto nel bacino dei rispondenti, che rispettano il principio della separazione delle responsabilità, evitando che il controllato per la sicurezza digitale, il CIO, controlli il controllore, il CISO. L'**88,2%** ha definito e segue policy e procedure organizzative per la sicurezza digitale, e di questi il 57,6% le ha definite solo per taluni processi/funzioni della sicurezza; quasi 1/3 ha stipulato una polizza assicurativa sui rischi digitali. Il **90,8%** delle aziende/enti rispondenti effettua l'analisi dei rischi ICT, il **71,8%** effettua auditing sulla sicurezza digitale, il **45,3%** ha definito un ERT, Emergency Response Team.
Le misure e gli strumenti tecnici di sicurezza digitale operanti sui sistemi informativi delle aziende/enti sono raccolte ed analizzate da OAD 2023 con un certo dettaglio, pur rimanendo a livelli generali, e per le varie analisi elaborate si rimanda al Capitolo 7. In sintesi sulle misure tecniche emerge quanto segue, ed occorre tener conto che le percentuali indicate fanno riferimento alle sole aziende/enti che hanno risposto alle domande del questionario sulle misure di sicurezza:

- Una specifica architettura per la sicurezza digitale basata su standard e best practice mondiali (NIST, ISO, ANSI/TIA 942, etc.) è definita ed implementata nel **68,5%** dei sistemi informativi delle aziende/enti rispondenti, ma di questi il 37% solo per le sue parti più critiche;

- le misure di sicurezza fisica e perimetrale di base sono presenti nella maggior parte dei sistemi informativi dei rispondenti, anche di quelli non dotati di Data Center; alcune carenze, ad esempio per UPS e sistemi di allarme, per i sistemi informativi molto piccoli, tipici nelle piccole e piccolissime organizzazioni;
- il **50%** dei sistemi informativi con almeno un Data Center sono a livello Tier III TIA, ed il **23%** è a livello IV, il più alto; quindi con elevati livelli di sicurezza digitale;
- per il controllo degli accessi al sistema informativo, le misure di IAA, Identificazione, Autenticazione, Autorizzazione, il **74,4%** dei rispondenti obbliga gli utenti privilegiati ad usare tecniche di autenticazione forte o quasi forte, e per gli utenti finali il **61,1%** consente l'utilizzo di diverse tipologie di autenticazione e autorizzazione a seconda del tipo di applicativo e del ruolo dell'utente;
- la gestione delle password è centralizzata per il **53,3%** dei sistemi informativi;
- il **77,8%** dei sistemi informativi ha tutte o almeno le più critiche connessioni ad Internet duplicate/ ennuplicate;
- per la sicurezza delle reti locali e geografiche, **66,7%,** dei sistemi informativi controlla centralmente funzionalità, prestazioni e livelli di sicurezza digitale delle reti, usando strumenti specifici quali DMZ, Firewall, DMZ, IPS/IDS, ed il 25,7% utilizza servizi in cloud, tipo SASE, per aumentare il livello di sicurezza delle reti;
- la protezione del software e degli applicativi dei sistemi informativi è prevalente attuata per gli applicativi più critici; il **43,8%** dichiara che i software ad hoc sono stati progettati e sviluppati in maniera sicura; il **73%** di tutto il software viene verificato/testato prima della sua messa in produzione; il **91%** effettua la manutenzione correttiva degli applicativi, e di questi il 36% solo per quelli più importanti/critici;
- diverse e complementari le misure per la protezione dei dati: per il **84,6%** dei rispondenti i dati sono classificati, i dati personali "sensibili" sono archiviati criptati per il **28,7**% e quelli riservati (non personali) sono criptati per il **41,4%**; **backup** affidabili e a regola d'arte sono effettuati nel **44,8%** dei sistemi informativi, e le relative procedure di ripristino da backup esistono e sono seriamente seguite nell' **81,4%** dei casi;
- il controllo, monitoraggio e gestione della sicurezza digitale è attuato, pur in diverse modalità e con diversi livelli di servizio, nell' **81,2%** dei sistemi informativi e di questi il **36,5%** la effettua centralmente, integrata con quella dell'intero sistema informativo;
- il **57,6%** delle aziende/enti rispondenti non dispone di certificazioni aziendali per la sicurezza digitale, ma il 17,6% dichiara di volerne acquisire una a breve;
- il **58,8%** delle aziende/enti rispondenti ha un Piano di Disaster Recovery, e di queste il 90% ha previsto, in diverse modalità, risorse ICT alternative da usarsi in caso di disastro: un significativo miglioramento rispetto a quanto rilevato da OAD negli anni precedenti, ed attuato non solo da grandi organizzazioni, ma anche da quelle piccole e molto piccole, per queste ultime grazie anche alla più facile disponibilità di risorse informatiche attivabili in cloud.

Il bacino di aziende/enti rispondenti emerso dall'indagine copre tutti i settori merceologici, incluse le Pubbliche Amministrazioni, anche se quasi ¼, il 24%, appartiene al settore ICT. In termini di dimensioni, come numero di dipendenti, delle Aziende/Enti rispondenti, il bacino emerso nell'indagine OAD 2023 è ben bilanciato tra quelle al di sotto dei 250 dipendenti e quelle più grandi: il **67%** dei rispondenti, più dei 2/3, appartiene a strutture con un organico inferiore ai 250 dipendenti, e di queste il **21,6%** sotto i 10, più di 1/5.

In estrema sintesi l'indagine OAD 2023 di AIPSI ha riscontrato nel 2022 un **fortissimo aumento degli attacchi digitali intenzionali**, subiti e rilevati dall'**85,1%** di aziende/enti rispondenti di ogni settore merceologico e di ogni dimensione, come numero di dipendenti: la più alta percentuale emersa da sedici anni consecutivi di indagini annuali OAD. Gli **impatti** di tali attacchi, ed in particolare di quelli agli ambienti web (che costituiscono l'approfondimento verticale di OAD 2023) sono stati **forti e significativi**, sia a livello tecnico sia a livello economico: e questo nonostante che i sistemi informativi dei rispondenti si posizionino in media **nella fascia alta del livello di sicurezza digitale**, in termini di misure tecniche ed organizzative implementate.

1bis. Executive Summary

With the present 2023 edition, the Observatory of Digital Attacks in Italy, OAD (Osservatorio Attacchi Digitali in Italia), reaches the sixteenth year of consecutive surveys into intentional digital attacks and security measures of IT systems in Italy, making use, as in previous years, of the precious collaboration of the Italian Postal and Telecommunications Police, which provided data and text of Chapter 8 of this Report.
OAD is the only independent survey in Italy, online via web, into intentional digital attacks on the IT systems of companies and public bodies operating in Italy. OAD does not predefine a specific pool of respondents, the same over the years, but allows anyone interested and involved in the management of an IT system full and free access to the online questionnaire, in a totally anonymous manner. Given the number of responses collected and their distribution among companies and public bodies of various sizes and belonging to different product sectors, the OAD survey produces, year by year, a clear photography of the phenomenon of the digital attacks in Italy and also of the security measures and tools in place in the IT systems of Italian public and private companies. OAD is able to involve in the survey also small and very small organizations, which constitute the vast majority in Italy (99.91% of private companies are SMEs, around 95% are those with less than 10 employees; quite similar the situation for the public bodies), which other national and international investigations are difficult to consider and analyze.

The 2023 OAD survey refers to the **entire year 2022**, when the tail end of the Covid-19 pandemic was still continuing, and the Russian Federation's invasion of Ukraine was in full swing. These two events have caused, in addition to "traditional" cybercrime, a strong increase in digital attacks also in Italy: 85.1% of the responding companies/institutions have detected intentional digital attacks on their information systems, a strong increase, as trend, compared to what was detected by OAD in previous years, and as highlighted in the figure below (fig. 1bis-1)

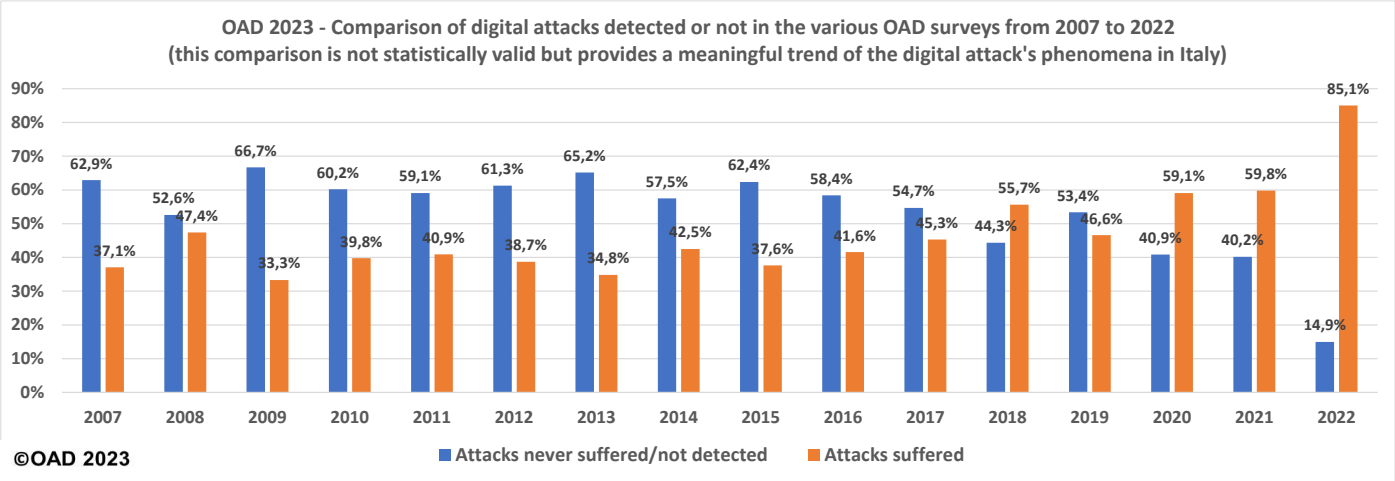


Fig. 1bis-1

This dramatic increase in digital attacks detected by OAD 2023 respondents is confirmed by the data provided by the Italian Postal and Communications Police: not only for Italian critical infrastructures, but also for computer scams and online fraud the numbers recorded have a factor of at least x 10 compared to those of previous years, as detailed in Chapter 8 of this Report.
The correlation of the data on the attacks detected with the size and turnover of the responding public/private companies shows for 2022 that the greatest number of digital attacks, and the most sophisticated, are aimed at organizations of large size and turnover. Small and very small organizations do not represent a target of specific interest

for cyber criminals, especially for targeted attacks, while they can be involved in mass attacks, such as those based on phishing and ransomware.

OAD distinguishes between what is attacked (referred as attack type) and how it is attacked, i.e. which attack techniques are used: OAD considers 14 different types of digital attacks, and 7 different families of attack's techniques. Of the considered types of attacks, the most widespread among the respondents are malicious/unauthorized modifications to the programs and configurations of the IT systems, with a value close to 30%, also caused in Italy by the widespread diffusion of malware and ransomware. This is followed by attacks on access control systems with 23.5%, DoS/DDoS attacks with 19.6%, and attacks on networks with 18.5%. All other attack types have decreasing percentages. As attack techniques, the most widespread among respondents are the mixed use of various techniques, with 35.4%, and the social engineering, which constitute a typical entry point into the target IT system for the majority of the modern digital attacks.

The 2023 OAD survey focuses on web attacks, i.e on web sites, web applications and web platforms. Nowadays, most applications are web-based, and many of these are in cloud: a modern IT system is partly on premise and partly outsourced, often on one or more clouds from different suppliers (multi cloud). From the pool of the respondents, it emerges that 73.1% of their IT systems, almost 3/4 of the total, suffered in 2022 this type of attacks, and of these 54.3% for their outsourced web environments. The most exploited vulnerabilities for these attacks were, for 55.8% of respondents, technical vulnerabilities (of the web application, of the web platform, of the user device) and for 25.8% user vulnerabilities, both final users and above all privileged ones (system administrators, systems engineers, ICT suppliers, etc.).

With reference to the 10 most widespread web vulnerabilities highlighted by OWASP in 2022, those identified in the most serious attacks detected by the respondents are, at the top of the percentage diffusion ranking, the vulnerable and outdated components with 19 ,6%. This is followed with 10.8% by the insecure software design and with 10.4% by the security misconfiguration. For 11.2% of respondents, none of the top 10 OWASP vulnerabilities are the cause of their most serious web attack. An example of this type is a DoS/DDoS attack, in which the object of the web attack has no internal vulnerabilities, and suffers the saturation of Internet connections due to the fact that the appropriate network tools have not been activated to route the malicious saturation traffic.

The impacts of the most serious web attack are divided between technical impacts, in terms of duration of the outage, and economic impacts, such as costs at the IT budget level and their possible repercussions on the overall company balance sheet. The technical impact was high and significant for 73.6% of the responding companies, with a block of ICT systems lasting more than 2 days, a truly long time in the ICT sector. Such a high percentage is even more worrying as it emerges from the respondent companies which have, on average, a very good level of digital security measures. The economic impact has seen a significant increase in costs at the budget level of the IT system (use of new security tools and services, user and specialist training, technical and legal consultancy, communications with the media, etc.). The economic impact was high and significant for 24% of the responding companies, whose technical costs had a strong impact on their balance sheet. These high percentages confirm the high danger and criticality of thr 2022 digital attacks in Italy.
Among the respondents, the probable reasons for the most serious attack are fraud (25%), followed by sabotage (23.1%) and blackmail (22.7%). This is followed by digital warfare (11.5%) and hacktivism (10.8%), although there are difficulties in distinguishing these attacks from those of "traditional" cybercrime. The reasons of a digital attacks are mainly and largely economic, as detected in previous OAD surveys.
The provable attackers for the most serious attack see in first place, 32.7%, actors "external" to the affected company, with whom internal users often collaborate, voluntarily or involuntarily: typical examples are the opening of email phishing, accessing malicious sites, providing your account to a colleague or interlocutor.

To better understand the phenomenon of digital attacks, OAD broadly analyzes the type and role of the IT system of the respondents, and what digital security measures it has implemented.

The role of the IT system in supporting activities and processes of the company is essential for 2/3 of the respondents. 53.8% of the IT systems considered in this survey are small-medium sized, do not have a Data Center, and are managed in Italy: the typical characteristics for a small or medium organization, the most widespread in Italy. 42.6% are large, with one or more Data Centers, in Italy and/or other countries. Of the total IT systems of the respondents, 86.2% are controlled and managed in Italy. 95% use outsourced ICT services, especially in the cloud, regardless of the their size, in terms of number of employees: even small organizations now widely use cloud services, while in previous OAD editions this was not the case. 13.1% of IT systems provide essential services for Italy, and therefore subject to the NIS and in the near future to the new European regulations such as NIS2, DORA, etc.

In the 2023 OAD questionnaire, the questions on the technical and organizational measures for cyber security were left optional: 42.2% of respondents answered them, with a prevalence of companies in the ICT sector, including cloud service providers.
The organizational aspects of digital security are crucial for its effective and effective implementation and management, given that the greatest vulnerabilities, and the most difficult to eliminate or reduce, are the users of IT systems.
Organizational measures for digital security, historically lacking and neglected, especially in SMEs, have improved, comparing them as trends with those of previous years. An organizational structure for digital security is present in 74.1% of the respondent companies, whose manager is the CISO, Chief Information Security Officer: in 52.4% of cases within the UOSI, Information Systems Organizational Unit, therefore reporting to the CIO, Chief Information Officer; in other cases the CISO is in other organizational structures, a further indicator of the good level of digital security in place in the pool of respondents, which respect the principle of separation of duties. 88.2% have defined and follow organizational policies and procedures for digital security, and of these 57.6% have defined them only for certain security processes/functions of their company; almost 1/3 have taken out a digital risk insurance policy. 90.8% of the responding companies carry out ICT risk analysis, and 71.8% digital security auditing. 45.3% have defined an ERT, Emergency Response Team.
In summary on the technical measures active in the respondents' IT systems, the following emerges, and it must be taken into account that the percentages indicated refer only to to those who answered the optional questions on security measures:

- a specific cyber security architecture, based on international standards and best practices (NIST, ISO, ANSI/TIA 942, CSA, etc.) is defined and implemented in 68.5% of the IT systems, but of these the 37% only for its most critical parts;
- physical security measures are present in most of the respondents' IT systems, even those without a Data Center; some shortcomings, for example for UPS and perimeter alarm systems, for very small IT systems;
- 50% of IT systems with at least one Data Center are at Tier III TIA level, and 23% are at level IV, the highest;
- for access control to the IT systems (IAA, Identification, Authentication, Authorization measures), 74.4% of respondents oblige privileged users to use strong or quasi-strong authentication techniques, and for end users 61.1% allows the use of different types of IAA, depending on the type of application and on the user's role;
- password management is centralized for 53.3% of IT systems;
- 77.8% of IT systems have all or at least the most critical Internet connections duplicated/multiplied;
- for the networks' security, 66.7% of IT systems centrally controls the digital security of their networks, using specific tools such as DMZ, Firewall, DMZ, IPS/IDS, and 25.7 % uses cloud services, such as SASE, to increase the level of network security;
- the software and applications' protection is mainly in operation for the most critical applications; 43.8% declare that ad hoc software has been designed and developed in a secure manner; 73% of all software is verified/tested before being put into production; 91% carry out corrective maintenance of the applications, and of these 36% only for the most important/critical ones;
- many and complementary measures for data protection: for 84.6% of respondents the data are classified, "sensitive" personal data are encrypted for 28.7% and confidential data (but non-personal) are encrypted for

41.4%; reliable and professional backups are carried out in 44.8% of the IT systems, and the related backup recovery procedures exist and are seriously followed in 81.4% of cases;

- the control and management of digital security are in operation, albeit in different ways and with different service levels, in 81.2% of IT systems and of these 36.5% carry it out centrally, integrated with that controlling the entire IT system;
- 57.6% of the responding companies do not have corporate certifications for digital security, but 17.6% declare they intend to acquire one soon;
- 58.8% of the responding companies have a Disaster Recovery Plan, and of these 90% have provided, in various ways, alternative ICT resources to be used in the event of a disaster: a significant improvement compared to what was found by OAD in previous years, and implemented not only by large organizations, but also by small and very small ones, for the latter thanks also to the easier availability of IT resources that can be activated in the cloud.

The pool emerged from the survey covers all product sectors, including Public Administrations, although the relative majority, 24%, belongs to the ICT sector. In terms of number of employees, the pool is well balanced between those with less than 250 employees and the larger ones: 67% of the respondents, more than 2/ 3, belongs to structures with a workforce of less than 250 employees, and of these 21.6% are under 10, more than 1/5.

In a nutshell, the AIPSI OAD 2023 survey found a very strong increase in intentional digital attacks in 2022, suffered and detected by 85.1% of responding public/private companies in every product sector and of every size: the highest percentage emerging from sixteen consecutive years of OAD annual surveys. The impacts of these attacks, and in particular those on web environments (which constitute the vertical OAD 2023 in-depth analysis) were strong and significant, both on a technical and economic level: and this despite the fact that the IT systems of the respondents were, on average, in the high range of the digital security level.

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 informatici di aziende ed enti operanti in Italia, e sulle misure di sicurezza tecniche ed organizzative 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 dei rispondenti, 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 (per approfondimenti si veda §3.5) e che difficilmente sono considerate nelle altre indagini nazionali ed internazionali.
Obiettivo primario di OAD è 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.
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 annuale vuole e deve 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 e basato sui dati raccolti della sicurezza digitale in Italia in termini di misure tecniche ed organizzative, di leggi e normative sia italiane che europee, di strumenti, di attacchi e dei loro impatti e conseguenze.
Per la sua importanza in termini di comunicazione, sensibilizzazione e formazione sulla cybersecurity, il progetto **OAD** fa parte dell'iniziativa strategica nazionale **Repubblica Digitale**[1], come evidenziato in https://repubblicadigitale.innovazione.gov.it/it/i-progetti/.

L'approccio seguito per tutte le indagini OAD è di coinvolgere liberamente e in maniera rigorosamente anonima il maggior numero di possibili rispondenti al questionario online, di aziende ed enti di ogni settore merceologico e di ogni dimensione, divulgando l'indirizzo (URL) del questionario tramite tutti i canali mediatici di AIPSI, oltre che con l'aiuto delle associazioni patrocinanti. Questo approccio non definisce quindi un preciso campione di riferimento, ma al termine della fase di disponibilità online del questionario, fa emergere un insieme non omogeneo di rispondenti di diversi settori merceologici, Pubbliche Amministrazioni incluse, e con organizzazioni di diverse dimensioni come numero di dipendenti, dalle più piccole, con meno di 10 dipendenti, alle più grandi con più di 5.000..

OAD 2023 arriva al **16° anno** consecutivo di indagini online via web, e si è focalizzato sugli **attacchi subiti nel 2022** verticalmente per i **siti e gli ambienti web** dei sistemi informativi delle aziende/enti rispondenti ma ha posto nel questionario due domande sulle altre tipologie di attacco rilevate nel 2022, per poter continuare l'analisi dei trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 al 2022. Nell'ottica di semplificare il questionario in modo da ridurre il tempo necessario a compilarlo, pur mantenendo significativi i contenuti per l'analisi del fenomeno attacchi digitali e garantire una continuità con le principali informazioni raccolte nelle precedenti indagini, è stata anche resa opzionale la parte sulle misure di sicurezza in essere, ma raccomandata per poter ottenere, al completamento del questionario, l'automatica ed anonima macro valutazione del livello di sicurezza del sistema informativo oggetto delle risposte.
Nel questionario online, la parte di domande sugli attacchi subiti nel 2022, sia generali che verticali sugli ambienti e le applicazioni web, era obbligatoria: per chi non avesse rilevato attacchi, le domande relative venivano automaticamente saltate. Erano obbligatorie anche le domande inerenti la tipologia di azienda/ente a cui appartiene il sistema

[1] Iniziativa strategica nazionale promossa dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri nel quadro della strategia "Italia 2025": ha l'obiettivo di combattere il divario digitale di carattere culturale presente nella popolazione italiana, per sostenere la massima inclusione digitale e favorire l'educazione sulle tecnologie del futuro, accompagnando il processo di trasformazione digitale del Paese (si veda: https://repubblicadigitale.innovazione.gov.it/it/il-programma/)

informativo oggetto delle risposte, i futuri attacchi più temuti, il ruolo del compilatore del questionario. Il completamento dell'intero questionario, inclusa la parte opzionale sulle misure di sicurezza in essere, forniva in automatico una macro valutazione qualitativa del livello di sicurezza che emergeva dalle risposte fornite. Per approfondimenti sugli aspetti metodologici dell'indagine OAD 2023 si rimanda all'**Allegato A** di questo rapporto.

L'arco temporale di riferimento di OAD 2023 è **l'intero anno 2022** durante il quale un elemento dominante e caratterizzante gli aspetti di sicurezza digitale è stata la **guerra in Ucraina** causata dall'invasione della Federazione Russia. Si è poi avuta una coda della **pandemia Covid 19**, che ha continuato ad avere effetti, sia in termini medici-sanitari, sia in termini di attacchi digitali, pur se di impatto minore rispetto agli anni precedenti.
A questi due fattori si aggiungono quelli che si possono considerare "tradizionali" attacchi digitali per compiere prevalentemente frodi di vario genere, dai furti sui conti corretti (frodi finanziarie) ai ricatti con ransomware, dalla saturazione delle risorse dei sistemi informativi (DoS/DDoS) ai furti di informazioni e di dispositivi ICT (in particolare gli smartphone).

Il questionario OAD 2023 è rimasto online da fine gennaio 2023 a fine agosto 2023: i rispondenti sono stati complessivamente **326**, un numero superiore a quello della precedente edizione, ma dello stesso ordine di grandezza delle indagini OAD degli anni precedenti: questo nonostante la forte semplificazione del questionario, il forte sforzo di AIPSI per promuovere il questionario online, anche con il coinvolgimento delle associazioni patrocinanti, elencate nell'**Allegato D** di questo rapporto.

La fig. 2-1 mostra le copertine dei Rapporti finali 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 - reti (come anche indicato dall'acronimo ICT[2] usato in Europa e sovente usato anche nei Rapporti OAD), dato che gli attacchi digitali possono colpire sia la parte di rete sia la parte informatica, o entrambe, di un sistema informativo.

Fig. 2-1

2 ICT, Information and Communication Technology.

Come per le edizioni precedenti OAD 2023 annovera il patrocinio 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 significativo per poter allargare e stimolare il bacino dei compilatori del questionario via web, tipicamente tramite i loro soci e simpatizzanti, oltre che per far conoscere e divulgare il rapporto finale.

Il presente Rapporto OAD 2023 , 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, ma non è e non può essere un libro sulla sicurezza digitale. Specifici concetti, 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 la comprensione del presente rapporto si richiede pertanto 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 nell'ambito della sicurezza digitale.

3. Il quadro generale degli attacchi digitali intenzionali

L'indagine OAD fa riferimento al solo contesto italiano nel 2022, ma per comprendere meglio il fenomeno degli attacchi digitali è importante inquadrare tale contesto in quello più generale a livello europeo e mondiale. Gli attacchi digitali nel 2022 a livello mondiale

Innumerevoli le indagini nel 2022 sui rischi e sugli attacchi digitali livello mondiale, prevalentemente condotte da fornitori ICT e di sicurezza digitale, sovente su specifici settori merceologici, quali enti pubblici, sanità, banche, o su specifiche tipologie e/o tecniche di attacco, quali ad esempio malware e DDos/DoS.

Quanto emerge da tutte le indagini è una **forte crescita degli attacchi digitali e del rischio cibernetico nel 2022 rispetto agli anni precedenti**: forte crescita che è avvenuta **anche in Italia** ed è stata **riscontrata nelle risposte ad OAD 2023**, come riportato in §4, e nei dati forniti dalla Polizia Postale e delle Comunicazioni in §8.

A livello mondiale Il Global Risk Report[3] del World Economic Forum, WEF, nella sua ultima versione evidenzia come il diffondersi e la crescita del cybercrime e dell'insicurezza dell'ICT siano tra i primi dieci rischi "globali" a livello mondiale, sia a breve che a lungo termine, come evidenziato nella fig. 3-1.

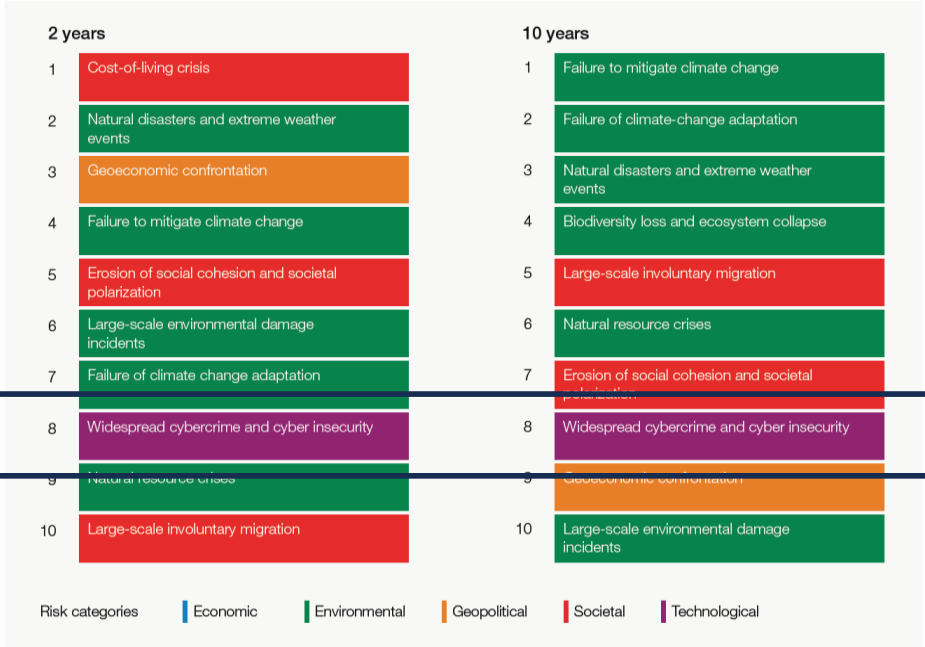


Fig. 3-1 (Fonte: WEF)

Dallo stesso rapporto WEF, la fig. 3-2 mostra il grado di severità, anche nel lungo termine, dei vari rischi globali considerati. Quelli digitali, evidenziati dal colore viola, includono:

- **Adverse outcomes of frontier technologies (risultati negativi dalla frontiera ICT): conseguenze negative, intenzionali o involontarie, dei progressi tecnologici su individui, imprese, ecosistemi e/o economie. Include, ma non è limitato a: intelligenza artificiale, interfacce cervello-computer, biotecnologia, geoingegneria, informatica quantistica e metaverso.**
- **Breakdown of critical information infrastructure** (guasto/caduta di un'infrastruttura ICT che supporta informazioni critiche): deterioramento, sovraccarico o arresto di infrastrutture o servizi fisici e digitali critici

[3] https://www.weforum.org/reports/global-risks-report-2023/

che comportano il guasto di Internet, dei dispositivi cellulari, dei servizi pubblici o dei satelliti. Derivante da, ma non limitato ad, attacchi informatici, danni fisici intenzionali o non, tempeste solari.

- **Digital inequality and lack of access to digital services** (disuguaglianza digitale e mancanza di accesso ai servizi digitali): accesso frammentato o ineguale alle reti e alle tecnologie digitali derivante da investimenti insufficienti e da un basso livello delle competenze digitali, potere d'acquisto insufficiente o restrizioni governative sulle tecnologie.
- **Digital power concentration** (concentrazione del potere digitale): concentrazione di risorse, capacità o conoscenze digitali critiche tra un numero limitato di individui, aziende o stati che possono controllare l'accesso alle tecnologie digitali e richiedere prezzi discrezionali. Derivante dal, ma non limitato al, fallimento della regolamentazione antitrust e dagli investimenti inadeguati all'eco sistema dell'innovazione o dal controllo statale sulle tecnologie chiave.
- **Widespread cybercrime and cyber insecurity** (criminalità informatica diffusa e cyber insicurezza): spionaggio informatico o crimini informatici sempre più sofisticati. Include, ma non è limitato, a: perdita di privacy, furto o frode di dati, spionaggio informatico.

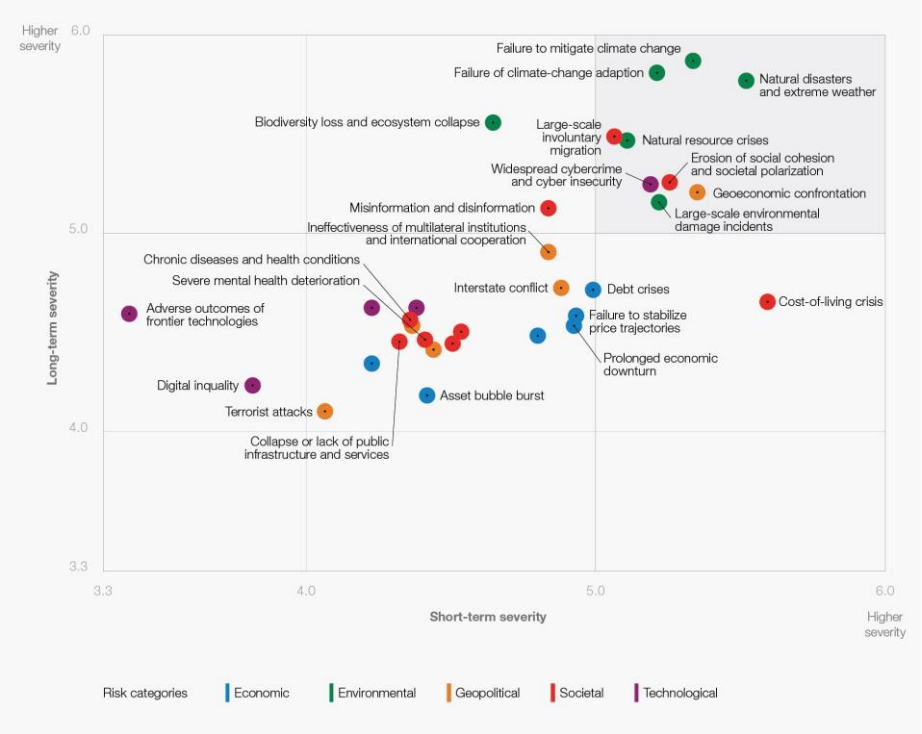


Fig. 3-2 (Fonte: WEF)

La fig. 3-3 evidenzia le correlazioni tra i sopra elencati rischi globali inerenti la sicurezza digitale e gli altri rischi globali considerati dal WEF. Si noti come il diffondersi del cybercrime e la conseguente **crescita dell'insicurezza digitale** sia strettamente correlata da un lato agli altri rischi cyber, dall'altro alla disinformazione, agli attacchi terroristici e ai conflitti tra Stati. E questi tre rischi globali sono elementi chiave delle guerre informatiche ed ibride[4].

[4] 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).

Si deve poi considerare che è difficile individuare e classificare un attacco digitale come una azione di cyber warfare, rispetto ad un "normale" attacco, all'azione di un terrorista, di un attivista (hacktivist), e così via: chi attacca il più delle volte non si dichiara, anzi cerca di mascherare il suo attacco, affiancandolo spesso con varie "fake news" fuorvianti. Un attacco digitale potrebbe far parte di una cyber warfare[5] quando ha un certo livello di sofisticazione, che richiede competenze e risorse che un "normale" hacker difficilmente potrebbe disporre, è chiaro l'obiettivo target dell'attacco ed il momento ed il contesto in cui l'attacco viene portato. La guerra digitale, o cyber warfare, introduce lo **spazio "cyber"**, che si affianca a quelli di terra, mare, cielo e spazio, e 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.
A livello europeo, per la sicurezza digitale, i suoi rischi, le minacce ed i principali attacchi occorsi nei paesi dell'UE sono molto importanti i vari rapporti pubblicati da ENISA, l'Agenzia europea per la cybersicurezza (https://www.enisa.europa.eu/), in particolare l'"*ENISA Threat Landscape (ETL) Report*" pubblicato nell'ottobre 2022 e l'"*Identifying emerging cyber security threats and challenges for 2030*", pubblicato a marzo 2023.

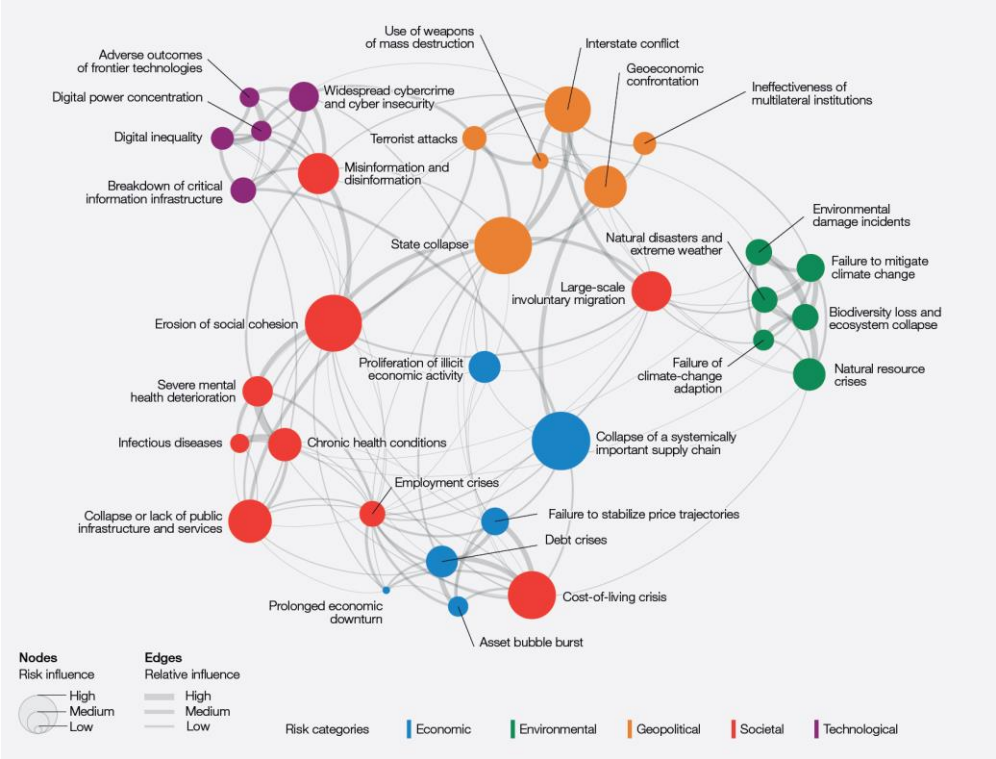


Fig. 3-3 (Fonte: WEF)

La fig. 3-4, da quest'ultimo ripresa, mostra le dieci vulnerabilità emergenti e più gravi nel prossimo futuro, entro il 2030. La mappa in figura evidenzia come molte delle minacce digitali previste a lungo termine sono già presenti oggigiorno: le minacce di oggi rimarranno nel futuro pressanti ma avranno cambiato carattere, avranno maggiori correlazioni e dipendenze, e la diffusione e lo sviluppo di nuove tecnologie aggiungeranno criticità maggiori e maggior complessità per contrastarle. Il rapporto inoltre dettaglia questi 10 rischi indicando i probabili attaccanti, le probabili tecniche di attacco, i probabili impatti, e gli scenari più rilevanti per attuarli, scenari illustrati nella fig. 3-5.

[5] 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*".

Fig. 3-4 (Fonte: Enisa)

SCENARIOS					
	Scenario 1	**Scenario 2**	**Scenario 3**	**Scenario 4**	**Scenario 5**
TRENDS	The increased usage of new technologies in remote maintenance	Diminishing availability of fresh water	The increasing difficulty for law enforcement to access data stored on (encrypted) networks and the use of collected data	Non-traditional work structures like freelancing are rising in popularity ("gig economy")	Increasing introduction of (technical) legislation in Europe
	The use of Distributed Ledger Technologies is growing	The increasing geopolitical influence of communication providers	There is an increasing number of devices that are not (or are unable to be) regularly patched	Increasing reliance on automation and connectivity of sustainable energy production	Satellite control infrastructure is increasingly critical
	Advancement of deep fake technology	The increased political power of non-state actors	Decision-making is increasingly based on automated analysis of data	There is increasing popularity of everything as a service (XaaS) demand and supply	AI-based systems are increasingly deployed with bias or issues that impact inclusivity, safety, ethics, privacy, trustworthiness, and explainability
	Collecting and analyzing data to assess user behavior is increasing, especially in the private sector	The increasing relevance of (cyber) security in elections	The public health issues arising from the mental health problems of victims of cybersecurity	Automation of agricultural skills and workforce	The rise of digital authoritarianism
	The increased and improved connectivity of illegal businesses	The rise of smart cities	The capacity to control data about oneself (individual, company, or state) is becoming more desirable and more technically difficult	Industrial switch from fossil fuels to hydrogen or electric (demand)	Mass extinction and loss of biodiversity continues

Fig. 3-5 (Fonte: Enisa)

Scenari ed evoluzione futura della sicurezza digitale che, secondo il citato rapporto di ENISA, devono considerare i trend PESTEL[6] al 2030. In particolare, per i primari trend tecnologici ENISA prevede:

- una crescente domanda e offerta di tutto come servizio (everything as a service, XaaS);
- la crescente criticità delle infrastrutture digitali per il controllo satellitare;
- crescenti problemi nell'implementazione ed utilizzo di sistemi basati sull'intelligenza artificiale, che influiscono sull'inclusività, sulla sicurezza, sull'etica, sulla privacy, sull'affidabilità;
- la diffusione della Realtà Estesa (Extended Reality, indicata con XR)[7];

[6] PESTEL è l'acronimo di Political, Economic, Social (or Socio-cultural), Technological, Environmental and Legal.

[7] La Realtà estesa, indicata con l'acronimo XR, è il termine che include le diverse tecnologie della realtà virtuale (VR), realtà aumentata (RA), realtà mista (MR) XR è una tecnologie immersiva che consente l'incontro e l'integrazione tra mondi fisico, reale, e quello virtuale. Secondo McKinsey, si veda https://www.mckinsey.com/spContent/bespoke/tech-trends/pdfs/mckinsey-tech-trends-outlook-2022-immersive-reality.pdf, l'utilizzo attuale e futuro di XR è crescente nel metaverso, e riguarda quattro macro aree: formazione e assessment; progettazione e sviluppo del prodotto; miglioramento della consapevolezza "situazionale"; casi d'uso B2C, ad esempio nei giochi, nel fitness, nella vendita al

- la crescente interconnessione ed interoperabilità dei veicoli tra loro e con il mondo esterno, e che dipendono sempre meno dall'intervento umano;
- la crescente diffusione dei Digital Twin (gemelli Digitali)[8].

3.1 I principali attacchi digitali a livello mondiale nel 2022

Attacchi digitali per frodi e "tradizionale" criminalità informatica, e in parallelo gli attacchi inerenti il Covid e la guerra in Ucraina hanno letteralmente fatto esplodere il fenomeno a livello mondiale.
Dati gli innumerevoli attacchi, è difficile, e comunque arbitrario, individuare tra le infinite fonti gli attacchi principali, intendendo per tali quelli che hanno avuto maggiori impatti, o hanno coinvolto un gran numero di vittime, o hanno introdotto innovative tecniche informatiche per essere attuati.
Per sintetizzare i principali attacchi a livello mondiale, OAD 2023 ha fatto soprattutto riferimento alla banca dati **Mitre-CVE**, Common Vulnerabilities and Exposures, che registra e classifica tutte le vulnerabilità tecniche individuate (https://cve.mitre.org/), al **FIRST**, Forum of Incident Response and Security Teams (https://www.first.org/), a vari rapporti di **ENISA**, alla statunitense **CISA**, Cybersecurity Infrastructure Security Agency (https://www.cisa.gov/), l'Agenzia statunitense per la sicurezza informatica e delle infrastrutture negli USA, al **CSIS**[9]**,** Center for Strategic and International Studies, centro indipendente di ricerca, alle segnalazioni ed ai rapporti dello **CSIRT Italia**, oltre che ad alcuni dei più autorevoli rapporti di enti ed industrie ICT e del settore sicurezza digitale.

Le minacce ed i rilevati attacchi più diffusi nel 2022 a livello mondiale includono **social engineering, ransomware, malware, cryptojacking, minacce legate alla posta elettronica, minacce ai dati, minacce alla disponibilità con saturazione di risorse o blocco/distruzione delle risorse ICT di Internet, attacchi alla supplychain, disinformazione e mala informazione (fake news), minacce non intenzionali**.

Le minacce non intenzionali (chiamate "non-malicious incidents"), riguardano incidenti involontari nella gestione operativa dei sistemi ICT, causati da errori degli operatori, dalla estrema urgenza e fretta negli interventi, dalla mancanza di specialisti esperti (ad esempio ammalati di Covid o per malattie non curate a causa Covid) sostituiti da personale non sufficientemente preparato, dalla difficoltà di cooperare efficacemente da remoto, e così via. Questi incidenti non intenzionali **non sono considerati nell'indagine OAD**, ma ENISA ha giustamente rilevato la loro cresciuta diffusione in tempi critici come quelli attuali, considerandoli nel 2022 una significativa minaccia da non trascurare.

Gran parte degli attacchi, soprattutto quelli effettuati dall'esterno dell'azienda/ente, **utilizzano il phishing e lo spear phishing** come **vettore iniziale dell'attacco**: queste email malevole contengono come allegati malware, e sovente ransomware, con file di di tipo ISO[10] e .LNK[11]; oppure consentono, in logica di social engineering, di acquisire l'account del destinatario della email, e con questo accedere illegalmente alle sue risorse ICT: in pratica è un tipo di **furto**

dettaglio (showroom virtuale). Il Metaverso rappresenta un 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).

[8] Digital Twin è la rappresentazione virtuale di un'entità fisica, vivente o non vivente, di una persona o di un sistema anche complesso connessa a una parte fisicae con la quale può scambiare dati e informazioni, sia in modalità sincrona (in tempo reale), che asincrona (in tempi successivi) (definizione di Wikipedia)

[9] CSIS è un'organizzazione di ricerca politica bipartisan e senza scopo di lucro, dedicata a promuovere idee pratiche per affrontare le più grandi sfide del mondo. Tra i vari argomenti di ricerca le tecnologie, la geopolitica, la sicurezza digitale, le minacce transnazionali, l'intelligence.

[10] Un file ISO, spesso chiamato anche "Immagine ISO", è un singolo file che rappresenta perfettamente il contenuto di un intero CD, DVD o Blu-ray disc. Individuato dal formato file ".ISO", è una tipologia di immagine disco composta da tutti i dati contenuti in ogni singolo settore del supporto di memoria ottico, inclusi i dati e i file relativi al file system del disco stesso.

[11] File .LNK: l'estensione .LNK è utilizzata dai sistemi operativi Windows come riferimento, tipicamente in locale, ad un file originale, di cui assumono tutte le caratteristiche. Windows utilizza .LNK come l'estensione del file per i collegamenti ai file locali, e .URL per collegamenti a file remoti. Nel phishing e spear phishing un file con estensione .LNK il più delle volte è un malware o ransomware.

dell'identità digitale e di **snoofing**. Molti degli attacchi, non solo di malware, sfruttano le **backdoor lasciate aperte** nei programmi in produzione, ossia operanti nel sistema informativo.
La maggior parte delle tecniche di attacco usate nel 2022 non sono nuove, ma alcune sono state rese più sofisticate e più efficaci. Alcune "vecchie" vulnerabilità e le relative tecniche di attacco, ritenute ormai non più utilizzabili, sono state riprese, sia per adattarle ai nuovi contesti, quali il cloud, sia perché alcuni sistemi informativi hanno dismesso gli strumenti di contrasto (o tali strumenti non sono più in grado di contrastarli).
La maggior parte degli attacchi digitali di una certa complessità, e quindi potenziale gravità dell'impatto, dopo la fase di "**primo ingresso**" al sistema target (il citato vettore iniziale), effettua dei "**movimenti laterali**" (lateral movement): è una tattica per spostarsi (di qui il termine "laterale") all'interno di una rete per cercare di accedere a varie risorse ICT per comprometterle, fino ad **arrivare al sistema obiettivo** (target), o comunque trovare risorse ICT più preziose e vulnerabili.

Le maggiori innovazioni ed evoluzioni delle minacce e dei conseguenti attacchi e delle loro tecniche, nel **2022** riguardano in particolare:

- crescita e diffusione di **malware distruttivi**, tipo i **wiper** realizzati da gruppi di cracker vicini alla Federazione Russa. Oltre a l'HermeticWiper e il WhisperGate, funzionalmente descritti nel Rapporto OAD 2021 cui si rimanda (scaricabile dopo il login da https://www.oadweb.it/it/rapporti-e-relativi-convegni/2021-22/per-scaricare-il-rapporto-oad-2021-aggiornamento-aprile-2022.html), sono apparsi altri malware, divenuti sempre più modulari e adattabili a diverse piattaforme e sistemi operativi: tipici esempi di wiper usciti nel 2022 includono IsaacWiper, Caddy Wiper, AWFULSHRED, SOLOSHRED, Azof, Acidrain, DoubleZero, DesertBlade. Alcuni wiper hanno come target i sistemi OT, Operation Technology, ad esempio Industroyer.V2. Sempre nel 2022 è apparso il primo wiper open source, Endurance;
    - Altri malware hanno poi continuato a circolare, quali Emotet, IcedID, Qakbot, Bumblebee, ed il nuovo Anchor. Alcune indagini hanno rilevato la crescita di **worm via USB**, ad esempio Raspberry Robin;
- evoluzione dei **ransomware**: crescente diffusione del Ransomware-as-a-Service (**RaaS**) e potenziamento di alcuni ransomware già esistenti. Ad esempio attacco agli hypervisor nei cloud, diffusione tramite il controllo dei domini e degli ambienti di gestioni.. Nel periodo considerato, secondo ENISA (si veda https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks) i ransomware che hanno causato più incidenti sono stati Conti e LockBit. Per approfondimenti in italiano su alcuni dei più diffusi ransomware si veda https://www.csirt.gov.it/pubblicazioni;
- evoluzione degli attacchi **Dos/DDoS**, che si rivolgono anche agli ambienti virtualizzati, a quelli IoT, alle reti mobili, estendendo ed amplificando così fortemente il loro campo d'azione;
- crescita attacchi digitali all'azienda/ente target partendo dai fornitori o dai clienti tramite la "supply chain" logistica ed informatica che consente l'interoperabilità tra i loro sistemi informativi (**supply-chain attack**);
- diffusione di **cryptojacking** (chiamato anche hidden cryptomining) al crescere dell'uso di criptovalute. Con tecniche di hijacking, ovvero dell'uomo in mezzo, vengono illegalmente estratte (mining) ed usate criptovalute dai computer di ignari possessori delle stesse. E' in pratica una frode finanziaria con le criptovalute, realizzata e realizzabile tramite tecniche di hijacking e con l'uso di malware (si veda §8);
- crescita e sofisticazione degli attacchi alla posta elettronica aziendale, la "**Business Email Compromise**", che include anche il phishing, lo spear phishing, lo spamming malevolo;
- crescente utilizzo di strumenti di **intelligenza artificiale** (AI, Artificial Intelligence) per individuare vulnerabilità e realizzare attacchi ulteriormente sofisticati, tipo **APT, Advanced Persistent Threat**, in grado di studiare e sfruttare in maniera multipla e contemporanea le possibili vulnerabilità presenti in un sistema ICT.

La crescita, la sofisticazione e la diffusione delle nuove tecniche d'attacco è facilitata dalla diffusione, anche a prezzi limitati, di **cyberattack as a service** e di hacker "a pagamento", indicati in lingua inglese "**hacker for hire**". Si diffondono Ransomware as a Service, DoS as a Service, Phishing as a Service, e così via, e non solo nel darkweb. Molti degli hacker for hire fanno parte di ben noti gruppi criminali di cracker, con un nome noto che li contraddistingue, come ad esempio

il Gruppo Conti ed il Gruppo Sandworm, o che lo cambiano per sfuggire alle ricerche delle polizie; altri sono hacker esperti che si offrono come freelance per diventare cracker e per guadagnare di più, anche se illegalmente.

Si diffonde inoltre ampiamente **disinformazione** e **mala-informazione** (fake news). Ben conosciuta in ambito sanitario e politico, ora è crescente anche in ambito ICT e della **sicurezza digitale**, sui relativi prodotti e servizi, sulle aziende che li forniscono oltre che sugli enti che se ne occupano in vario modo, a partire dalle Agenzie nazionali, quali CISA, ENISA, ACN, e così via.

3.1.1 Esempi di significativi di attacchi a livello mondiale nel 2022

Come già anticipato in §3.1, nel 2022 la guerra della Federazione Russa contro l'Ucraina è stato il principale fattore di attacchi digitali condotti da gruppi legati agli stati, ed in particolare quelli che fanno riferimento alla Federazione Russa: attacchi che possono essere chiaramente considerati nella guerra digitale, in corso da tempo e ben prima dell'invasione dell'Ucraina, contro paesi occidentali da parte di stati quali Federazione Russa, Cina, Corea del Nord, tutte nazioni comuniste, ed altri stati di base islamici, tra i quali spicca l'Iran. Nella logica della cyber warfare e della guerra ibrida, le vulnerabilità ICT si sono rapidamente trasformate in vere e proprie armi.
Le controparti occidentali a loro volta contrattaccano con il supporto o il diretto intervento di gruppi di hacker/cracker internazionali, tra i quali Anonymus, GhostSecurity, Cyber Partisans, probabilmente con il supporto di strutture governative cyber occidentali che non vogliono essere individuate.
A livello ucraino, le loro strutture cyber erano piuttosto deboli, e a fine febbraio 2022 l'Ucraina ha lanciato l'iniziativa "IT Army of Ukraine"[12] per contrattaccare a livello cibernetico la Federazione Russa. Il loro primo attacco noto è il DDoS del sito web Vesti95.ru, il giornale ufficiale del Ministero della Politica Nazionale, delle Relazioni Esterne, della Stampa e dell'Informazione della Repubblica Cecena. Un altro dei primi attacchi DDoS di IT Army, a marzo 2022, è stato contro il sistema di pagamenti del provider QIWI, diffuso in Russia e in altri stati del Common-wealth of Independent States (CIS), ed ai primi di maggio contro EGAIS, il sistema automatico di monitoraggio in Russia della produzione e della distribuzione di bevande alcoliche. EIGAS è di proprietà della Federazione Russa. L'elenco potrebbe continuare, varie fonti ritengono che IT Army of Ukraine abbia messo a segno nel 2022 più di 2000 attacchi.

Alcuni dei più significati attacchi digitali nel 2022, scelti come esempi, includono:

- **Gennaio 2022**
  - data breach a FlexBooker, società che fornisce online un sistema di schedulazione e prenotazioni, che ha coinvolto circa tre milioni d'utenti, con il furto dei loro account (ID e password) e delle loro licenze di guida, che sono stati poi messi in vendita;
  - nei primi mesi del 2022 l'ampio e ripetuto furto di codice software e di informazioni riservate da parte del gruppo Lapsus$ ad importanti aziende quali Nvidia, Samsung e Ubisoft; dati che sono stati poi pubblicati dietro ad apparenti tentativi di estorsione. Lapsus$ sembra inoltre che abbia violato e diffuso parti del codice sorgente di Microsoft Bing e di Cortana, e ha sicuramente violato l'accesso ad Okta, un provider di servizi di autenticazione;

- **Febbraio 2022**
  - attacco a Swissport, società di gestione dei servizio aeroportuali in Svizzera tramite il ransomware ALPHV (*aka BlackCat*) che ha causato l'interruzione dei servizi ed il ritardo di voli;

[12] IT Army è un "esercito cibernetico" costituito da hacker volontari ucraini e internazionali che lavorano in collaborazione con funzionari del Ministero della Difesa ucraino per prendere di mira le infrastrutture e i siti web russi. Per approfondimenti: https://www.cfr.org/cyber-operations/ukrainian-it-army e soprattutto https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf

- attacco al gruppo tedesco Marquard & Bahls , attivo nei servizi energetici (gas&oil) e della chimica, che ha portato al blocco di più di 200 stazioni di servizio in Germania; gli autori sono la gang russa BlackHat che in passato aveva già attaccato impianti e condutture gas&oil (pipeline);

- **Marzo 2022**
  - furto di cripto valute, equivalenti a più di 600 milioni di US$, da parte del gruppo Lazarus della Corea del Nord al Ronin Bridge di Axie Infinity. Quest'ultimo è un videogioco per guadagnare in cripto valute basato sulla blockchain di Ethereum e alla sua blockchain di supporto (sidechain[13]) Ronin di Sky Mavis che fornisce il suo Wallet (servizio di portafoglio per criptovalute); l'interoperabilità tra il gioco ed il wallet avviene tramite il Ronin Bridge;
  - attacco, probabilmente malware o ransomware, all'azienda giapponese Kojima Industries fornitrice di componenti plastici ed elettronici alla Toyota, che ha fatto sospendere a quest'ultima 28 linee di produzione in 14 stabilimenti in Giappone per paura di un conseguente attacco "supply chain";

- **Aprile 2022**
  - attacco ransomware dal gruppo Conti al Ministero delle Finanze del Costa Rica, che ha paralizzato le attività di import/export con perdite di decine di milioni di dollari al giorno;
  - attacco DDoS ad istituti pubblici e privati della Romania, quali il Ministero della Difesa, le ferrovie statali, la polizia, la banca privata OTP Bank da parte di cracker filo-russi;
  - attacco da gruppi filo russi alle facility energetiche ucraine;
  - rimozione da tutte le reti, a livello mondiale, da parte di enti statunitensi di un malware che avrebbe potuto svolgere diverse funzioni, da quelle di sorveglianza a quelle di struttive; la produzione di questo malware è attribuito ad organizzazioni filo russe;

- **Maggio 2022**
  - a maggio 2022 vari attacchi DDoS ad istituzioni italiane, dal Senato al Ministero della Difesa e all'Istituto Superiore di Sanità, da parte di persone o gruppi filo russi;
  - a maggio 2022 attacco, probabilmente da gruppi iraniani, ai sistemi di diffusione sonora municipali di Gerusalemme ed Eliat, attivando i sistemi di sirene antiaeree in entrambe le città;
  - violazione dei dati dei sistemi informativi del Shields Health Care Group, con sede nel Massachusetts, che ha colpito circa due milioni di persone negli Stati Uniti. I dati rubati includevano nomi, numeri di previdenza sociale, date di nascita, indirizzi e informazioni sulla fatturazione, oltre a informazioni mediche come diagnosi e i contenuti delle cartelle cliniche;

- **Giugno 2022**
  - a giugno 2022 violazione dei dati (data breach) di circa un milione e mezzo di utenti alla Flagstar Bank;
  - hacker hanno rubato e pubblicato file e foto noti come "The Xinjiang Police Files" che mostrano violazioni dei diritti umani commesse dal governo cinese contro la popolazione uigura;
  - attacco a tre aziende siderurgiche statali iraniane, costringendole a fermare la produzione;
  - attacco ai sistemi informativi di vari enti sanitari ed ospedalieri negli US, con furto di informazioni sensibili dei pazienti;

- **Luglio 2022**
  - attacco da parte del gruppo filorusso Killnet alla società statale di energie della Lituania;

[13] Una sidechain *è una* blockchain separata eseguita in modo indipendente da Ethereum ed è connessa alla Rete principale di Ethereum da un ponte bidirezionale, in questo caso il Ronin Bridge

- gruppi filo russi hanno violato una società di media ucraina per trasmettere su più stazioni radio che il presidente ucraino Zelenskyy era in condizioni critiche. Un esempio assai significativo di diffusione di false informazioni;
- attacco all'Organizzazione iraniana per la cultura e la comunicazione islamica (ICCO), con il blocco di almeno 6 siti web, la collocazione di immagini di leader della resistenza iraniana su altri quindici siti, l'accesso ai dati sensibili dell'ICCO e la cancellazione dei contenuti di database e computer;

- **Agosto 2022**
  - attacco alle istituzioni governative del Montenegro, violando i sistemi informatici di diversi enti statali;
  - attacco a DESFA, il più grande distributore di gas naturale della Grecia, causando un'interruzione del sistema e l'esposizione dei dati;
  - attacco DDoS da parte di un gruppo filo russo al Parlamento finlandese, con l'inaccessibilità al suo sito web;
  - attacco all'italiana GSE[14], Gestore dei Servizi Energetici, compromettendo i server, bloccando l'accesso ai sistemi e sospendendo l'accesso al sito web del GSE per una settimana;

- **Settembre 2022**
  - attacco da parte di un gruppo filo russo al sito web del MI5[15] (Military Intelligence, Sezione 5), l'agenzia di controspionaggio e sicurezza nazionale del Regno Unito;
  - vari attacchi del gruppo Anonymus contro due siti web del governo iraniano, ed altri siti web di media iraniani;
  - attacco da parte di un gruppo filo russo al sito web parlamentare a livello statale della Bosnia ed Erzegovina, rendendo i siti e i server inaccessibili per diverse settimane;
  - attacco da parte di un gruppo iraniano ai sistemi informativi del governo albanese, attacco che ha causato anche il blocco del Total Information Management System, un servizio utilizzato per tracciare le persone che entrano ed escono dall'Albania;

- **Ottobre 2022**
  - attacco da parte di un gruppo filo russo a vari siti web del governo statale degli Stati Uniti, e che li ha messo offline, inclusi quelli del Colorado, del Kentucky e del Mississippi;
  - attacco ransomware ad una piattaforma di comunicazione in Australia, che gestisce i dati del Dipartimento della Difesa, con violazione di dati governativi riservati;

- **Novembre 2022**
  - numerosi attacchi da parte di attori, persone e gruppi, affiliati allo stato cinese contro alcune piccole nazioni del sud-est asiatico per scopi di cyberspionaggio;
  - attacco con danneggiamento alla rete delle Ferrovie dello Stato danesi dopo aver attaccato l'ambiente di test del software di un subappaltatore IT delle ferrovie;
  - attacco ai sistemi informativi governativi del Guadalupe, che ha causato il loro totale blocco per proteggere i dati durante le fasi di risposta all'attacco;
  - attacco da un gruppo filo iraniano dell'agenzia statunitense U.S. Merit Systems Protection Board, sfruttando la vulnerabilità log4shell. Dopo aver violato la rete, è stato installato software di mining di criptovaluta e distribuito malware per ottenere dati sensibili;
  - attacco DDoS da parte del gruppo Killnet al sito del Parlamento Europeo

[14] GSE Spa è interamente partecipata dal Ministero dell'economia e delle finanze: ad essa è attribuito l'incarico di promozione e sviluppo delle fonti rinnovabili e dell'efficienza energetica.
[15] Il servizio di sicurezza dell'MI5 è diretto a proteggere la democrazia parlamentare britannica e gli interessi economici e a contrastare il terrorismo e lo spionaggio nel Regno Unito (UK).

- **Dicembre 2022**
  - frode informatica attuata da attori legati al governo cinese, che hanno rubato almeno 20 milioni di dollari in fondi di soccorso COVID-19 al governo degli Stati Uniti, compresi prestiti alla Small Business Administration e soldi dell'assicurazione contro la disoccupazione;
  - attacco DDoS contro il Ministero della Difesa Danese, con interruzione dell'accesso al suo sito web;
  - attacco DDoS da parte di gruppi filo russi contro i server della Città del Vaticano, con la messa offline del suo sito ufficiale;
  - attacco al sito web del Ministero dell'Agricoltura in Italia, rendendolo non accessibile;
  - serie di attacchi dal gruppo filo russo Sandworm a varie infrastrutture critiche ucraine, accompagnati da propaganda filo-russa;
  - attacchi di phishing, che contenevano malware progettato per lo spionaggio, da parte di attori filo cinesi contro vittime del governo, dell'istruzione e del settore della ricerca in tutta l'Asia del Pacifico.

Questo elenco, seppur lungo, rappresenta solo un esempio, e certo non esaustivo nemmeno per gravità probabile, dei moltissimi attacchi rilevati nel mondo, ed evidenzia la quantità di quelli attuati da parte di gruppi filo russi, filo cinesi e filo iraniani, oltre che alcune delle risposte dei gruppi filo ucraini e filo occidentali: le prevalenti tecniche d'attacco riguardano DDoS e malware-ransomware.

3.2 I principali attacchi digitali in Italia nel 2022

Anche l'Italia nel 2022 ha subito un forte aumento degli attacchi digitali intenzionali: sono continuati gli attacchi iniziati con la pandemia Covid e quelli "soliti" di criminalità informatica, anche se alcuni tecnicamente più sofisticati e più critici da contrastare, ma soprattutto sono iniziati attacchi digitali riconducibili alla guerra digitale relativa all'invasione della Ucraina, alcuni dei quali riportati nell'elenco dei principali attacchi a livello mondiale in §3.1.1.
A fianco dei vari e specifici attacchi digitali, sono inoltre aumentate in modo significativo **informazioni false**, sia su siti web, spesso malevoli, sia sui social, causando una **voluta ampia disinformazione** su vari temi, a partire dalla guerra in Ucraina e dal tema Covid/vaccini, ma con ben più gravi impatti nel quotidiano in Italia 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 ma alla quale il mondo occidentale liberale non ha ancora prestato la giusta attenzione e, forse, non sta ancora rispondendo con la dovuta forza.
Nei secoli scorsi, la disinformazione e le false notizie, e non solo in tempo di guerra, hanno sempre costituito un'arma, ma nell'attuale epoca di Internet diffusa a livello mondiale, con un'infinità di informazioni sui siti web e sui social, il fenomeno delle "fake news" ha raggiunto livelli così ampi da renderli estremamente critici: è sempre più difficile capire se un'informazione è corretta oppure no.
Pubbliche amministrazioni e ambiti sanitari sono stati i principali obiettivi della guerra informatica causata dall'invasione dell'Ucraina e dalla contrapposizione geopolitica occidente-anti occidente. Ne sono esempi gli attacchi ai siti del Senato di vari Ministeri: da quello della Difesa, da quello dell'Istruzione, dei Beni Culturali, della Transizione Ecologica , dell'Agricoltura. Tutti con attacchi prevalentemente basati su DDoS, ed alcuni con attacchi di natura meramente dimostrativa. Nel mirino anche le Pubbliche Amministrazioni Locali (PAL), dai siti delle Regioni a quelli di aziende del trasporto pubblico locale, alle aziende pubbliche energetiche, ad alcune ARPA, Agenzia Regionale per la Protezione dell'Ambiente. Attacchi diffusi anche ad ospedali e aziende sanitarie quali ASL, Aziende Sanitarie Locali, non solo con DDoS ma anche con ransomware (quelli di origine filo russa, ad esempio del Gruppo Conti, fanno molto probabilmente parte di azioni di guerra digitale verso uno Stato sostenitore dell'Ucraina): vari casi in Lombardia, a Torino, a Padova, con disservizi significativi per i pazienti. Sempre in ambito PA, nel corso del 2022 sono state attaccate anche le Ferrovie dello Stato, la Cassa Depositi e Prestiti, l' Agenzia delle Entrate, queste ultime due con data breach e furto di informazioni.

In ambito privato sono state attaccate banche, industrie manifatturiere note a livello mondiale, aziende dei trasporti, della vendita e della distribuzione soprattutto online.
Le tecniche prevalenti per tutti gli attacchi sono state il social engineering, soprattutto con il phishing, il DDoS, il ransomware/malware, e in alcuni casi tecniche multiple per il data breach e conseguente furto di informazioni. I ransomware più diffusi in Italia nel 2022 includono Lockbit 2.0, ALPHV (BlackCat), Grief e Conti.

3.3 Le vulnerabilità causa degli attacchi

Tutte le minacce cibernetiche, intenzionali e non, si basano su vulnerabilità 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 per l'ICT è il più delle volte involontaria, e causata da fattori quali l'inconsapevolezza, l'imprudenza, l'imperizia, l'ignoranza, dovute e spesso aggravate dalla mancanza di formazione e addestramento, tipiche vulnerabilità organizzative cui si sommano sovente altre carenze ed inefficienze organizzative, quali la mancanza di procedure scritte e divulgate, la mancanza di reali controlli e così via.

3.3.1 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** (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 scoperta e resa pubblica, questi siti riportano le modalità per eliminarle o ridurle, se esistono e sono state provate. Ogni prodotto/servizio ICT, di qualsiasi produttore, ha delle vulnerabilità tecniche individuate.
Alla data della scrittura del presente rapporto OAD, settembre 2023, il totale delle vulnerabilità individuate è di **212.202**, e di queste vulnerabilità più di **25.000** sono state scoperte nel 2022.

La fig. 3.3.1-1 mostra il numero di vulnerabilità nel 2022 per i primi 20 venditori come numero di vulnerabilità sui loro prodotti, derivato da CVE. La fig. 3.3.1-2 mostra il numero di vulnerabilità complessivo, in ogni tempo, per i primi 20 venditori, e mettendo tale numero in riferimento con il numero complessivo di prodotti del venditore, sempre da CVE. Questa correlazione è significativa: a parità di vulnerabilità complessive, il venditore che ha numerosi prodotti ha un numero di vulnerabilità per prodotto assai minore rispetto al venditore che ha relativamente pochi prodotti, ed è quindi di fatto più sicuro. E' il caso del confronto tra Microsoft e Google, entrambi ai primi due posti nelle classifiche delle due figure. Da esse emerge un altro dato di fatto, che contrasta con una diffusa convinzione: che i sistemi Apple abbiano poche vulnerabilità e quindi la loro sicurezza intrinseca sia assai più elevata rispetto ai principali concorrenti. Le classifiche CVE riportate nelle due figure evidenziano che Apple si posiziona rispettivamente all'ottavo (nel 2022) e al quinto posto in ogni tempo: con una media di 35 vulnerabilità per prodotto, altri sistemi operativi ed ambienti operativi (middleware) hanno mediamente meno vulnerabilità, come ad esempio, quelli di IBM, RedHat, Apache ed altri.

Le vulnerabilità tecniche crescono parallelamente alla crescita della complessità dei moderni sistemi informatici, sempre più difficili da gestire anche se di piccole dimensioni e con limitate funzionalità, come sono generalmente quelli usati da piccole e piccolissime organizzazioni. In termine generali, per le vulnerabilità tecniche, è bene evidenziare che:

- 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;
- non esiste prodotto ICT, di nessun fornitore, che non abbia delle vulnerabilità note.

	Vendor Name	Number of Vulnerabilities
1	Google	1770
2	Microsoft	952
3	Fedoraproject	947
4	Debian	923
5	Oracle	529
6	Netapp	499
7	Adobe	461
8	Apple	456
9	IBM	419
10	Jenkins	391
11	Tenda	390
12	Siemens	339
13	Huawei	322
14	Cisco	317
15	Linux	313
16	Redhat	303
17	Intel	248
18	Qualcomm	246
19	Apache	224
20	Totolink	209

Fig. 3.3.1-1 (Fonte: CVE Mitre)

Ogni vulnerabilità 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 del 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 3.1 (e sarà presto introdotta la versione 4) ed è composto da tre gruppi di metriche: base, temporale e ambientale**.** 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.
La fig**.** 3.3.1-3 riporta l'esempio, dal NVD di NIST, del livello di severità di base attribuito ad una vulnerabilità del 2022 sui sistemi SAP.

	Vendor Name	Number of Products	Number of Vulnerabilities	#Vulnerabilities/#Products
1	Microsoft	812	10914	13
2	Google	179	10369	58
3	Oracle	1080	9248	9
4	Debian	118	8416	71
5	Apple	196	6814	35
6	IBM	1507	6678	4
7	Cisco	6470	5955	1
8	Redhat	518	5070	10
9	Adobe	336	4990	15
10	Fedoraproject	24	4675	195
11	Canonical	51	4024	79
12	Linux	23	3367	146
13	Opensuse	61	3185	52
14	Mozilla	38	2875	76
15	HP	17310	2214	0
16	Netapp	368	2109	6
17	Apache	348	2090	6
18	Qualcomm	2655	1772	1
19	Huawei	1932	1738	1
20	Siemens	4050	1649	0

Fig. 3.3.1-2 (Fonte: CVE Mitre)

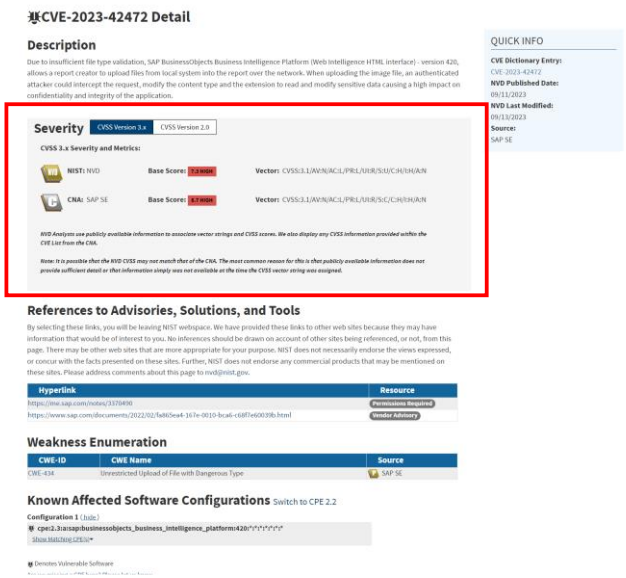


Fig. 3.3.1-3 (Fonte: NVD di NIST)

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).

3.3.2 Le vulnerabilità delle persone

Le vulnerabilità delle persone rappresentano per il mondo digitale rischi ancora più diffusi e gravi rispetto a quelle tecniche: e possono essere amplificate dalle vulnerabilità organizzative di cui in §3.3.3
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 dato dall'analisi DESI[16] sul livello di digitalizzazione dell'economia e della società, grazie alla voce "capitale umano", una dei 4 indicatori che costituiscono l'intero indice:

- il capitale umano: capacità di accedere ed usare Internet, e le competenze specialistiche in ambito digitale, che comprendono le capacità di sviluppo di programmi software ed anche quelle relative alla sicurezza digitale;
- la connettività: è misurata dalla diffusione della banda larga, in termini di copertura della banda larga fissa, della banda larga mobile e dei prezzi della banda larga;
- l'integrazione delle tecnologie digitali: la digitalizzazione del business e l'e-commerce;
- i servizi pubblici digitali: fa riferimento all'e-Government[17].

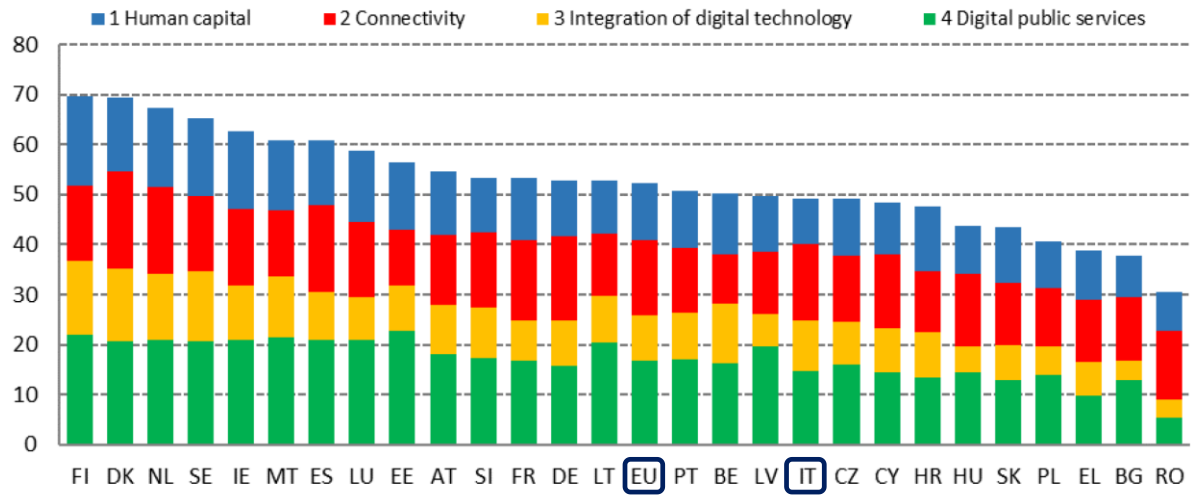


Fig. 3.3.2-1 (Fonte: DESI – Commissione Europea)

[16] 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.
Si veda https://digital-trategy.ec.europa.eu/it/policies/desi
[17] "e-Government" ha il generale significato di "uso dell'ICT nei processi amministrativi delle PA per migliorare ed innovare i servizi forniti ai cittadini". L'OCSE in particolare lo definisce come "l'uso delle nuove tecnologie dell'informazione e della comunicazione (ICT) da parte delle pubbliche amministrazioni applicato ad un vasto campo di funzioni amministrative. In particolare, il potenziale networking offerto da internet e dalle sue tecnologie ha il potenziale di trasformare le strutture e le procedure amministrative" e la Commissione Europea come "usare le nuove tecnologie per aumentare la partecipazione al processo democratico".

La fig. 3.3.2-1 mostra che l'Italia, nel complesso degli indicatori DESI per il 2022, si trova ancora al di sotto della media europea, pur avendo migliorato di alcuni posti negli ultimi anni.
La fig. 3.3.2-2, con la linea blu tratteggiata, evidenzia come l'Italia sia invece ancora all'ultimo posto, tra tutti i paesi europei, nelle competenze più avanzate riguardanti il mondo digitale, sia lato utenti sia lato specialisti ICT. Il problema delle competenze ICT in Italia, anche solo di base, costituisce un grave "minus" nella competitività del paese, non solo in ambito europeo ma mondiale.
Le specifiche competenze per la sicurezza digitale sono ancor più ridotte, essendo un di cui delle più generali dell'ICT, ed incidono sul livello di sicurezza digitale delle singoli organizzazioni e dell'intero sistema paese.
Considerando l'enorme numero di piccole e piccolissime aziende e amministrazioni pubbliche, l'incompetenza sulla sicurezza digitale lascia ampio spazio al millantato credito e a comportamenti scorretti di numerosi attori ed interlocutori dell'offerta, che rasentano sovente la truffa. La bassa o nulla competenza nella sicurezza digitale è un effetto leva per una sua forte terziarizzazione, a livello operativo, ma al contempo pone difficoltà nella scelta del fornitore idoneo a fornire una soluzione adeguata alla propria realtà.

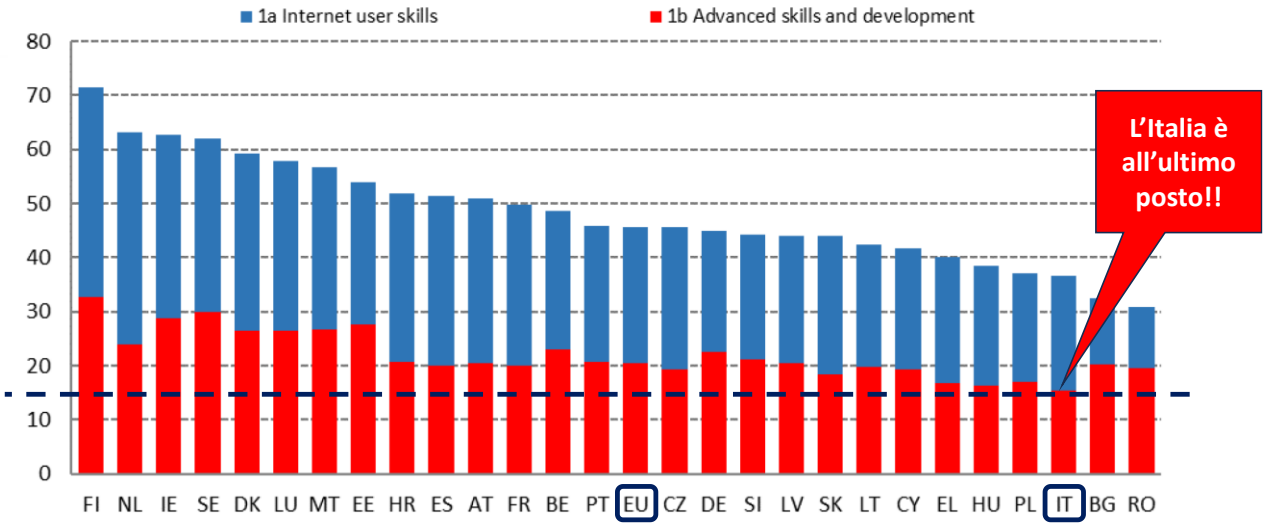


Fig. 3.3.2-2 (Fonte: DESI – Commissione Europea)

3.3.3 Le vulnerabilità organizzative

Gli aspetti organizzativi sono determinanti per l'attuazione di una reale 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 poter gestire operativamente la sicurezza digitale, e avere serie e aggiornate informazioni per governare strategicamente la sicurezza digitale del sistema informativo. Sarebbe opportuno terziarizzare la sua gestione operativa e di poter disporre di consulenti realmente esperti per la governance. Ma in entrambi i casi occorre saper scegliere i fornitori, e saperli controllare ed indirizzare rispetto alla propria specifica realtà. 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 ed aggiornate competenze nella cybersecurity: il cerchio delle incompetenze si potrebbe così chiudere 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 nel Rapporto 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 almeno le competenze necessarie per saper scegliere fornitori competenti e affidabili, e saperli supervisionare nei loro interventi, operativi o strategici, sulla sicurezza digitale.

La sicurezza digitale del sistema informativo non deve essere considerata solo come un problema tecnico, ma soprattutto come uno di business, dato che è determinante per la continuità operativa dell'intera azienda/ente.

3.2 Gli attaccanti e le loro motivazioni

Nel tempo la tipologia degli attaccanti si è profondamente evoluta: dai singoli che per verificare le proprie capacità e talvolta per dimostrare che un determinato codice software non era sicuro, gli attuali ethical hacker, a gruppi di specialisti, cracker, con ampie risorse tecniche e finanziarie che operano a livello mondiale con fini criminali e/o per governi nell'ambito di guerre idigitali. Il cybercrime è oggi un business ad alto rendimento, data anche la difficoltà di contrastarlo, nonostante le varie leggi e normative in atto a livello italiano, europeo e in altri paesi. Alcuni malware si trovano facilmente in Internet, e sta emergendo un mercato di "CyberAttack as a Service" e di specialisti che si offrono, a pagamento, per condurre attacchi digitali.
ENISA, nel suo ultimo rapporto "Threat landscape 2022"[18], considera le seguenti categorie di attori che minacciano la sicurezza digitale: attori sponsorizzati da Stati, cyber criminali, hacker a noleggio (for-hire actors), hacktivist.

Chi effettua un attacco digitale lo fa con sue specifiche motivazioni, che possono variare di caso in caso. Lo specialista che opera singolarmente come cracker, al di fuori di gruppi organizzati, è ora una rarità, tipicamente il singolo che effettua un attacco per vendicarsi di torti subiti, o il giovane, anche poco esperto ma con parecchio tempo libero a disposizione, che prova in maniera casuale e quasi massiva ad attaccare persone, enti ed aziende per vedere che cosa è capace di fare e magari che cosa può ottenere.

L'indagine, e quindi il questionario, OAD 2023 sono focalizzati sugli **attacchi in ambito web**. In tale contesto in §4 sono approfonditi i risultati dell'indagine per quanto riguarda i probabili attaccanti e le loro motivazioni. In sintesi la maggior parte degli attacchi è dall'esterno, talvolta con l'involontaria complicità di utente interno.
La motivazione principale di un attacco è prevalentemente economica, ossia di un illecito guadagno, talvolta associata ad altre motivazioni, quali la vendetta, l'hacktivism, la guerra digitale.

In merito alle **guerre digitali**, esse non si limitano alla guerra ibrida dell'invasione dell'Ucraina, ma alle ulteriori e crescenti tensioni geopolitiche tra mondo occidentale e paesi illiberali e/o a forte connotazione islamica.
Nella guerra ibrida contro l'Ucraina ed i suoi alleati, in primis US ed Unione Europea, i primi attacchi digitali furono effettuati direttamente dai servizi segreti della Federazione Russa, quali probabilmente Gru e Fsb (ex KGB) [19], e da gruppi da questi ultimi pilotati come il Gruppo Conti, ben noto per i vari ransomware creati e diffusi con alti guadagni sui relativi ricatti, ed il Gruppo Sandworm pilotato da Gru.
In generale è difficile poter individuare i vari gruppi di cyber criminali, dato che i più ben si camuffano e si nascondono, ma altri si palesano e addirittura si fanno pubblicità su loro siti web. Tra i più noti gruppi di hacker/cracker, oltre ai già citati Gruppi Conti e Sandworm, Anonymous, che si è schierato contro la Federazione Russa dopo l'invasione dell'Ucraina, Cult of the Dead Cow, storicamente uno dei primi gruppi US, Chaos Computer Club, ritenuto il più grande gruppo europeo di ethical hacker, Dark Side tra i primi ad offrire servizi RaaS, Ransomware as a Service, Equation Group operante per la statunitense NSA (National Security Agency), Fancy Bear pilotato dal governo russo e probabilmente

[18] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[19] Per approfondimenti si veda l'articolo dell'autore: https://www.agendadigitale.eu/sicurezza/ucraina-come-agisce-la-guerra-cyber-e-quali-impatti-sulleuropa/

anch'esso coinvolto in vari attacchi contro paesi e personaggi occidentali oltre che contro l'Ucraina, Lazarus guidato dalla Nord Corea insieme a Bureau 121 creatore di Wannacry, Machete operativo prevalentemente nei paesi sudamericani, PLA Unit 61398 guidato dalla Cina ed autore di numerosi attacchi ad enti ed imprese US, Shadow Brokers, probabili co-autori di Stuxnet e diffusori di Wannacry e NotPetya, Unit 8200 alle dipendenze del governo israeliano e probabilmente coinvolto nella creazione di Stuxnet. Per un più ampio elenco, non esaustivo, di gruppi cyber, governativi, criminali o altro, si veda: https://en.wikipedia.org/wiki/List_of_hacker_groups.
Per un elenco dei più noti criminali informatici si veda: https://en.wikipedia.org/wiki/List_of_computer_criminals.

3.3 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[20], solo in parte proattive e preventive[21], e pochissime predittive[22].
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[23], 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**", ma in Italia prevalentemente usate, ad oggi, solo da grandi organizzazioni, 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;
- una crescente e forte automazione dei processi e delle attività della gestione operativa della sicurezza digitale, con l'uso di tecniche di Machine Laerning (ML) e di altre tecniche di intelligenza artificiale (AI)[24];
- 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 AI 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 privacy;

[20] 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.
[21] 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.
[22] 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.
[23] **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/
[24] 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.

- l'introduzione di soluzioni EDR, Endpoint[25] Detection & Response[26], 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 interoperanti con il sistema informativo target;
- inizio utilizzo soluzioni di "Threat Intelligence";
- la crescente adozione di misure di sicurezza digitale "as a service", e la crescente terziarizzazione della sicurezza digitale, soprattutto a livello di gestione operativa;
- 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 centro iper specializzato, che alcune grandi organizzazioni, ad esempio di fornitori ICT e TLC, hanno al proprio interno, ma che è anche fornito "as a service" da specializzati MSSP, Managed Security Service Provider;
- l'adozione, oggi ancora embrionale, di soluzioni XR, Extended Reality, e del metaverso[27], 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 delle aziende/enti, non solo di quelle più critiche.

Occorre pertanto:

- attivare e gestire al meglio tutte le attuali misure;
- far crescere la consapevolezza e le competenze a tutti i livelli sulla sicurezza digitale, 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**, che dovranno essere attuate quasi tutte entro il 2024: le principali sono elencate nella tabella in fig. 3.4-1.

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.

[25] 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.

[26] 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.

[27] 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).

Normativa	Riferimento	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

Fig. 3.4-1

Volutamente in questa tabella si sono inserite all'inizio due normative , il GDPR e l'EU Cybersecurity Act per la loro importanza pratica per la sicurezza digitale in Europa. Altre normative, più o meno recenti, sono state e sono ancora di riferimento diretto o complementare, dalla strategia decennale sulla cybersecurity (https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy) al Cyber Relisience Act[28] e alle normative sull'intelligenza artificiale, sull'identità digitale, sui dati e sul loro governo, sui chip.
I paragrafi del successivo §7 forniscono una fotografia delle misure di sicurezza, tecniche ed organizzative, in essere nei sistemi informativi delle aziende/enti che hanno risposto alle domande "opzionali" sull'argomento del questionario online OAD 2023.

3.4.1 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.
Moderne piattaforme e soluzioni quali SIEM, SOAR, SESA, e le stesse tecniche di blockchain, costituiscono sistemi molto complessi e già difficili da gestire per grandi organizzazioni con elevate competenze al proprio interno, figuriamoci per le piccole e piccolissime così diffuse in Italia!
Ma 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 il mercato di questo tipo di fornitori di servizi di sicurezza gestiti, indicate come MSSP, Managed Security Service Provider, ed incominciano ad essere utilizzati i servizi di grandi player.
Uno dei loro principali strumenti è il SOC[29], il sistema di controllo delle attività di un sistemo informatico, reti incluse, focalizzato sul monitoraggio di eventi legati alla sicurezza e che integra vari strumenti e misure di sicurezza, quali le moderne soluzioni di cui sopra. Grandi strutture hanno e gestiscono un SOC al loro interno, ma la maggior parte, ed in particolare le strutture di medie e piccole dimensioni, terziarizzano in tutto o in parte la gestione della sicurezza digitale a MSSP che a loro volkta sono dati o utilizzano SOC di altre Terze Parti..
Per ulteriori approfondimenti sull'argomento si rimanda all'articolo "CyberSecurity as a Service e Managed Security Services: quali vantaggi per Pmi e PA", si veda https://www.aipsi.org/breaking-news/820-articolo-su-cybersecurity-as-a-service-e-managed-security-services-quali-vantaggi-per-pmi-e-pa-su-agenda-digitale.html

[28] Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (2022/0272(COD)).
[29] SOC, Security Operation Center, è l'insieme di un team di esperti ed un sofisticato sistema di monitoraggio di eventi legati alla sicurezza e che integra vari strumenti e misure di sicurezza.

3.5 *Il quadro di riferimento Italiano per la sicurezza digitale*

3.5.1 Aziende e PA in Italia

I più recenti dati ISTAT sulle imprese attive in Italia fanno riferimento al 2020, e come riportato nel Cap 14 del Rapporto ISTAT pubblicato nel 2022 (https://www.istat.it/storage/ASI/2022/capitoli/C14.pdf), si contano 4 milioni 354 mila imprese attive, cui corrispondono 17 milioni e 138 mila addetti. Ma in questa ultima analisi ISTAT fa ancora riferimento ai dati 2019 per la ripartizione per classe di addetti, come riportato in fig. 3.5.1-1.
Nel 2020 c'è stato un aumento di numero di aziende rispetto al 2019 di 141.021, e la ripartizione per classe di addetti ben poco si discosta da quella del 2019. I dati più significativi sono che le aziende non PMI, quindi dai 250 dipendenti in su sono l'1% del totale e tra **le PMI, complessivamente il 99,9%**, quelle più piccole, fino a 9 dipendenti, sono la stragrande maggioranza con un **94,8%** sul totale.

Numero dipendenti	Numero aziende	%
0-9	3.990.961	94,8%
10-19	135.638	3,2%
20-49	55.137	1,3%
50-249	23.186	0,6%
250 e oltre	4.057	0,1%
TOTALE	**4.208.979**	

Fig. 3.5.1-1 (Fonte: ISTAT 2022 su dati 2019)

Per comprendere e ben considerare la realtà delle Pubbliche Amministrazioni (PA) in Italia, e la loro situazione nei Sistemi Informativi e nella loro sicurezza digitale, occorre considerare la loro complessa articolazione in PA Centrali (PAC) e Locali (PAL).
La PA italiana è costituita, in accordo con l'art. 1 comma 2 del D.lgs 30 marzo 2001 n. 165 (https://www.gazzettaufficiale.it/eli/id/2001/05/09/001G0219/sg) da:

- Presidenza del Consiglio dei ministri, i ministeri e le loro articolazioni centrali e locali, le istituzioni scolastiche, le agenzie[30] e le aziende autonome[31];
- le autorità amministrative indipendenti, che sono Enti pubblici con personalità giuridica: attualmente sono solo l'Amministrazione degli archivi notarili ed i Monopoli di Stato ;
- le regioni, le province, le città metropolitane, i comuni e gli altri enti territoriali locali quali ad esempio comunità montane, le comunità isolane, le unioni di comuni e i consorzi fra enti territoriali;
- gli altri enti pubblici, nazionali e locali, tra cui le istituzioni universitarie, gli enti pubblici di ricerca, le camere di commercio, industria, artigianato e agricoltura e gli enti che compongono il Servizio Sanitario Nazionale.

Per approfondire la realtà della PA si vedano anche le informazioni sull'IPA, Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi, in https://www.indicepa.gov.it/ipa-portale/dati-statistiche.

[30] Una Agenzia è distinta dall'organizzazione ministeriale, svolge una funzione pubblica ed è sottoposta a direzione o vigilanza da parte di un organo politico. Esempi: Agenzia delle Entrate, Agenzia del Demanio, AIFA, etc.; nel settore ICT AgID e ACN.
[31] Una Azienda Autonoma è una organizzazione che fa parte dello Stato o di altro ente pubblico e che è normalmente priva di personalità giuridica, ma possiede caratteri che le conferiscono un certo grado di compiutezza e separatezza. Il suo compito è di fornire e gestire servizi di pubblico interesse. Testo unico delle leggi sull'ordinamento degli enti locali- D.Lgs. 18 agosto 2000, n. 267 (https://web.camera.it/parlam/leggi/deleghe/testi/00267dl.htm). Molte Aziende Autonome nel passato sono state privatizzate o trasformate in Ente pubblico economico o in Agenzia.

Il totale dei dipendenti pubblici, al 2020, risulta di circa 3.200.000, secondo i dati forniti dalla Corte dei Conti nella sua "Relazione sul Costo del Lavoro Pubblico 2020" (https://www.corteconti.it/Download?id=fc101a7e-cc6c-4cd4-8561-a7cbcf05a1af), anche se con dati del 2018, oltre che in https://openbdap.rgs.mef.gov.it/it/PIM/Esplora.

Nel 2022 la Pubblica Amministrazione italiana ha speso oltre 7 miliardi di euro in ICT (Tecnologie dell'informazione e della comunicazione), registrando un aumento del 5,8% rispetto al 2021.
Un dato che secondo le stime continuerà a crescere nel prossimo triennio, anche grazie ai fondi del PNRR.
Piattaforme e infrastrutture ICT rappresentano i principali macro-ambiti in termini di spesa, rispettivamente con il 49% e il 20% del totale, seguiti da servizi (14%), dati (8%), sicurezza informatica (4%), governance (3%) e interoperabilità (2%). Ormai pienamente diffuso è l'uso del cloud: ne fanno ricorso il 100% delle PA locali, il 95% delle Regioni e Province autonome e l'89% delle PA centrali; l'utilizzo di nome utente e password proprie per l'accesso da parte dei cittadini ai servizi di alcune PA continua invece a scendere, a favore delle identità digitali Spid, CIE e CNS.

Grazie al PNRR ed alla strategia per la digitalizzazione delle PA, si sta completando, sotto la guida del DTE, Dipartimento Trasformazione Digitale, di ACN e con la costituzione di una società ad hoc per gestirlo, il **PSN, Polo Strategico Nazionale,** un sistema in cloud ad altissima sicurezza e affidabilità per ospitare i dati ed i servizi critici e strategici delle PA italiane: per approfondimenti https://www.polostrategiconazionale.it/.

Aumenta e migliora, infine, anche l'indice di digitalizzazione complessivo delle PA: rispetto alle scorse rilevazioni, infatti, è cresciuta la percentuale di Amministrazioni appartenenti ai cluster dei Digital leader (12%) e degli Advanced (66%), mentre cala quello delle PA classificate come Digital starter (21%) e Growing (1%).

AgID realizza un Piano Triennale per l'informatica nella PA, arrivato ora con l'aggiornamento 2021-23 (si veda https://www.agid.gov.it/it/agenzia/piano-triennale), ed effettua sulla spese e sull'attuazione dei vari progetti dei controlli su circa il 50% della PA, Difesa esclusa.
La fig. 3.5-2 fornita dall'ISTAT su un suo parziale censimento sulle PAC e PAL (si veda https://www.istat.it/it/archivio/264488), evidenzia che la maggior parte di esse sono piccolissime organizzazioni, e che il 95% è costituito da strutture fino a 249 dipendenti, paragonabili quindi alle PMI private. Questo censimento è del 2018, ed è l'ultimo disponibile alla data.

CLASSI DI DIPENDENTI	Istituzioni per numero dipendenti	%
da 0 a 9	6.383	47,6
da 10 a 49	4.595	34,3
da 50 a 249	1.751	13,1
da 250 a 999	362	2,7
da 1,000 a 24,999	306	2,3
25,000 e oltre	9	0,1
Totale	**13.406**	**100,0**

Fig. 3.5-2 (ISTAT)

3.5.2 La spesa in sicurezza digitale in Italia nel 2022

Le due più attendibili fonti per il mercato ICT e per la sicurezza digitale in Italia sono le annuali ricerche di Anitec-Assinform e Assintel, che sono associazioni patrocinanti OAD 2023 e alle quali il presente rapporto fa riferimento.

- Il **Rapporto Anitec-Assinform** "Il Digitale in Italia 2023" stima l'intero mercato digitale in Italia nel 2022 in € 77, 085 Mldi, che rappresenta il 4% del Pil.
  - Il mercato della cybersicurezza, in Italia e nel 2022, ha un valore stimato di € **1.590,1 Mlni**, che crescerà nel 2023 a **1.825,5 Mlni**, con un incremento del 14,8%. Tale stima include sia il mercato business che quello consumer.
- Il **Rapporto 2022 di Assintel** considera solo il mercato ICT business, non quello consumer, che valuta complessivamente in € 36,34 Mldi, ma non fornisce dati specifici sul mercato della sicurezza digitale in Italia.
  - Un dato interessante del rapporto è la spesa in ICT, in funzione del numero di dipendenti, nelle imprese "digitalizzate", ossia quelle con almeno 1 PC ed 1 collegamento ad Internet, e che include anche la quota parte del costo complessivo della sicurezza digitale. Il Rapporto Assintel stima il numero di imprese digitalizzate in poco più di 3,8 milioni di unità e al 94% sono costituite da piccole imprese con meno di 9 addetti. La spesa media annua ICT per azienda digitalizzata è in generale di poco inferiore a 9.500 euro, ma molto differenziata in relazione alle dimensioni: in media, le imprese italiane con meno di 9 addetti spendono ciascuna poco più di 2.500 euro all'anno, mentre le imprese con oltre 250 addetti spendono in ICT in media oltre 3,7 milioni di euro all'anno ciascuna. Inoltre il Rapporto pone la "Next Generation Security" tra gli acceleratori dell'innovazione.

Nel complesso la spesa per la sicurezza digitale in Italia è attorno allo 0,07% del suo Pil[32], la più bassa rispetto ai Paesi del G7 e comunque troppo bassa per una moderna nazione digitalizzata, o ancor più che ha in corso un deciso piano di digitalizzazione: a questo basso valore contribuisce sicuramente l'elevato numero di piccolissime organizzazioni, che finora hanno implementato solo alcuni dei servizi di base della sicurezza digitale.

3.5.3 Il PNRR ed il suo impatto nella trasformazione digitale del Paese

Il PNRR[33], Piano Nazionale di Riprese e Resilienza, è il piano italiano per poter usufruire dei finanziamenti, in parte a fondo perduto, del Next Generation dell'Unione Europea (NGEU)[34] che rappresenta la risposta europea alla grave crisi pandemica con importanti investimenti e riforme per:

- accelerare la transizione ecologica e digitale;
- migliorare la formazione delle lavoratrici e dei lavoratori;
- e conseguire una maggiore equità di genere, territoriale e generazionale.

Per l'Italia il NGEU è un'imperdibile opportunità di sviluppo, ma richiede, a fronte dei finanziamenti forniti, l'attuazione effettiva di importanti riforme da tempo indispensabili. L'Italia è fragile dal punto di vista economico, sociale ed ambientale , e tra le cause di queste fragilità c'è l'arretratezza nel digitale, dovuta sia ai ritardi e all'arretratezza/mancanza di idonee infrastrutture ICT (in particolare connessioni ad Internet in larga banda) sia la prevalenza di piccole e piccolissime organizzazioni, private e pubbliche, che sono state lente nell'adottare efficacemente l'innovazione tramite il digitale, sia l'incapacità/incompetenza sul digitale per parte del management, pubblico e privato, nell'effettuare le giuste scelte e di sfruttare le opportunità dell'innovazione digitale, sovente con la complicità di cattivi consigli da parte di consulenti e fornitori.

La digitalizzazione e l'innovazione di processi, prodotti e servizi rappresentano un fattore determinante della trasformazione dell'Italia e devono caratterizzare ogni politica di riforma del Piano.

[32] Pil, Prodotto interno lordo (ai prezzi di mercato). Secondo la definizione ISTAT: "è il risultato finale dell'attività di produzione delle unità produttrici residenti. Corrisponde alla produzione totale di beni e servizi dell'economia, diminuita dei consumi intermedi ed aumentata dell'Iva gravante e delle imposte indirette sulle importazioni."

[33] https://www.governo.it/sites/governo.it/files/PNRR.pdf

[34] https://ec.europa.eu/info/strategy/recovery-plan-europe_it

Il PNRR, congruentemente con il NGEU, si articola in sedici Componenti, raggruppate in sei Missioni e sintetizzate nella tabella di fig. 3.5.3-1 (per i dettagli si rimanda a https://italiadomani.gov.it/it/home.html). La Tabella evidenzia le risorse assegnate a missioni e componenti del PNRR. A tali risorse, si aggiungono quelle rese disponibili dal REACT-EU che, come previsto dalla normativa UE, vengono spese negli anni 2021-2023 nonché quelle derivanti dalla programmazione nazionale aggiuntiva.
La digitalizzazione è un asse strategico e trasversale all'intero PNRR, definita nella Missione 1 ed articolata nella Componente 1 per le PA e nella Componente 2 per il sistema produttivo delle aziende. Questa Missione ha l'obiettivo di dare un impulso decisivo al rilancio della competitività e della produttività del Sistema Paese. Si deve comunque tener conto, come evidenziato nel PNRR, che "Lo sforzo di digitalizzazione e innovazione è centrale in questa Missione, ma riguarda trasversalmente anche tutte le altre. La digitalizzazione è infatti una necessità trasversale, in quanto riguarda il continuo e necessario aggiornamento tecnologico nei processi produttivi; le infrastrutture nel loro complesso, da quelle energetiche a quelle dei trasporti, dove i sistemi di monitoraggio con sensori e piattaforme dati rappresentano un archetipo innovativo di gestione in qualità e sicurezza degli asset (Missioni 2 e 3); la scuola, nei programmi didattici, nelle competenze di docenti e studenti, nelle funzioni amministrative, della qualità degli edifici (Missione 4); la sanità, nelle infrastrutture ospedaliere, nei dispositivi medici, nelle competenze e nell'aggiornamento del personale, al fine di garantire il miglior livello di assistenza sanitaria a tutti i cittadini (Missioni 5 e 6)."

Gli **aspetti di sicurezza digitale** sono evidenziati nella Componente 1 della Missione 1, data la loro arretratezza in particolare nei sistemi informativi delle PA, a parte le debite eccezioni, ma sono da considerarsi anche per tutti gli altri Componenti nelle varie Missioni. "La trasformazione digitale della PA contiene importanti misure di rafforzamento delle difese *cyber*, a partire dalla piena attuazione della disciplina in materia di "Perimetro di Sicurezza Nazionale Cibernetica". Gli investimenti sono organizzati su quattro aree di intervento principali. In primo luogo, sono rafforzati i presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio intercettatati verso la PA e le imprese di interesse nazionale. In secondo luogo, sono costruite o rese più solide le capacità tecniche di valutazione e audit continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale. Inoltre, si investe nell'immissione di nuovo personale sia nelle aree di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione e investigazione del crimine informatico diretto contro singoli cittadini, sia in quelle dei comparti preposti a difendere il paese da minacce cibernetiche. Infine, sono irrobustiti gli asset e le unità *cyber* incaricate della protezione della sicurezza nazionale e della risposta alle minacce *cyber*. Tutto ciò è svolto in pieno raccordo con le iniziative Europee e alleate, per assicurare la protezione degli interessi comuni dei cittadini e delle imprese. Come investimento sulla sicurezza digitale in questo solo M1C1 sono previsti 0,62 Miliardi di €.

Tra le realizzazioni più importanti in corso per la sicurezza digitale:

- M1:
  - creazione del Polo Strategico Nazionale (PSN) , https://www.polostrategiconazionale.it/ per dotare la Pubblica Amministrazione di un'infrastruttura cloud sicura, efficiente ed affidabile;
  - definizione dell'architettura dell'ecosistema di cybersecurity nazionale, l'individuazione dei luoghi in cui sorgeranno i laboratori, i centri di verifica e certificazione, la centrale di audit per le misure di sicurezza digitale;
- M6:
  - lavori in corso, seppure con alcuni ritardi, per la Piattaforma Nazionale di Telemedicina: stesura capitolato e successiva gara per la progettazione, sviluppo e gestione della piattaforma, per un valore di 250 mlni €;
  - per l'ammodernamento del parco tecnologico ospedaliero, Regioni e Provincie Autonome stanno acquistandole da Consip.

M1. DIGITALIZZAZIONE, INNOVAZIONE, COMPETITIVITÀ, CULTURA E TURISMO	PNRR (a)	React EU (b)	Fondo complementare (c)	Totale (d)=(a)+(b)+(c)
M1C1 - DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA PA	9,75	0,00	1,40	11,15
M1C2 - DIGITALIZZAZIONE, INNOVAZIONE E COMPETITIVITÀ NEL SISTEMA PRODUTTIVO	23,89	0,80	5,88	30,57
M1C3 - TURISMO E CULTURA 4.0	6,68	0,00	1,46	8,13
Totale Missione 1	**40,32**	**0,80**	**8,74**	**49,86**
M2. RIVOLUZIONE VERDE E TRANSIZIONE ECOLOGICA	PNRR (a)	React EU (b)	Fondo complementare (c)	Totale (d)=(a)+(b)+(c)
M2C1 - AGRICOLTURA SOSTENIBILE ED ECONOMIA CIRCOLARE	5,27	0,50	1,20	6,97
M2C2 - TRANSIZIONE ENERGETICA E MOBILITA' SOSTENIBILE	23,78	0,18	1,40	25,36
M2C3 - EFFICIENZA ENERGETICA E RIQUALIFICAZIONE DEGLI EDIFICI	15,36	0,32	6,56	22,24
M2C4 - TUTELA DEL TERRITORIO E DELLA RISORSA IDRICA	15,06	0,31	0,00	15,37
Totale Missione 2	**59,47**	**1,31**	**9,16**	**69,94**
M3. INFRASTRUTTURE PER UNA MOBILITÀ SOSTENIBILE	PNRR (a)	React EU (b)	Fondo complementare (c)	Totale (d)=(a)+(b)+(c)
M3C1 - RETE FERROVIARIA AD ALTA VELOCITÀ/CAPACITÀ E STRADE SICURE	24,77	0,00	3,20	27,97
M3C2 - INTERMODALITÀ E LOGISTICA INTEGRATA	0,63	0,00	2,86	3,49
Totale Missione 3	**25,40**	**0,00**	**6,06**	**31,46**
M4. ISTRUZIONE E RICERCA	PNRR (a)	React EU (b)	Fondo complementare (c)	Totale (d)=(a)+(b)+(c)
M4C1 - POTENZIAMENTO DELL'OFFERTA DEI SERVIZI DI ISTRUZIONE: DAGLI ASILI NIDO ALLE UNIVERSITÀ	19,44	1,45	0,00	20,89
M4C2 - DALLA RICERCA ALL'IMPRESA	11,44	0,48	1,00	12,92
Totale Missione 4	**30,88**	**1,93**	**1,00**	**33,81**
M5. INCLUSIONE E COESIONE	PNRR (a)	React EU (b)	Fondo complementare (c)	Totale (d)=(a)+(b)+(c)
M5C1 - POLITICHE PER IL LAVORO	6,66	5,97	0,00	12,63
M5C2 - INFRASTRUTTURE SOCIALI, FAMIGLIE, COMUNITÀ E TERZO SETTORE	11,17	1,28	0,34	12,79
M5C3 - INTERVENTI SPECIALI PER LA COESIONE TERRITORIALE	1,98	0,00	2,43	4,41
Totale Missione 5	**19,81**	**7,25**	**2,77**	**29,83**
M6. SALUTE	PNRR (a)	React EU (b)	Fondo complementare (c)	Totale (d)=(a)+(b)+(c)
M6C1 - RETI DI PROSSIMITÀ, STRUTTURE E TELEMEDICINA PER L'ASSISTENZA SANITARIA TERRITORIALE	7,00	1,50	0,50	9,00
M6C2 - INNOVAZIONE, RICERCA E DIGITALIZZAZIONE DEL SERVIZIO SANITARIO NAZIONALE	8,63	0,21	2,39	11,23
Totale Missione 6	**15,63**	**1,71**	**2,89**	**20,23**
TOTALE	191,50	13,00	30,62	235,12

I totali potrebbero non coincidere a causa degli arrotondamenti.

Fig. 3.5.3-1 Composizione del PNRR per Missioni e Componenti con valori in miliardi di €

3.5.4 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. 3.5.4-1 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.

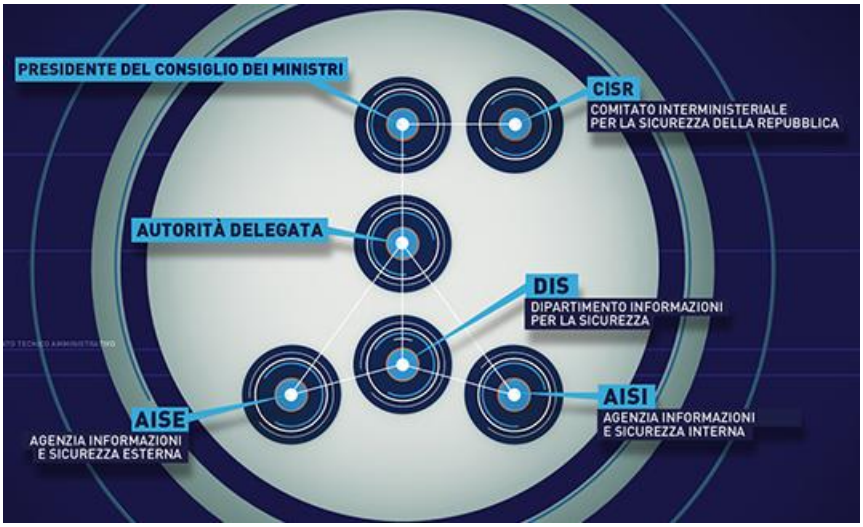


Fig. 3.5.4-1 (Fonte: Presidenza del Consiglio dei Ministri)

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 recentemente applicata dal Governo 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/). Ad ACN rispondono attualmente i seguenti enti:

- **NCS**, Nucleo per la cybersicurezza: ha funzioni di prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento;
- **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 (https://www.csirt.gov.it/guide);
- **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.

A livello militare la struttura operativa è il **COR**, **Comando Operazioni in Rete**: sotto la supervisione del Capo di Stato Maggiore della Difesa (Casmd), coordina le attività di sicurezza e difesa cibernetica delle Forze Armate e del Ministero della Difesa (https://www.difesa.it/SMD_/COR/Pagine/default.aspx).

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

- **Polizia Postale e delle Comunicazioni**: preposta al contrasto delle frodi postali e del crimine informatico (https://www.commissariatodips.it/)
  - **CNAIPIC**, 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.reportdifesa.it/tag/nucleo-speciale-tutela-privacy-e-frodi-tecnologiche-nstpft/)

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 cybernetica dei vari paesi membri dell'UE;
- **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/, che a maggio 2021 ha ufficialmente deciso di produrre un nuovo trattato mondiale sul crimine informatico, per poter rafforzare la prevenzione e le misure di sicurezza digitali in tutti i paesi del globo. Questo trattato dovrebbe essere presentato all'assemblea generale per la sua approvazione nel 2024, e attualmente sono in corso proposte, discussioni e trattative tra i vari paesi per cercare di arrivare ad un trattato condiviso.

.

4. Gli attacchi digitali in Italia dall'indagine OAD 2023

Nell'ottica di ridurre il tempo necessario a compilare il questionario OAD online, esso è stato semplificato ed è stato focalizzato sugli attacchi digitali subiti nel **2022 alle applicazioni ed agli ambienti web**, con due sole domande sugli altri attacchi rilevati, in modo da poter continuare l'analisi dei trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 ad oggi.

La fig. 4-1 mostra, percentualmente, il numero di attacchi digitali intenzionali rilevati dai rispondenti nel 2022 ed evidenzia un ulteriore **forte incremento** rispetto agli anni precedenti, trend approfondito nell'analisi effettuata commentando la fig. 4-2.

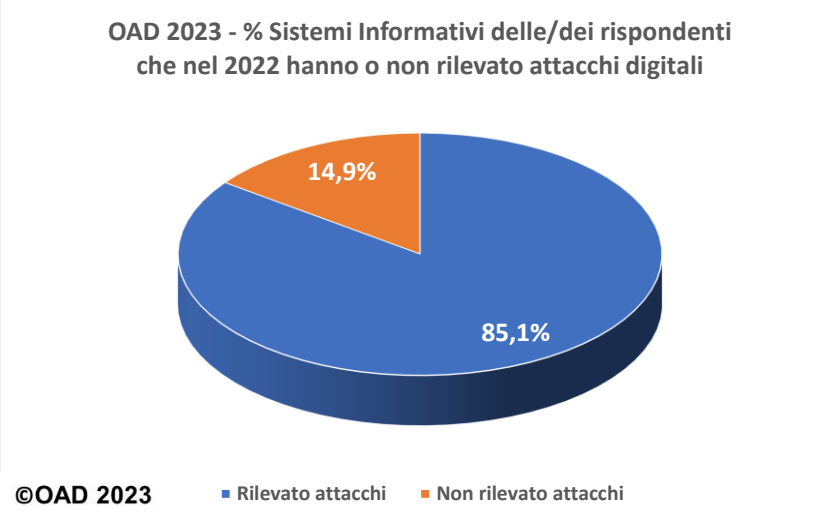


Fig. 4-1

La fig. 4-2 confronta il numero di attacchi rilevati nei diversi Rapporti OAI dal 2007 al 2023. 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 avuto un sali-scendi, evidenziato in figura dalla riga rossa, del numero di attacchi rilevati attorno a circa il 40% dei rispondenti: la riga verde evidenzia in tale periodo questo trend: l'onda altalenante delle percentuali di attacchi digitali rilevati dalle indagini 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 raggiunge il primo picco di 55,7%, la prima volta in cui la percentuale di attacchi rilevati supera, 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.

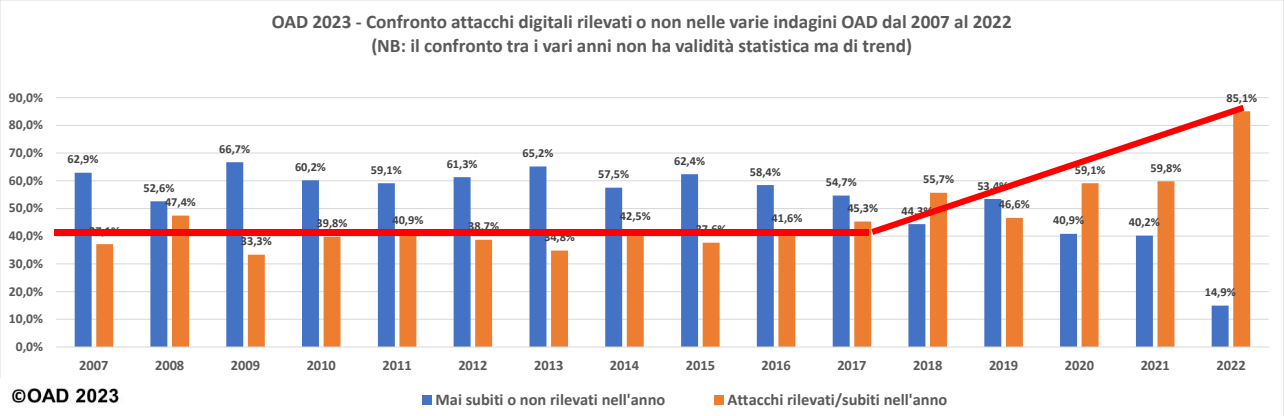


Fig. 4-2

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 sistemi informativi che hanno rilevato attacchi, con un delta tendenziale di poco più del 25%. Negli ultimi tre anni la percentuale di attacchi rilevati supera nettamente quella di attacchi non subiti.

Come già analizzato nel Capitolo 3, questo forte incremento è dovuto anche alla guerra cibernetica per l'invasione dell'Ucraina e per la "coda" del Covid, che si sommano agli attacchi digitali di criminalità informatica; ed è un chiaro indicatore di come da un lato gli attacchi intenzionali sono sempre più sofisticati e difficili da individuare e contrastare, dall'altro che le misure di sicurezza di contrasto in essere **non risultano essere ancora adeguate e sufficienti.**

Si deve tener conto, per quest'ultimo aspetto, dell'enorme numero di piccole e piccolissime organizzazioni in Italia sia in ambito privato che pubblico. Organizzazioni che nella maggior parte dei casi non hanno, e non possono di fatto avere, competenze e sovente capacità economiche per acquisire e gestire gli strumenti di sicurezza digitale, tecnici ed organizzativi, necessari (si veda anche §3.5.1 sul numero di piccole e piccolissime organizzazioni rispondenti). In Italia l'elevatissimo numero di piccole e piccolissime imprese pubbliche e privati, 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.
Questo è confermato analizzando la fig. 4-3 che mostra la distribuzione percentuale degli **attacchi NON subiti** nel 2022 per dimensione (numero di dipendenti) delle aziende/enti dei rispondenti. La percentuale di attacchi non subiti/rilevati è **decrescente** dalle piccolissime organizzazioni con meno di dieci dipendenti alle grandissime con più di 5001. La barra verde indica qualitativamente questo andamento.
Analogamente la fig. 4-4 mette in relazione la distribuzione percentuale degli **attacchi NON subiti** nel 2022 con il fatturato o le entrate per le Pubbliche Amministrazioni (PA) dei rispondenti, e la percentuale di attacchi non subiti/rilevati **decresce** dalle organizzazioni coi fatturati/entrate più bassi a quelle coi più alti, come indicato anche dalla barra verde.
Anche nell'indagine OAD 2023, come nelle precedenti, le organizzazioni più ricche e più note sono quelle che hanno un maggior numero di attacchi, soprattutto di quelli mirati (targeted). Per una corretta interpretazione delle correlazioni elaborate per produrre queste due ultime figure, si deve tener conto che le percentuali emerse dipendono anche dal numero di risposte ricevute.

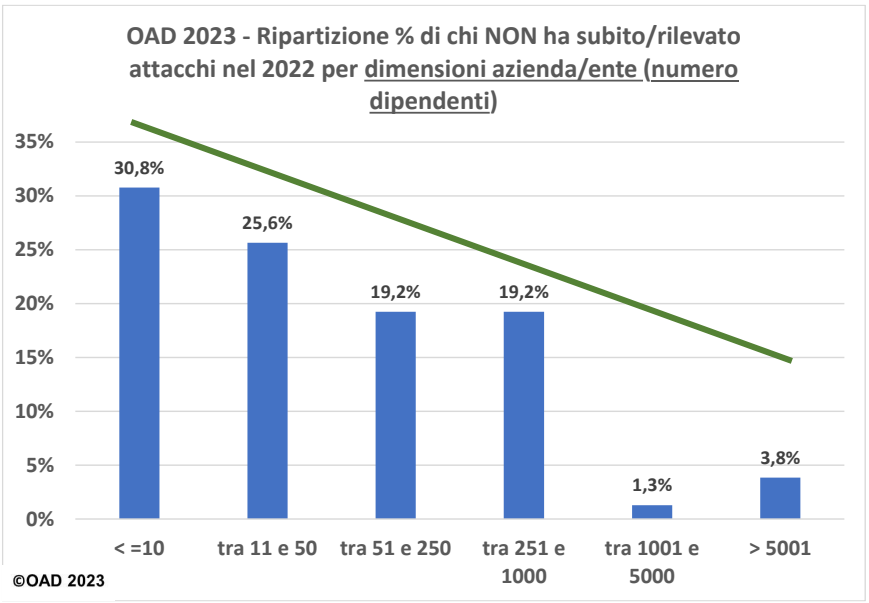


Fig. 4-3

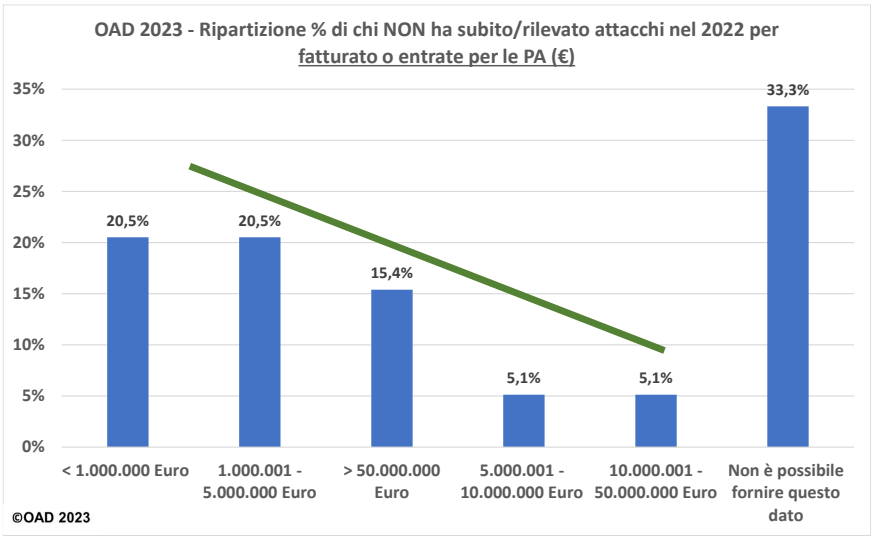


Fig. 4-4

4.1 Tipologie e tecniche di attacco emerse dall'indagine OAD 2023

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 attacco") dal **come si attacca** (indicata come "tecnica di attacco").

L'indagine OAD 2023 ha considerato nel questionario 14 diverse "famiglie di tipologie", dettagliate nell'Allegato A: queste "famiglie" o gruppi di attacco simili, consentono di non chiedere troppi dettagli in merito e semplificare la scelta di chi compila il questionario.

Come diffusione percentuale tra le aziende/enti rispondenti, la fig. 4.1-1 evidenzia al primo posto, con un **29,2%**, le **modifiche malevoli/non autorizzate ai programmi e alle configurazioni dei sistemi ICT**; 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.
Seguono al secondo posto di diffusione, con un **23,5%**, **i sistemi di controllo degli accessi** (IAA, Identificazione-Autenticazione-Autorizzazione), poi con un **19,6%** gli attacchi **DoS/DDoS**, e con un **18,5%** gli **attacchi alle reti** geografiche e locali. Come risulta dalle precedenti edizioni di OAD, queste tipologie di attacco sono quasi sempre ai primi posti come diffusione negli ultimi anni di indagine di OAD.
Nel campione emerso risulta non trascurabile la percentuale, più del 10%, per gli attacchi ai **sistemi OT**, Operational Technology, che includono i sistemi IoT/IIoT, i sistemi di automazione industriale, la robotica. Non trascurabile in quanto i sistemi OT sono tipici per aziende manufatturiere e per quelle attive nel controllo del territorio, quali ad esempio Comuni ed altre PAL, Pubbliche Amministrazioni Locale, e come risulta da fig. 6.2.2, le aziende/enti rispondenti di questi settori sono state relativamente poche.

.

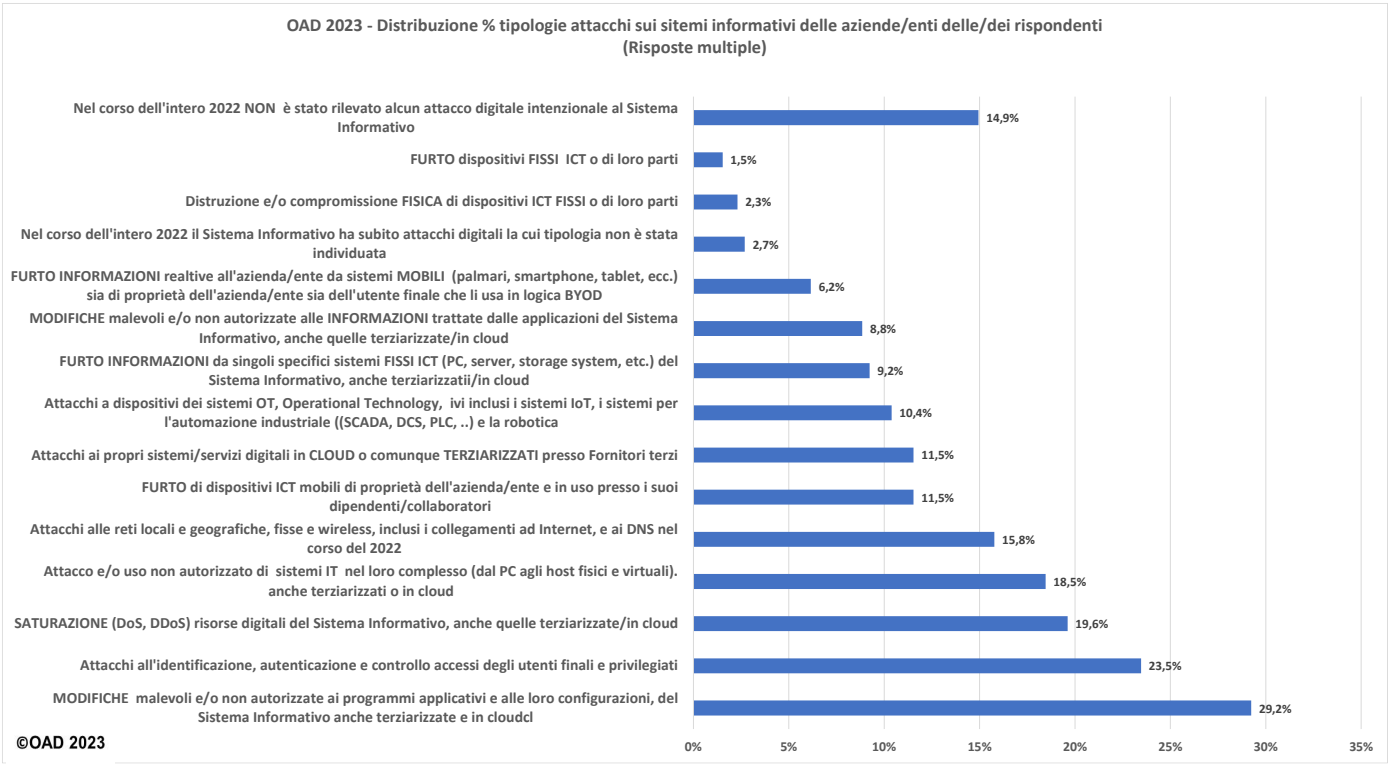


Fig. 4.1-1

La fig. 4.1-2 mostra la **diffusione**, in percentuale, delle **tecniche di attacco** usate nelle diverse tipologie di attacco di cui alla fig. 4.1-1.

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 sistema informativo 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 sistema informativo non si fossero accorti di essere sotto attacco.

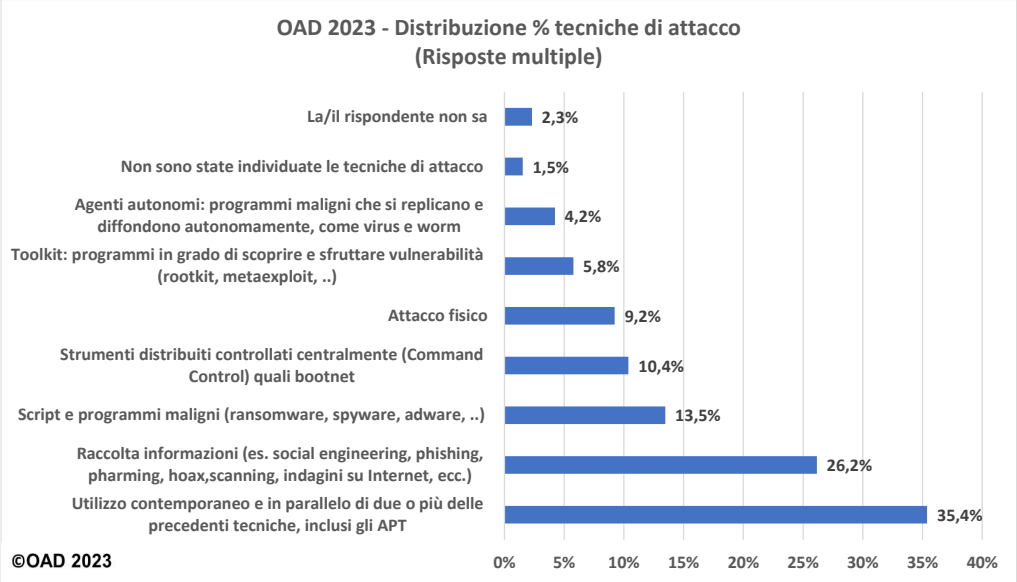


Fig. 4.1-2

Per ciascuna risposta sulla tipologia d'attacco, il questionario permetteva di indicare (opzionalmente) la **frequenza** di quel tipo di attacco nel 2022, indicando come:

- poco frequenti: =< 10 casi nell'anno 2022
- frequenti: >10 e <= 100 casi nell'anno 2022
- molto frequenti: > 100 casi nell'anno 2022

Le risposte avute, e da considerare solo come indicatori di massima, pongono come frequenti/molto frequenti i **malware/ransomware**, e, soprattutto per alcune organizzazioni di grandi dimensioni, il **DoS/DDoS**.

Nello stesso modo, per ogni tipologia di attacco, poteva essere indicato l'impatto per il più grave attacco di quel tipo subito. Le risposte, come per la frequenza di cui sopra, erano da inserire liberamente, secondo la volontà di chi compilava. L'aspetto interessante che emerge dalle indicazioni inserite è che i più gravi attacchi, con impatti significativi, sono stati poco frequenti.

Le fig. 4.1-3 e 4.1-4 mostrano per il 2022 la distribuzione percentuale degli attacchi digitali **non subiti/rilevati** correlata rispettivamente alle **dimensioni delle aziende/enti** rispondenti per numero di dipendenti e **per fatturato/entrate** (questo per le PA) dell'ultimo bilancio disponibile.
Come già indicato in precedenza, per una corretta interpretazione delle correlazioni elaborate per produrre queste due ultime figure, si deve tener conto che le percentuali emerse dipendono anche dal numero di risposte ricevute.
Entrambe le figure evidenziano come le organizzazioni dimensionalmente e finanziariamente **più piccole** sono quelle che hanno subito/rilevato **meno** attacchi digitali. La linea verde nelle due figure evidenzia questo, confermando quanto rilevato anche nelle precedenti indagini OAD: gli attacchi digitali, soprattutto quelli targeted, sono effettuati prevalentemente a organizzazioni di grandi dimensioni 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 sistemi informativi con elevatissimi livelli di sicurezza, che plausibilmente hanno proattivamente respinto e/o scoraggiato effettivi attacchi. Per le misure di sicurezza dei sistemi informativi dei rispondenti si rimanda al Capitolo 7.

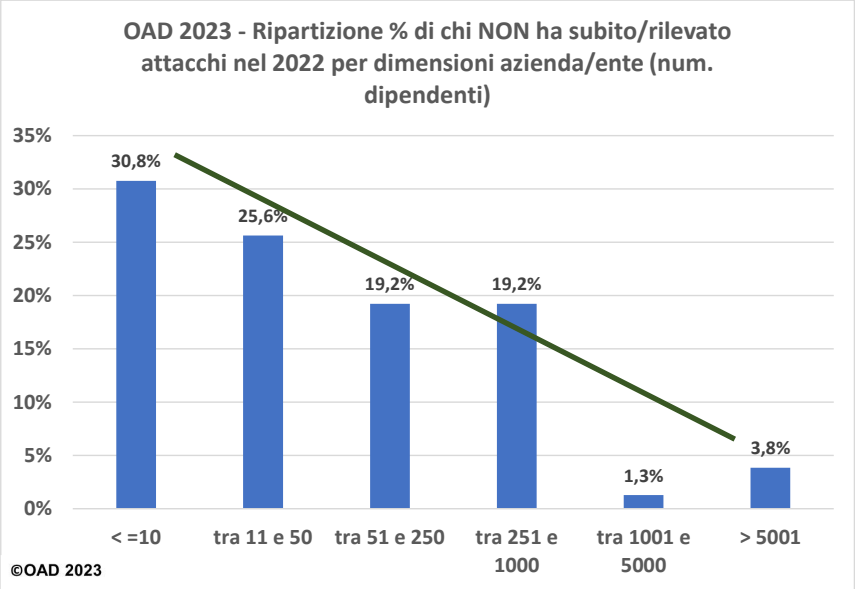


Fig. 4.1-3

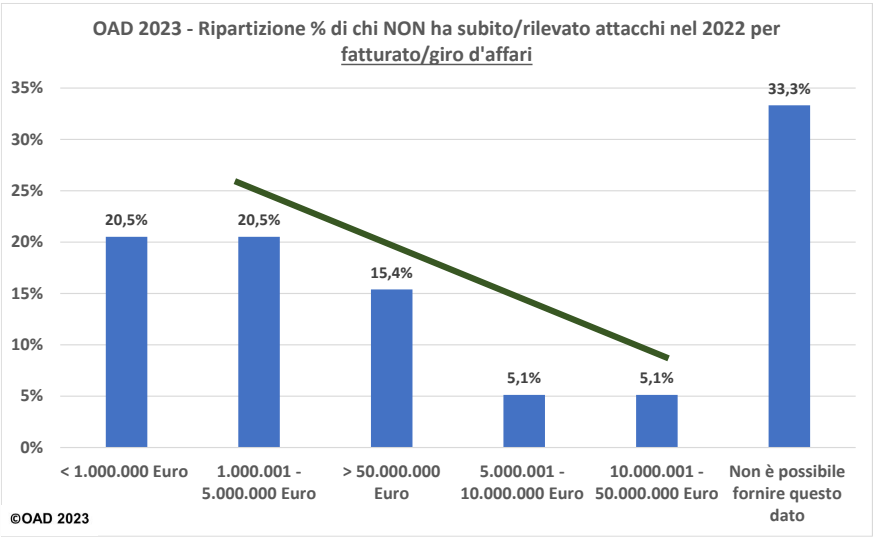


Fig. 4.1-4

4.2 Gli attacchi digitali alle applicazioni ed agli ambienti web in Italia dall'indagine OAD 2023

Come già sottolineato nei precedenti capitoli, l'indagine OAD 2023 è "verticale", focalizzata sugli **attacchi digitali in ambiti web**, che costituiscono ormai nei sistemi informativi la maggior parte degli ambiti applicativi, e per questo motivo attirano gran parte degli attacchi, sia di tipo target sia di tipo massivo, essendo comunque esposte in Internet. Già con OAD 2017[35] era stata effettuata un'indagine "verticalizzata" sugli attacchi agli applicativi, ed OAD 2023 può essere considerata il suo aggiornamento e la sua evoluzione sei anno dopo.

[35] Il Rapporto 2017 OAD è scaricabile gratuitamente, dopo il login, da https://www.oadweb.it/it/rapporti-e-relativi-convegni/2017.html.

Solo per l' "ambito web" il questionario OAD 2023 poneva domande di maggior dettaglio, mentre per tutte le altre tipologie di attacco erano presenti solo due domande, sulla tipologia e sulle tecniche di attacco, con i risultati descritti nel precedente §4.1.

Attacchi alle applicazioni ed agli ambienti **web** sono stati rilevati da quasi i ¾, il **73,1%**, dei rispondenti, e di questi il 54,3% per i propri ambienti web terziarizzati (ambienti terziarizzati che dovrebbe essere, mediamente, più sicuri di quelli on premise), come mostrato nella fig. 4.2-1 a risposte multiple.

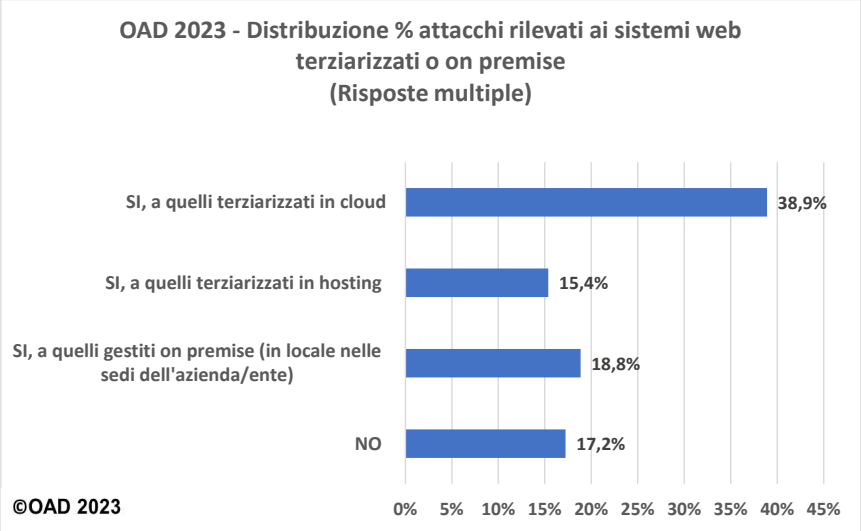


Fig. 4.2-1

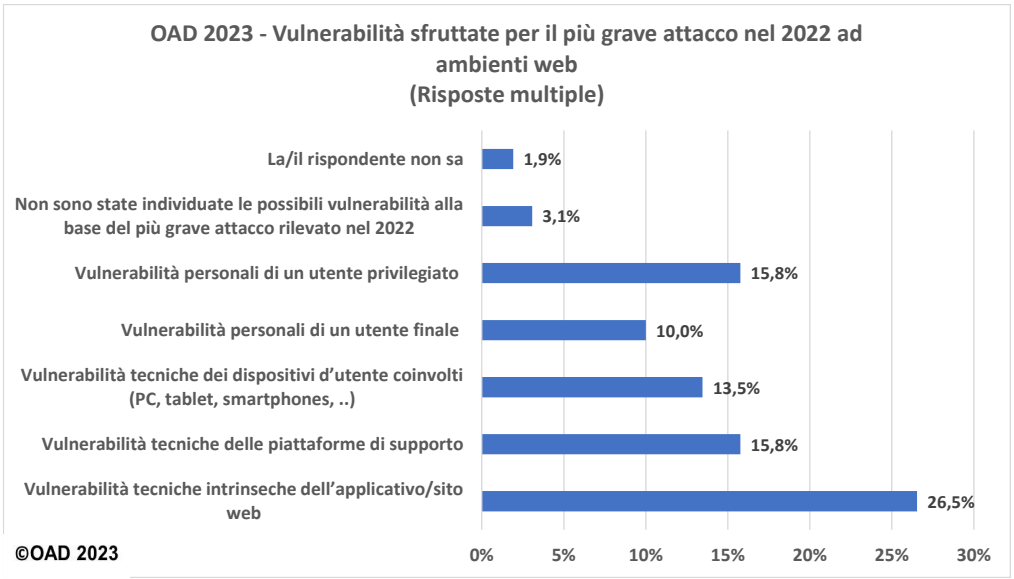


Fig. 4.2-2

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

La fig. 4.2-2 con risposte multiple mostra, per l'attacco più critico rilevato nel 2022, la diffusione in percentuale di quali vulnerabilità siano state, probabilmente, sfruttate. Come già indicato 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 assommano al 55,8%**, ma **quelle personali**, che in parte dipendono anche dall'organizzazione (ad esempio alla non formazione degli utenti sia finali sia privilegiati), **al 25,8%**. Questa indicazione è confermata anche dalle risposte opzionali inerenti tutte le tipologie d'attacco: la cattura di informazioni riservate tramite il social engineering. o il furto di cellulari non protetti, è una delle principali cause di un attacco, e vede, anche se inconsapevole, il coinvolgimento dell'utente. A conferma si veda anche la successiva fig. 4.2-7 sui probabili autori ed attori dell'attacco.

A distanza di sei anni dal precedente Rapporto 2017 OAD sulla sicurezza degli applicativi (web e non), le vulnerabilità intrinseche dell'applicazione web e delle piattaforme su cui poggia rimangono ai primi posti. Un valore assai critico, indicatore che più di ¼ della applicazioni web non sono intrinsecamente sicure e che anche molte piattaforme di supporto a tali applicazioni non sono sufficientemente sicure. Piattaforme che in molti casi sono fornite e gestite dai provider in hosting e/o in cloud.

Sulle **vulnerabilità tecniche degli ambienti web**, OAD ha richiesto un approfondimento nel questionario facendo riferimento alle 10 più diffuse vulnerabilità in ambito web secondo **OWASP**[36] e sempre in riferimento all'attacco più grave e critico rilevato nel 2022.
La tabella in fig. 4.2-3 elenca nell'ordine di diffusione "mondiale" le vulnerabilità Top Ten di OWASP, con una loro breve descrizione ed il link per l'approfondimento.
La fig. 4.2-4 riporta la diffusione percentuale dello sfruttamento (probabile) di queste vulnerabilità nell'attacco più grave agli ambienti web dei sistemi informativi nel bacino emerso dall'indagine 2023. Questa era la domanda più tecnica e da specialisti dell'intero questionario OAD 2023, ma solo l'8,1% ha risposto che non sapeva o che non era stata individuata la vulnerabilità usata.

La vulnerabilità in testa a questa classifica di **diffusione** tra i rispondenti è, con il **19,6%**, **componenti software non aggiornati o obsoleti**. Segue la **progettazione del software insicura**, con il **10,8%**, e **l'errata configurazione** degli strumenti di sicurezza. Seguono, a scalare e sotto il 10%, le altre vulnerabilità della top-ten. Significativo il **11,2%** che non ritiene nessuna di queste vulnerabilità la causa dell'attacco più grave: ad esempio un attacco DDoS per essere lanciato non ha bisogno di alcuna vulnerabilità nel software del web e della sua piattaforma, ma solo la mancanza di strumenti a livello delle connessioni Internet per bloccare o dirottare l'enorme flusso di dati che satura le linee.

Nel complesso le risposte avute a questa "difficile" domanda del questionario sono ragionevoli, per l'autore, considerando la realtà dei siti web anche di grandi organizzazioni, pubbliche e private.
Molti siti/applicazioni web sono mal progettati, senza o con poche misure di sicurezza; il forte utilizzo in questo contesto di software opensource porta sovente all'utilizzo di moduli e componenti totalmente obsoleti.
Dal cattivo progetto deriva in molti casi anche la cattiva configurazione dell'intero ambiente, e soprattutto degli strumenti di sicurezza, che sono lasciati di default per la fretta e/o per la loro non conoscenza; ed il default il più delle volte coincide con misure di sicurezza non attivate.

[36] OWASP, xxxxx (https://owasp.org/www-project-top-ten/),

Nome vulnerabilità	Breve spiegazione	Riferimento OSWAP
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. 4.2-3 (Fonte: OWASP)

Le fig. 4.2-5 e 4.2-6 fornisco precise ed interessanti informazioni sull'impatto tecnico, in termini di disservizio causato, e sull'impatto economico (qualitativo) dell'attacco più critico rilevato nel 2022 in ambito web.

L'**impatto** dell'attacco più grave è stato **pesante** per i sistemi informativi delle aziende/enti rispondenti, con il **73,6%** dei casi con un disservizio durato **da 2 giorni in su**, e con il **48,1%** che ha visto un significativo aumento dei costi a livello di **budget del sistema informativo**, ed il **24%** che ha visto questo costi ripercuotersi, anche fortemente, **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 hanno causato forti problemi alla funzionalità del sistema informativo attaccato, con i conseguenti costi diretti ed indiretti**.

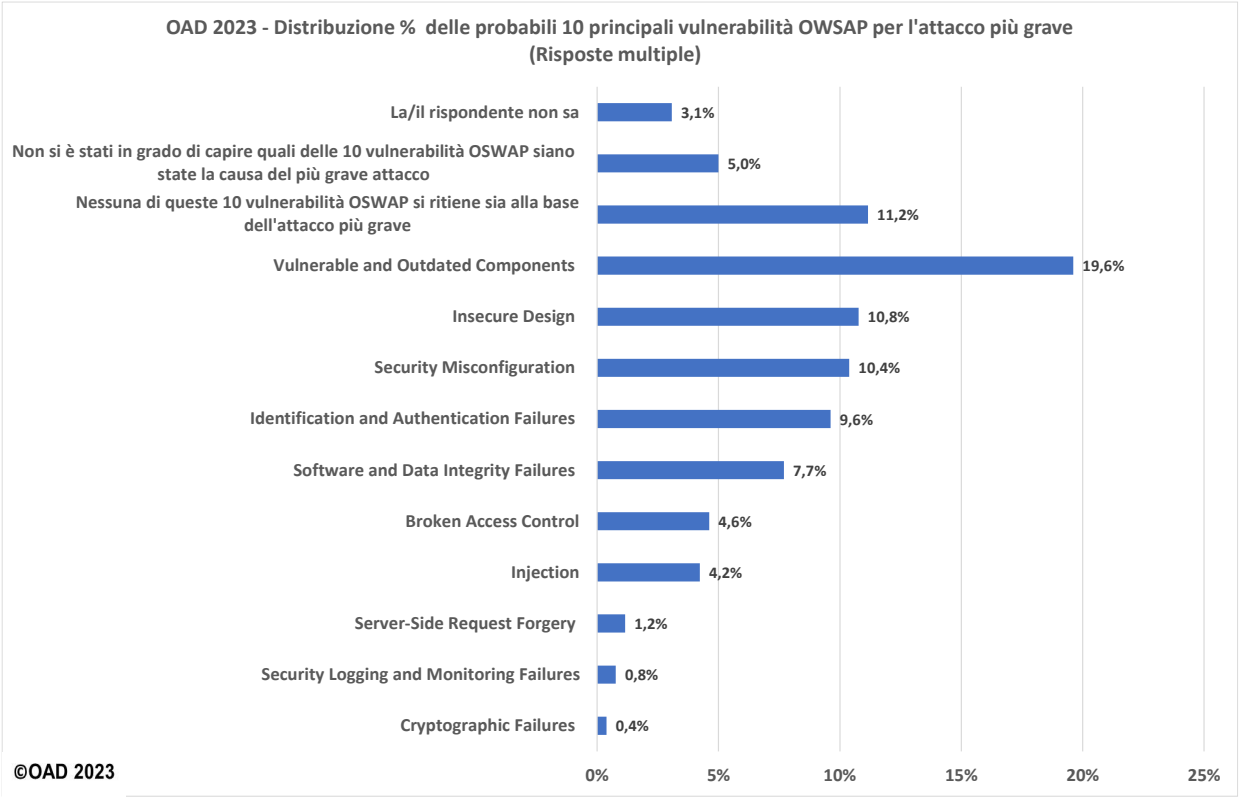


Fig. 4.2-4

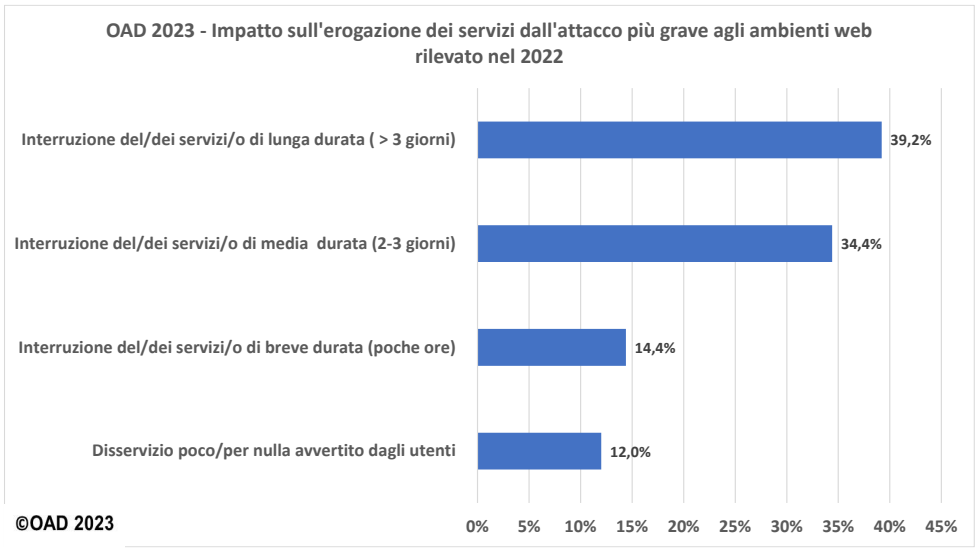


Fig. 4.2-5

La fig. 4.2-7 mostra, con risposte multiple, la distribuzione percentuale delle **possibili motivazioni per l'attacco più grave** sui siti e sulle applicazioni web del sistema informativo: i prime tre, con percentuali abbastanza vicine a decrescere , sono **la frode, il sabotaggio, il ricatto**. Il primo ed il terzo sono quasi ovvi, con un'alta percentuale sul ricatto dovuto principalmente alla larga diffusione di ransomware in Italia.

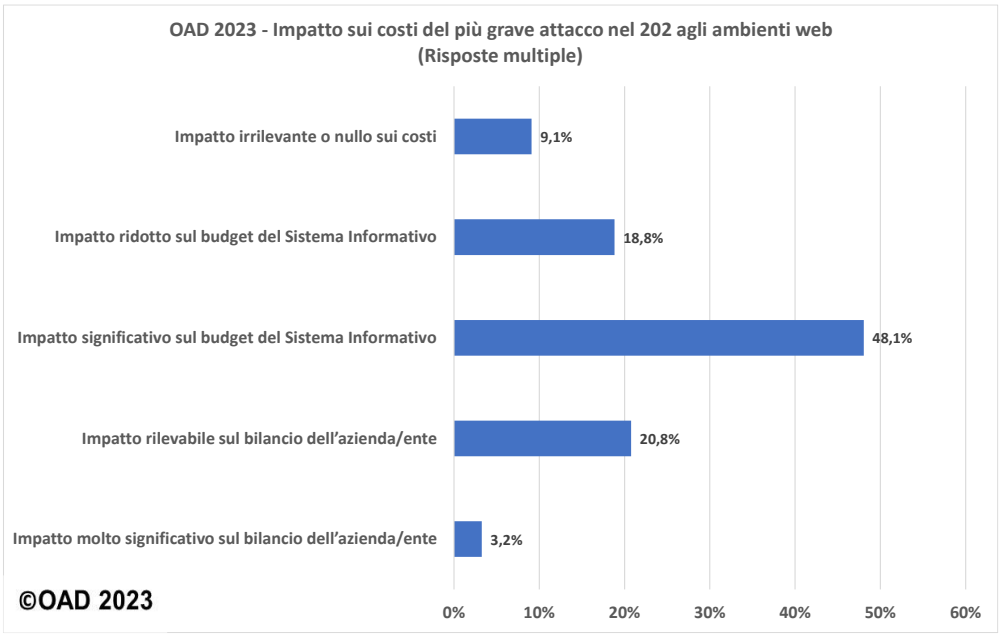


Fig. 4.2-6

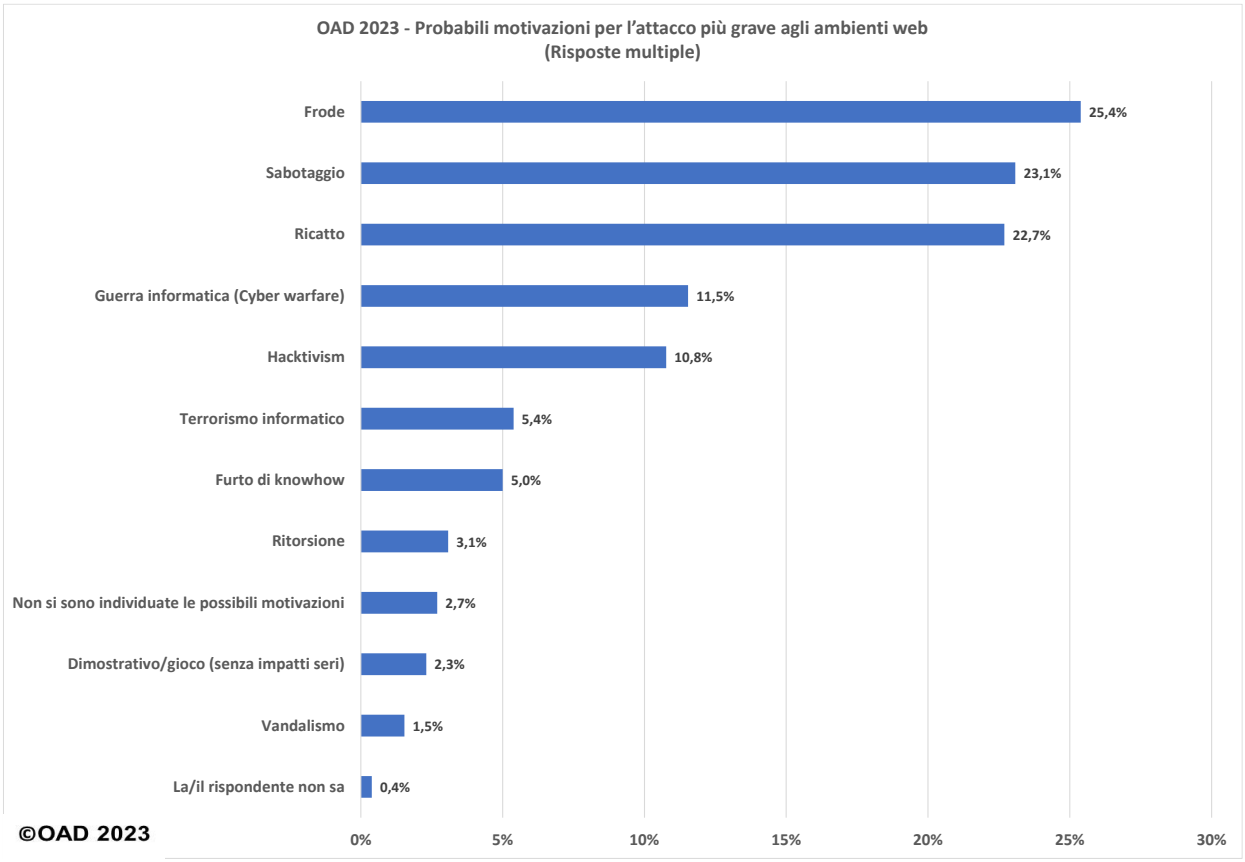


Fig. 4.2-7

A prima vista stupiscono percentuali così alte per il sabotaggio. Per l'autore anche questo dato è molto ragionevole, quasi ovvio: i 2/3 delle organizzazioni rispondenti sono al di sotto di 250 dipendenti, quindi PMI per le aziende private, come riportato in fig. 6.2-4; un attacco grave per queste organizzazioni comporta il più delle volte un disservizio informatico tale da ridurre, se non bloccare, l'operatività dell'intera azienda/ente. Potendo scegliere più risposte, molti che hanno selezionato frode e ricatto, hanno anche selezionato sabotaggio.

I **probabili attaccanti per l'attacco più grave** nel 2022 sono mostrati in fig. 4.2-8, con risposte multiple. **L'attacco dall'esterno** è stato selezionato da circa 1/3 dei rispondenti, tutti gli altri attori hanno percentuali molto inferiori. Al secondo ed al terzo posto si collocano gli ex dipendenti ed i dipendenti a tempo indeterminato, in pratica gli "ex" e gli attuali utenti del sistema informativo oggetto dell'attacco.
Nella maggior parte degli attacchi gravi, **l'attore è sconosciuto e operante da Internet**, ma in alcuni casi è aiutato, involontariamente, da utenti del sistema informativo bersaglio con i loro comportamenti, quali ad esempio aprire email di phishing, attivare gli allegati malevoli, inserire dati riservati e confidenziali nei social e/o nei form di siti malevoli, usare password deboli, comunicare il proprio account ad un collega, e così via.
E' opportuno evidenziare che solo il 6,2% non è stato in grado di determinare la provenienza dell'attacco.

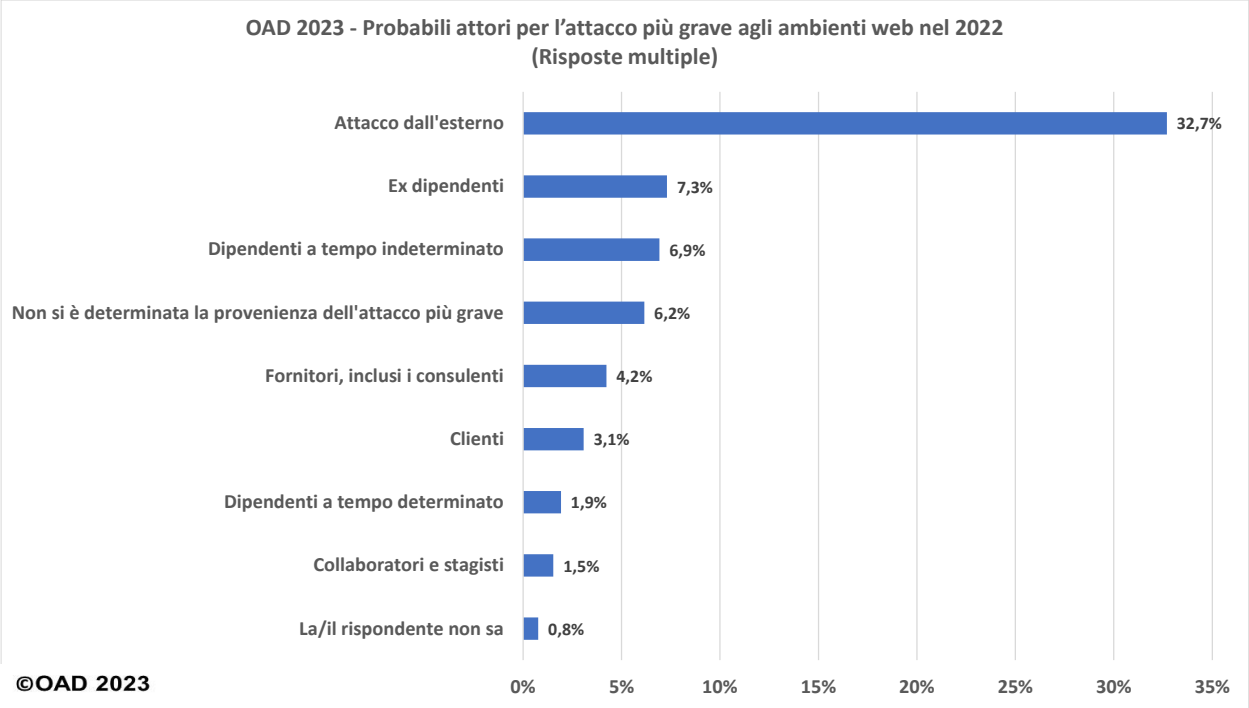


Fig. 4.2-8

Percentuale molto più bassa di quella rilevata nelle precedenti indagini OAD, il che evidenzia, anche, come sia aumentata la consapevolezza del fenomeno attacchi digitali in Italia.

La fig. 4.2-9, con risposte multiple, mostra la distribuzione percentuale, nel bacino dei rispondenti, **dell'ente interlocutore esterno cui 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. La maggior parte comunica l'accaduto ai propri fornitori e consulenti per farsi aiutare nel ripristinare la situazione ex ante, e con percentuali assai inferiori alle autorità preposte: a conferma, si veda la fig. 4.2-10 sulle azioni svolte dopo aver subito un (il più) grave attacco negli ambienti web.

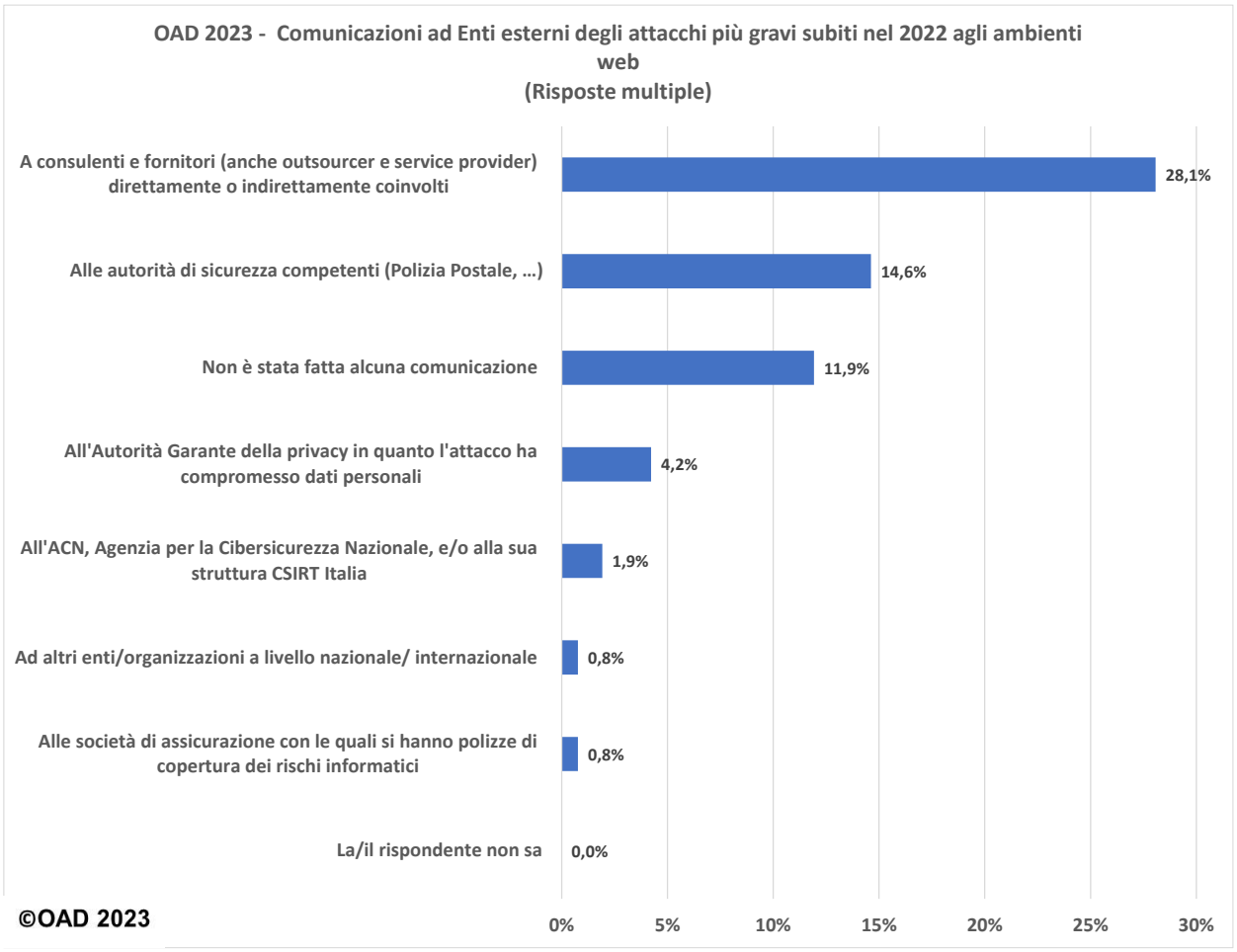


Fig. 4.2-9

Quasi il 12 % non comunica nulla a nessuno, e la fig. 4.2-10, con risposte multiple, **indica le ragioni della non comunicazione**: il 71% perché anche il più grave attacco rilevato non è così significativo e non rientra tra quelli che per legge devono essere comunicati. Un'ulteriore alta percentuale, 64,5%, teme che comunicare l'attacco in ogni modo comprometta la sua immagine. In molti settori merceologici, ed anche nelle PA, e nella mente di molti top manager, l'aver subito un attacco informatico è un'onta, fa presupporre 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. Le altre possibili motivazioni raccolgono percentuali irrisorie.

La fig. 4.2-11, con risposte multiple, indica, in percentuale, la diffusione delle **principali attività dopo aver subito il più grave attacco ad ambienti web**. Al primo posto, con un 71%, l'implementazione di nuovi strumenti di sicurezza digitali, che causano l'aumento dei costi sul budget informatico di cui in fig. 4.2-5. Seguono a decrescere ma con percentuali significative, altri interventi sul sistema informativo, quali la sostituzione delle risorse ICT vulnerabili, gli aggiornamenti, etc.
Colpisce il valore veramente basso sui corsi di formazione, che conferma l'annoso problema delle competenze degli utenti, molto meno quello, tendente a zero, dell'assicurazione sui rischi informatici: polizze assicurative ce ne sono, ma difficili da "configurare" ed ancora con costi troppo alti per le medie e piccole organizzazioni.

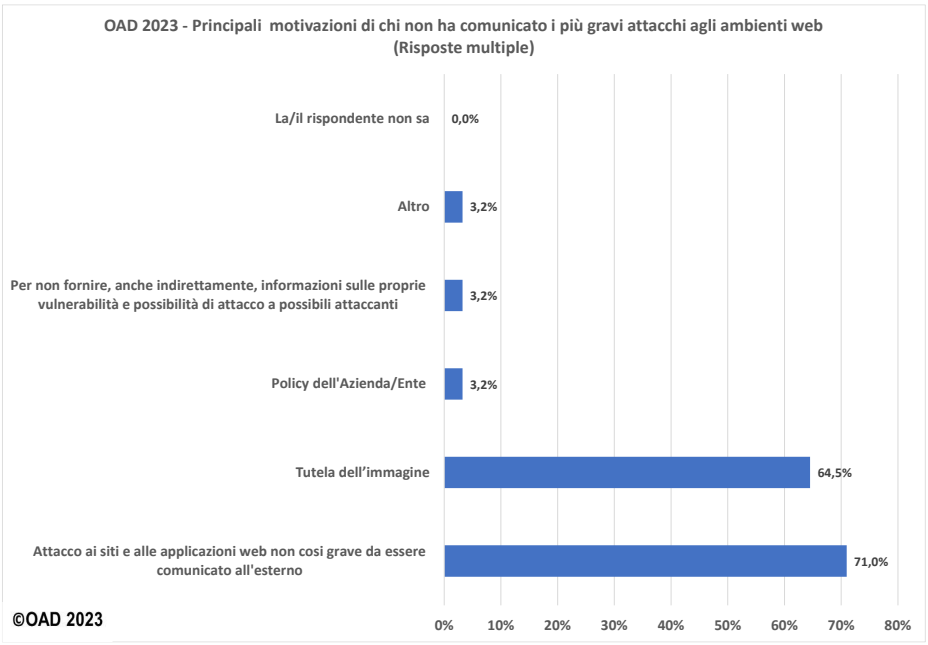


Fig. 4.2-10

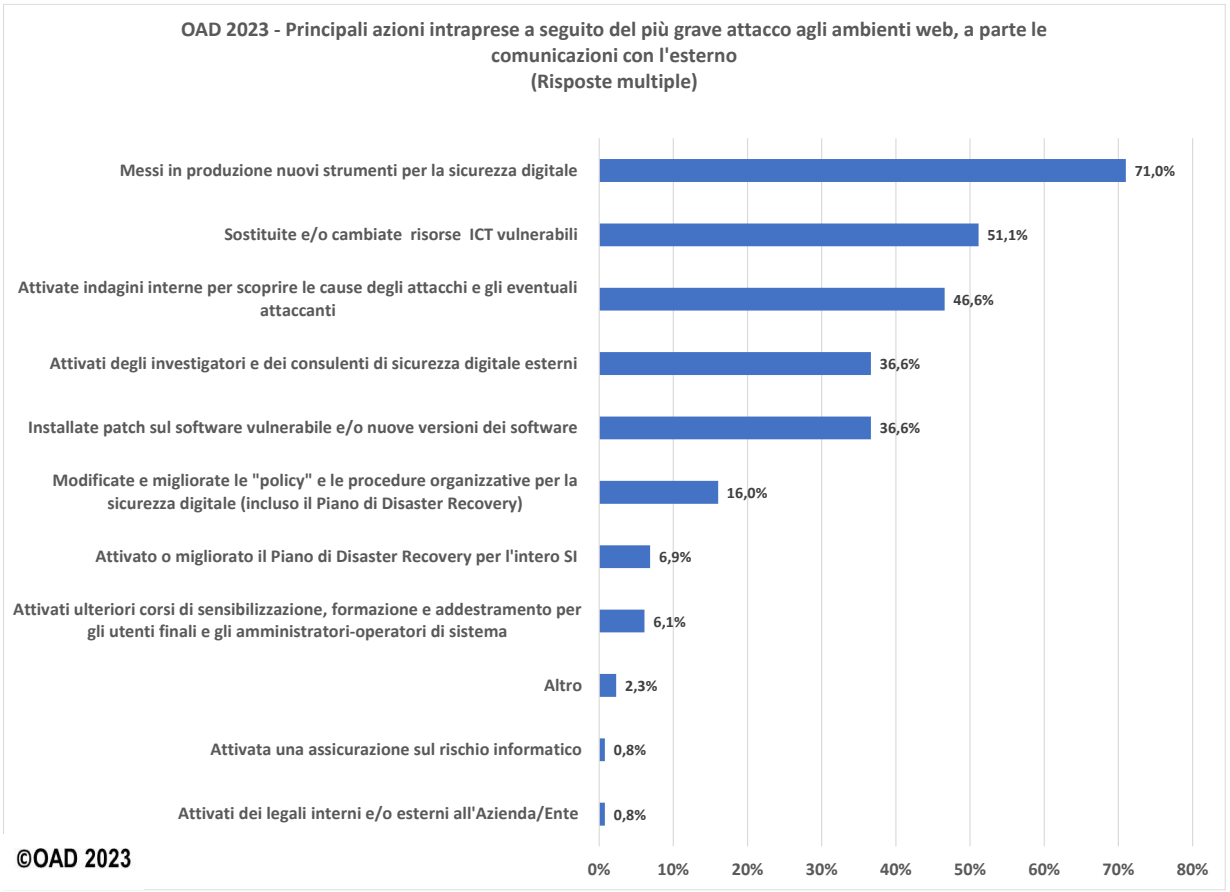


Fig. 4.2-11

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

Come indicato nel questionario online, come "prossimo" futuro è considerato la fine del 2023 ed i successivi anni 2024 e 2025.
La fig. 5-1, con risposte multiple, mostra che per più della metà delle aziende/enti rispondenti, **51,9%**, la tipologia di attacco più temuta nel prossimo futuro è data dalle "**Modifiche non autorizzate ai dati e alle informazioni trattate dal sistema informativo**": il timore di manipolazioni errate e malevoli delle informazioni che costituiscono uno dei principali asset dell'azienda/ente. Al secondo posto si posizionano, con il **47,7%**, le "**Modifiche non autorizzate ai programmi applicativi e di sistema, e alle configurazioni**", cui ha contribuito la larga diffusione in Italia di ransomware, e segue poi, con il **45%**, il più generale "**Uso non autorizzato di risorse ICT**".

Queste tre tipologie d'attacco sono le più temute, ciascuna con una percentuale tra il 45% ed il 51%. Seguono nella fascia percentuale del 33%, quindi di circa 1/3 delle risposte, il DDoS e gli attacchi ai sistemi di controllo degli accessi ai sistemi ICT.

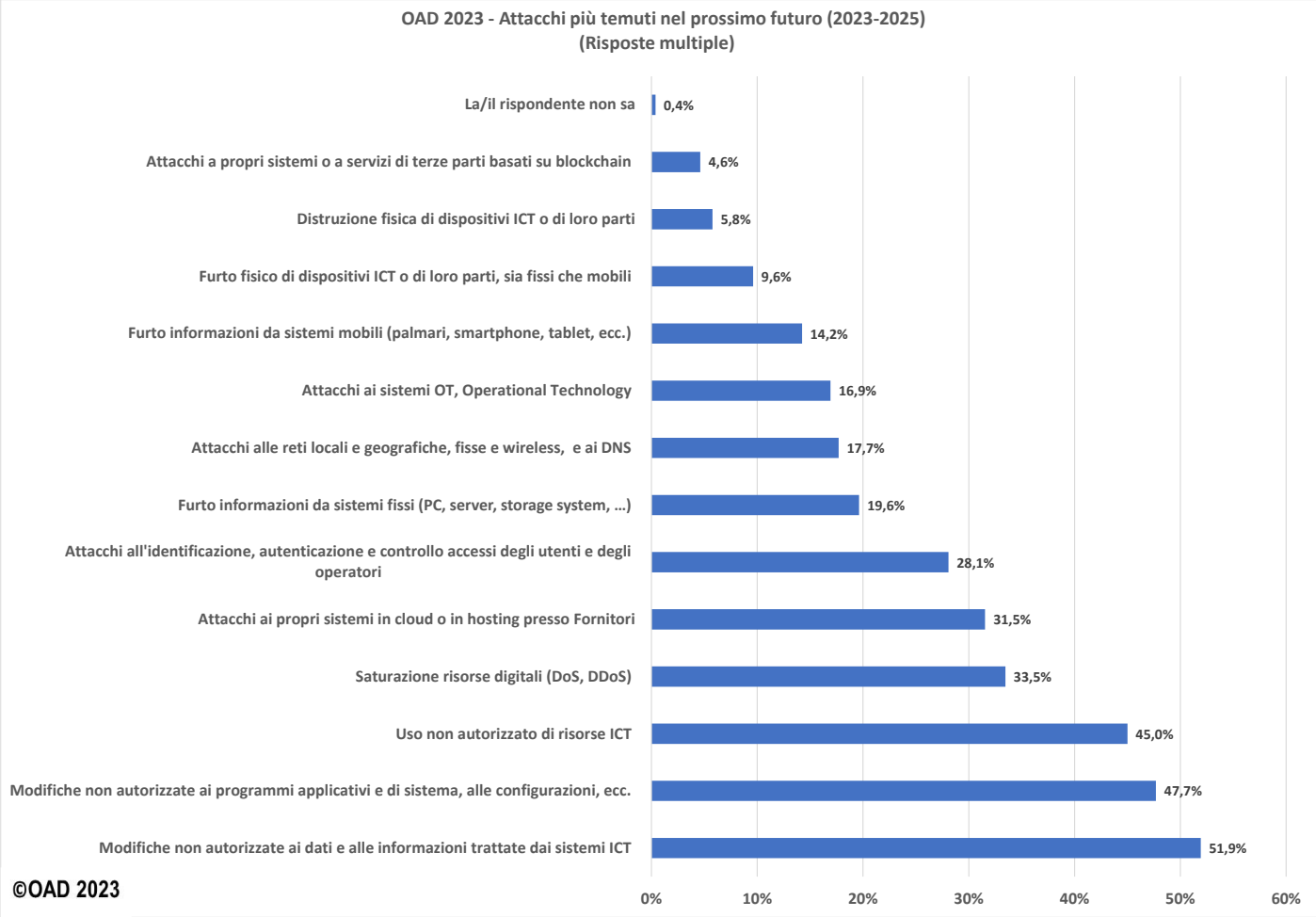


Fig. 5-1

Una terza fascia, tra il 10 ed il 20%, include il furto di informazioni da sistemi fissi e mobili, gli attacchi alle reti e gli attacchi ai sistemi OT, nei quali sono considerati i sistemi IoT/IIoT, l'automazione industriale, i robot.

Nella fascia sotto il 10% le altre 3 tipologie d'attacco. La bassa percentuale di timori sugli attacchi ai sistemi con blockchain sicuramente deriva dal fatto che ben poche della aziende/enti rispondenti utilizzano tale tecnica.

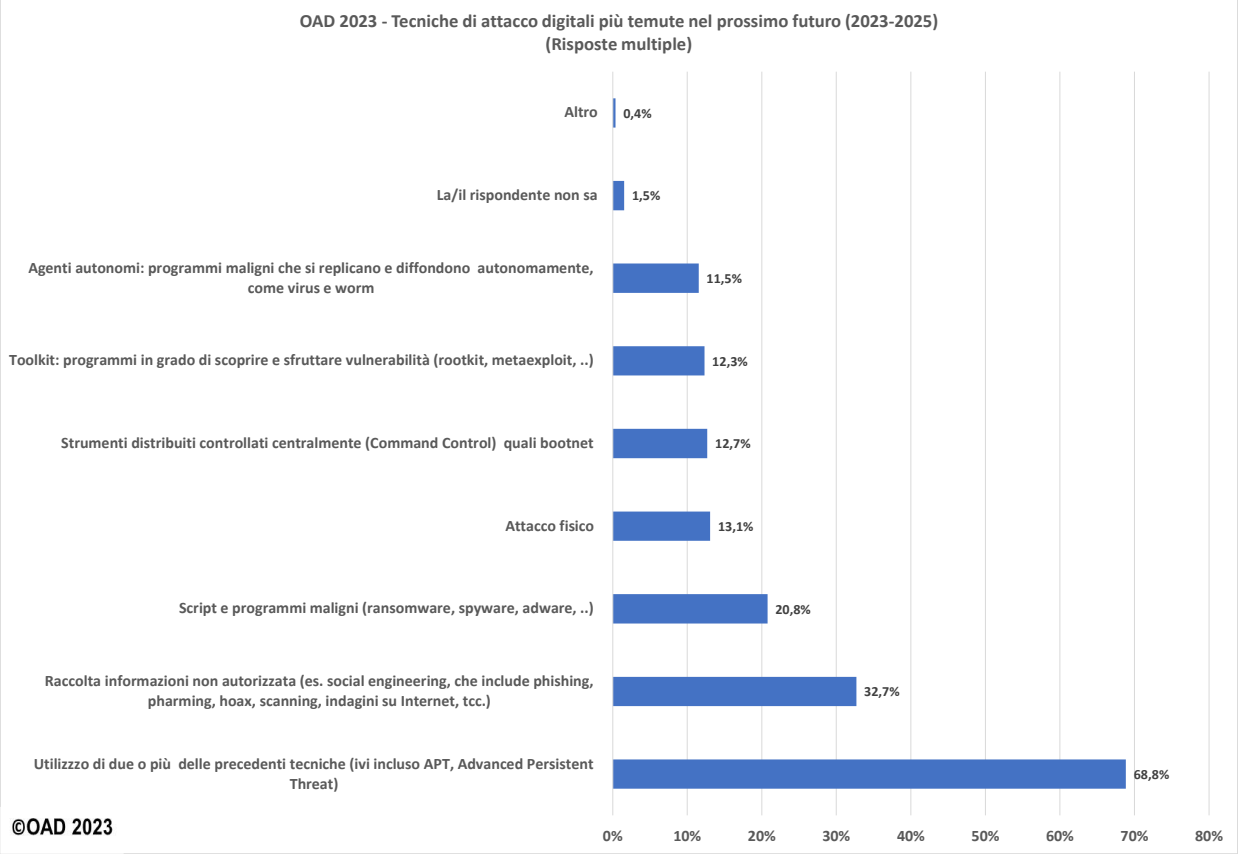


Fig. 5-2

La fig. 5-2, con risposte multiple, mostra le famiglie di tecniche per gli attacchi digitali più temute per il prossimo futuro. Con una altissima percentuale, quasi il **70%**, al primo posto "l'utilizzo di più tecniche", come ormai avviene per la maggior parte degli attacchi digitali. Al secondo posto, con **32,7%**, quasi la metà dei punti percentuali della prima "in classifica", ma che rappresentano circa 1/3 dei rispondenti, il **social engineering**, che costituisce una dei principali entry point per un attacco. Al terzo posto, con un **20,8%**, l'uso di script e di programmi maligni, nei quali rientrano i malware e ransomware. Queste famiglie di tecniche d'attacco ai primi 3 posti tra quelle più temute nel prossimo futuro sono le stesse, e nello stesso ordine pur con percentuali diverse, di quelle rilevate per tutti gli attacchi digitali nel 2022, si veda fig. 4.1-2. Seguono a scalare, ma con diversi punti percentuali di differenza, le altre famiglie di tecniche considerate.

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**, per più dei 3/4, seguite per più della metà dal **sabotaggio**. Prima del ricatto, tipico del ransomware assai diffuso in Italia, in questa indagine 2023 si trovano **l'attivismo** e la **guerra informatica,** quest'ultima causata dal protrarsi della guerra tra Ucraina e Federazione Russa, e dall'aumento delle tensioni geopolitiche tra il mondo occidentale liberale ed il resto del mondo.
Confrontando le motivazioni per i futuri attacchi più temuti, sintetizzati nella fig. 5-3, con le motivazioni probabili per gli attacchi subiti nel 2022 negli ambiti web della fig. 4.2-6, si nota che le prime due motivazioni sono le medesime, pur con percentuali diverse, ma per gli attacchi subiti il ricatto si posiziona al terzo posto, precedendo l'attivismo e la guerra informatica. Questo indica che per il futuro le aziende/enti rispondenti sanno come contrastare il ransomware, ma sono ben più preoccupati da attacchi ancor più pericolosi e devastanti causati dall'Hacktivism (che talvolta sconfina nel

fanatismo) e dalle guerre informatiche attuate non (solo) da gruppi criminali ma anche da ben organizzate e potenti strutture degli stati coinvolti.

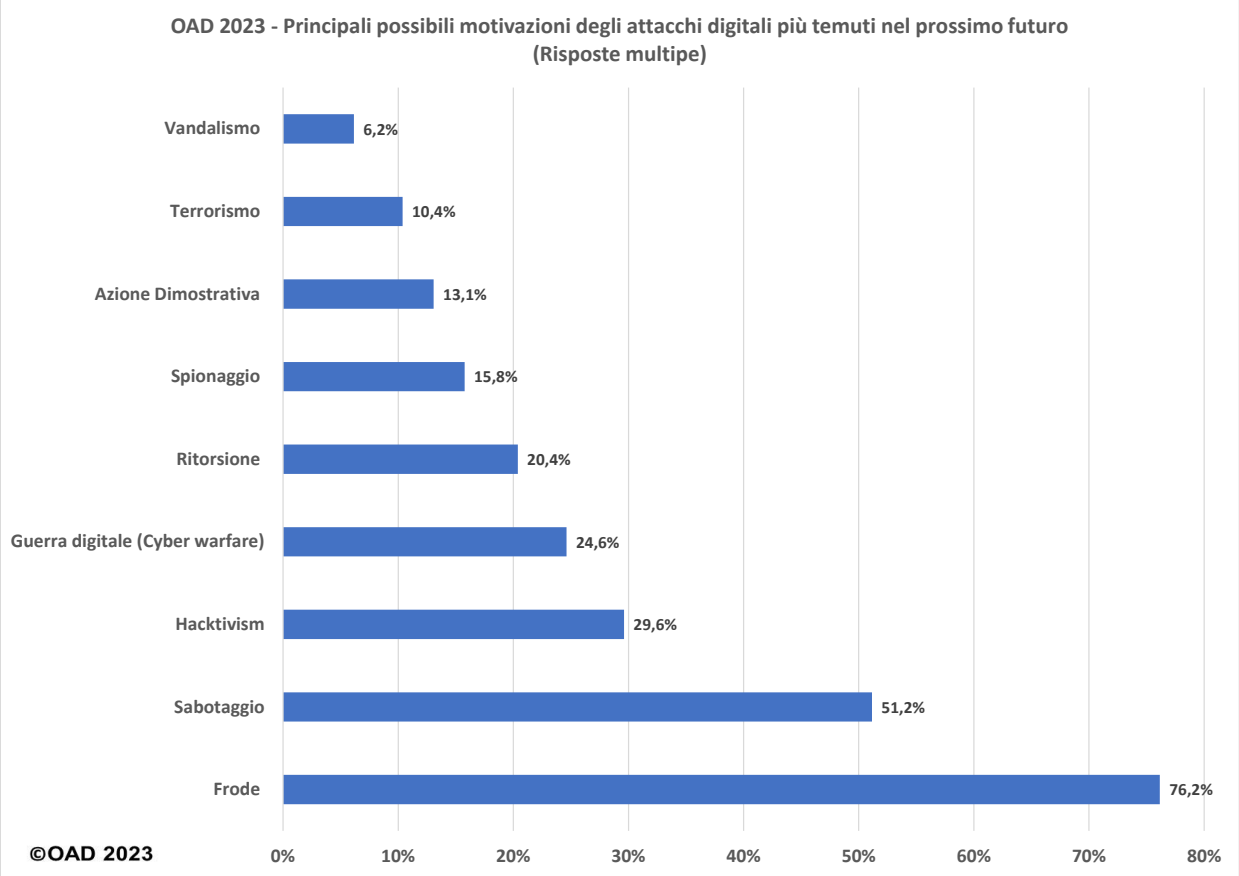


Fig. 5-3

A giudizio dell'autore la percentuale di circa ¼ dei rispondenti per la guerra digitale potrebbe essere più alta se all'indagine 2023 avessero partecipato in misura maggiore enti finanziari, aziende della sanità e pubbliche amministrazioni, che costituiscono un target proprio per la cyber warfare.

6. Il campione delle aziende/enti rispondenti e dei loro sistemi informativi emerso dall'indagine OAD 2023

Il presente capitolo fornisce una macro descrizione dei sistemi informativi 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 sistemi informativi dei rispondenti sono analizzate in §7.

6.1 Tipologia, ruolo e principali caratteristiche dei sistemi informativi delle aziende/enti rispondenti

La fig. 6.1-1 mostra che il sistema informativo di più della metà delle risposte, il 53,8%, è di piccole-medie dimensioni, non ha un Data Center, ed è gestito e controllato totalmente in Italia. Questa è la caratteristica tipica di un sistema informativo di una piccola o media organizzazione, che come evidenziato nel Capitolo 3, costituiscono la stragrande maggioranza in Italia.

Una delle caratteristiche di valore dell'indagine OAD è il coinvolgimento nel rispondere al questionario online delle piccolissime e piccole realtà italiane, che non sono normalmente oggetto di indagine da parte di molte altre indagini sia in Italia sia all'estero. Al secondo posto, ma con meno della metà percentuale del primo, il 19,1%, sistemi informativi di medio-grandi dimensioni con almeno un Data Center totalmente gestito in Italia. Per il 23,5% il sistema informativo è di grandi dimensioni, con più Data Center in Italia in altre nazioni, a supporto il più delle volte per una multinazionale: di questi il 13,3% è gestito e controllato dall'Italia. L'ultimo posto spetta a sistemi informativi di piccole-medie dimensioni in Italia, ma controllati dall'estero: è il tipico caso di filiali italiane di aziende straniere, che in Italia hanno sistemi ICT in logica dipartimentale. Dall'indagine emerge che ben l'86,2% dei sistemi informativi dei rispondenti, con almeno alcune parti operanti in Italia, sono controllati e gestiti in Italia.

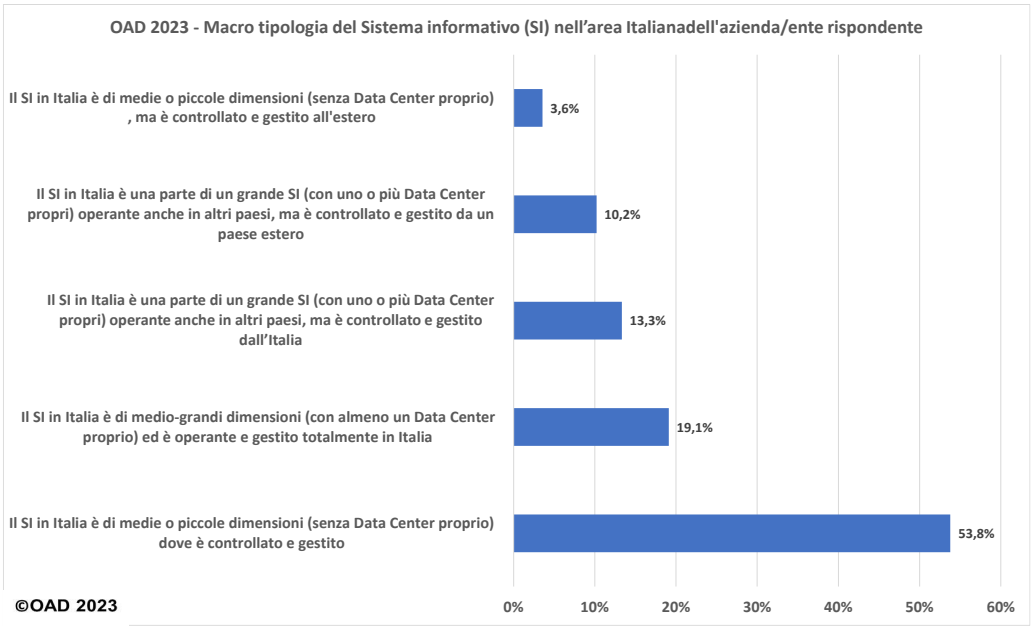


Fig. 6.1-1

La fig. 6.1-2 mostra, come distribuzione percentuale delle risposte avute, dove è situata a livello regionale la parte più significativa del sistema informativo in Italia, sia essa un Data Center o una computer room "primaria". Grazie ai vari e ripetuti solleciti di AIPSI, l'indagine OAD 2023 è riuscita a coprire tutte le regioni d'Italia, ma la maggior diffusione delle aziende/enti rispondenti è in Lombardia e Lazio.

Per meglio comprendere il fabbisogno di sicurezza digitale per il sistema informativo oggetto delle risposte, l'indagine OAD cerca di conoscere, almeno a livello qualitativo, quale è la sua strategicità per il business e per le attività dell'azienda/ente rispondente. La fig. 6.1-3 risponde a questa domanda ed evidenzia che per i 2/3 delle aziende/enti il sistema informativo 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. Solo per il 4,5% il sistema informativo è di mero "supporto" all'operatività dell'azienda/ente, e questo anche se il 67% delle organizzazioni rispondenti sono di piccole e medie dimensioni, si veda successiva fig. 6.2-4.
Un'altra caratteristica importante per la sicurezza digitale di un sistema informativo è se tratta dati personali, e quindi deve soddisfare obbligatoriamente ai requisiti del GDPR, e soprattutto se tratta dati personali "sensibili"[37]. La fig. 6.1-4 evidenzia che quasi tutti i sistemi informativi trattano dati personali, come quelli dei dipendenti, dei collaboratori, dei clienti, dei fornitori, dei consulenti, etc., ed il 38,6% di questi dati sensibili. L'1,3% dichiara di non trattare nel proprio sistema informativo dati personali, ma per l'autore questo è un errore dovuto alla non conoscenza dell'argomento da parte di chi ha compilato il questionario.
I dati personali non sono le uniche informazioni critiche trattate dalle applicazioni di un sistema informativo: si pensi ad esempio ai piani di sviluppo, ai segreti industriali, all'elenco dei clienti e dei fornitori con le condizioni di vendita ed acquisto, a dati di ricerca essenziali per l'innovazione e la competitività, e così via.
Il tema delle informazioni critiche si allaccia a quello delle infrastrutture "critiche" che forniscono servizi essenziali per il funzionamento di un intero paese. L'Unione Europea, nell'obbiettivo di potenziare ed omogeneizzare la sicurezza digitale dell'intera Unione, ha emanato una serie di normative, dal NIS/NIS2 a DORA, CER, etc., trattate in §3.4, che varie aziende ed enti pubblici dovranno seguire ed implementare, per garantire in ogni paese dell'Unione i più elevati livelli di sicurezza e segretezza digitale. Queste direttive e regolamenti europei specificano quali sono i sistemi informativi oggetto della normativa, così da non lasciare spazio all'interpretazione personale o di convenienza delle aziende/enti.
La fig. 6.1-5 mostra percentualmente quanti dei sistemi informativi dei rispondenti trattano informazioni altamente riservate e critiche, oltre a quelle personali soggette alla normativa sulla privacy, e che come tali richiedono un elevato livello di riservatezza e di protezione digitale. Il 43% dei sistemi informativi tratta informazioni critiche e riservate, e di questi il 13,1% gestiscono infrastrutture critiche e/o forniscono servizi essenziali per l'Italia, e rientrano tra i sistemi informativi oggetto delle nuove normative europee indicate in §3.4. Per l'autore questa percentuale è bassa, considerando il numero di aziende/enti rispondenti ad OAD 2023 che per il loro settore merceologico e per la loro attività dovrebbero rientrare in questa categoria: ma probabilmente chi rispondeva al questionario non era a conoscenza delle nuove normative europee.
La maggioranza delle aziende/enti rispondenti, il 57%, tratta informazioni necessarie al loro funzionamento, ma non ritenute molto critiche. Al di là del riferimento a NIS/NIS2, il questionario OAD 2023 lasciava libero il compilatore nella valutazione sul livello di criticità dei dati.

[37] Nel GDPR non si fa più riferimento al termine sintetico di dato "sensibile", come nelle precedenti direttive sulla privacy, per indicare dati personali sanitari, su orientamento politico, sindacale, religioso, filosofico, e così via. Per comodità di sintesi viene comunque usato nel presente Rapporto.

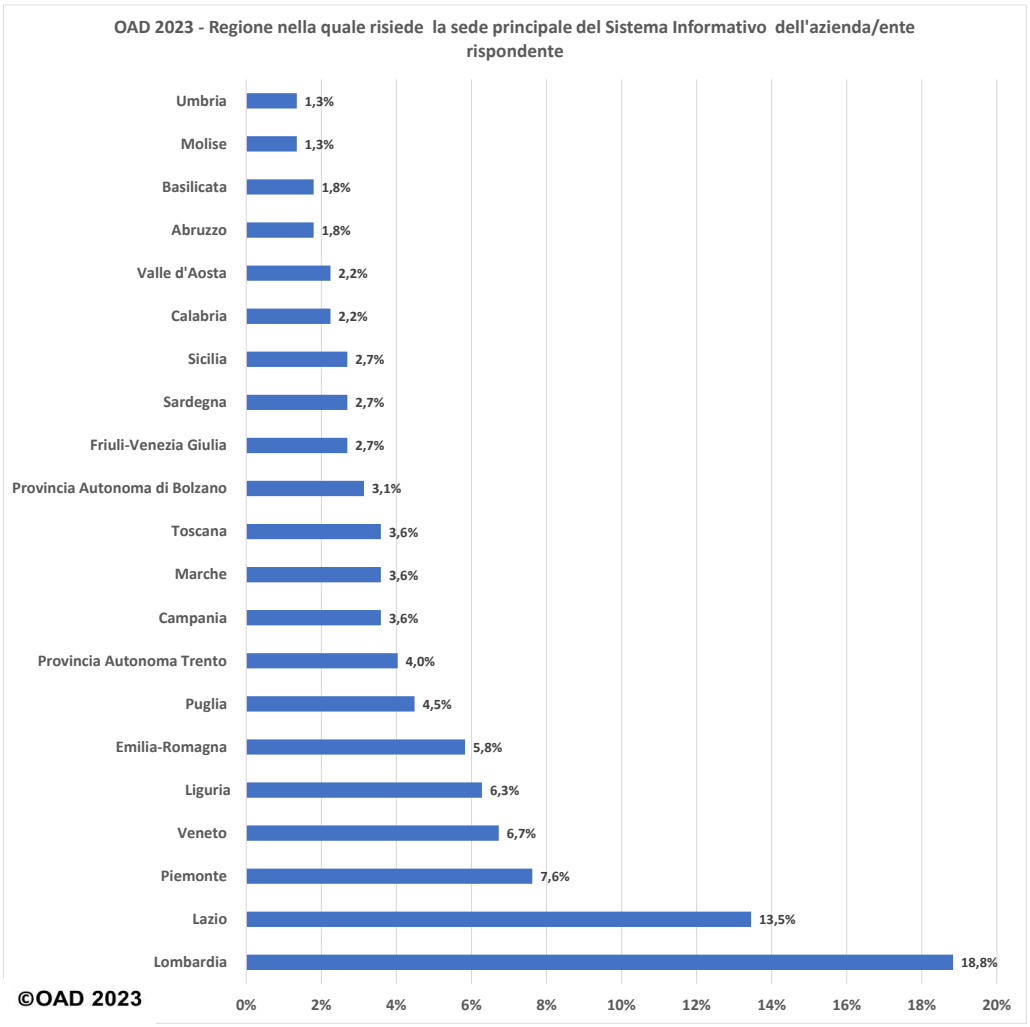


Fig. 6.1-2

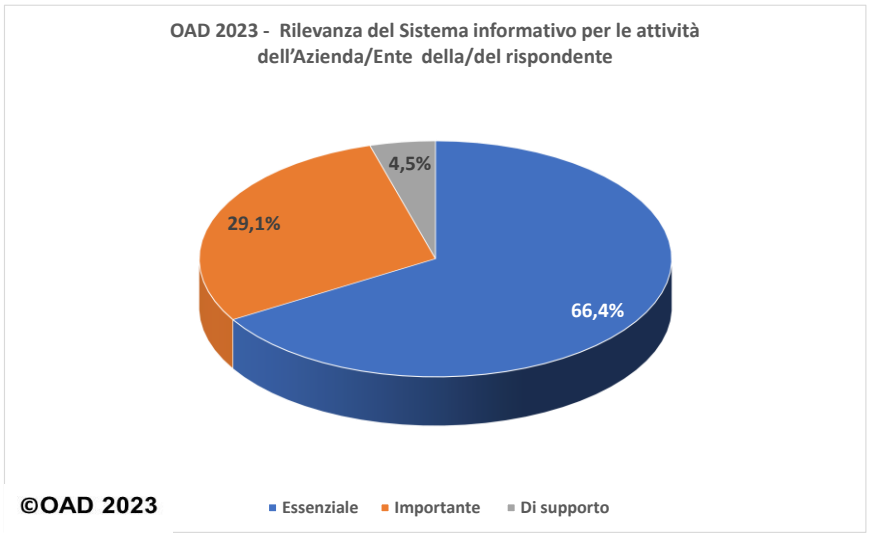


Fig. 6.1-3

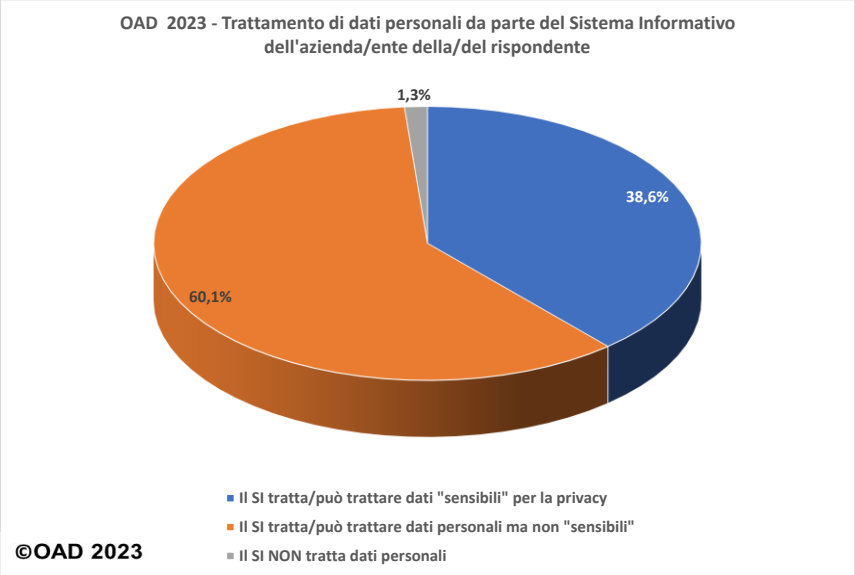


Fig. 6.1-4

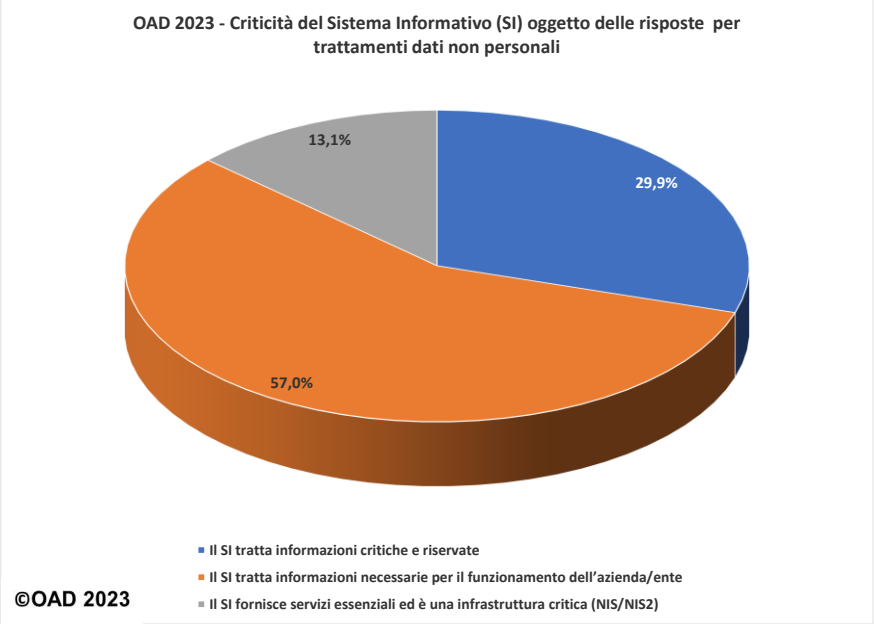


Fig. 6.1-5

Come evidenziato nella fig. 6.1-6, la quasi totalità dei sistemi informativi dei rispondenti, il 95% utilizzano ormai servizi terziarizzati, ed il più delle volte da fornitori diversi. Indipendentemente dalle dimensioni e dalle funzioni espletate con i vari applicativi, questi sistemi sono realtà ibride, in parte on premise ed in parte multi cloud dinamiche: realtà che comportano una maggior complessità per la sicurezza digitale e la sua gestione. Questo dato è inoltre significativo in quanto evidenzia il trend dell'accettazione e diffusione nell'uso di servizi ICT terziarizzati, confrontando i dati emersi e man mano cresciuti nei sedici anni di indagini OAD/OAI a partire dal 2007.

La terziarizzazione è stata usata non solo per le applicazioni, gli ambienti di sviluppo e le infrastrutture ICT, in cloud IaaS/PaaS/SaaS, ma anche alle gestione terziarizzata dell'intero sistema informativo, o di sue parti, e della sua sicurezza: in tale logica sono emerse offerte per MSS[38], Managed Security Services e CSaaS[39], Cyber Security as a Service, che potranno essere sempre più utilizzate dalle realtà piccole e piccolissime.

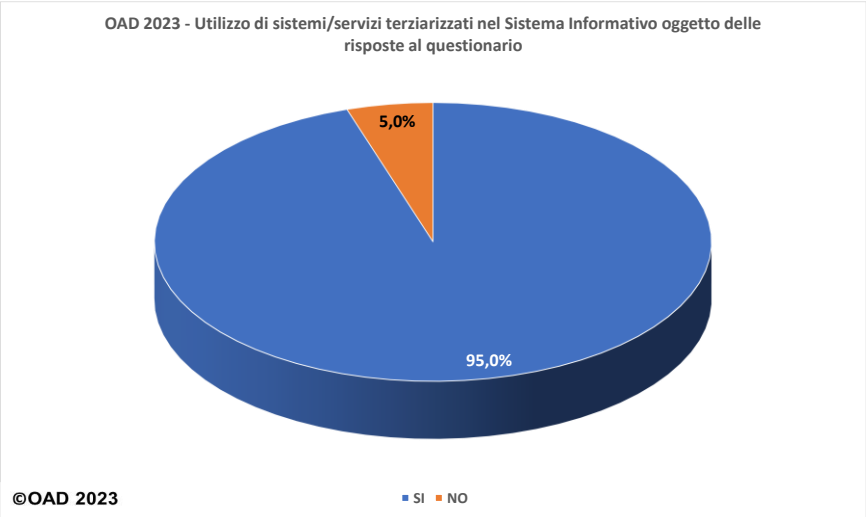


Fig. 6.1-6

Dato che la terziarizzazione dei sistemi e dei servizi ICT, in particolare con il cloud, è un elemento che fortemente caratterizza un sistema informativo e la sua sicurezza digitale, si è voluto correlare questo dato con la classe di dipendenti delle aziende/enti rispondenti.
La fig. 6.1-7 mostra tale correlazione tra l'utilizzo di servizi terziarizzati (tipicamente in cloud) e le dimensioni aziendali: per una corretta interpretazione della correlazione, si deve tener conto che le percentuali emerse dipendono anche dal numero di risposte ricevute. Infatti dalla figura emerge che le strutture organizzative con meno di 250 dipendenti, le PMI per le aziende, utilizzano applicazioni e servizi terziarizzati per il 70,6%. Nell'indagine OAD 2023 alcune grandi e grandissime organizzazioni sono i provider di servizi terziarizzati e in cloud, ed essi difficilmente utilizzano a loro volta terziarizzazioni di loro concorrenti; questo il motivo, oltre al minor numero di rispondenti, perché le organizzazioni con più di 250 dipendenti hanno in figura una percentuale complessiva solo del 29,4%.

[38] MSS, Managed Security Services, indica la gestione terziarizzata dei servizi di sicurezza digitale. La terziarizzazione di questi servizi può essere totale o parziale, ed erogata da uno o più consulenti, o da una o più aziende specializzate. Può inoltre essere svolta con strumenti informatici inseriti all'interno del SI del cliente stesso, o esterni, di proprietà dei e/o utilizzati dalle terze parti coinvolte.
[39] CSaaS, CyberSecurity as a Service, fa riferimento ai servizi di sicurezza digitale erogati in cloud, e che possono essere gestiti direttamente da chi si occupa della sicurezza digitale del SI, sia il persone interno all'azienda/ente sia il personale esterno di terze parti, quali consulenti e società che li gestiscono in nome e per conto dei responsabili del sistema informativo del cliente.

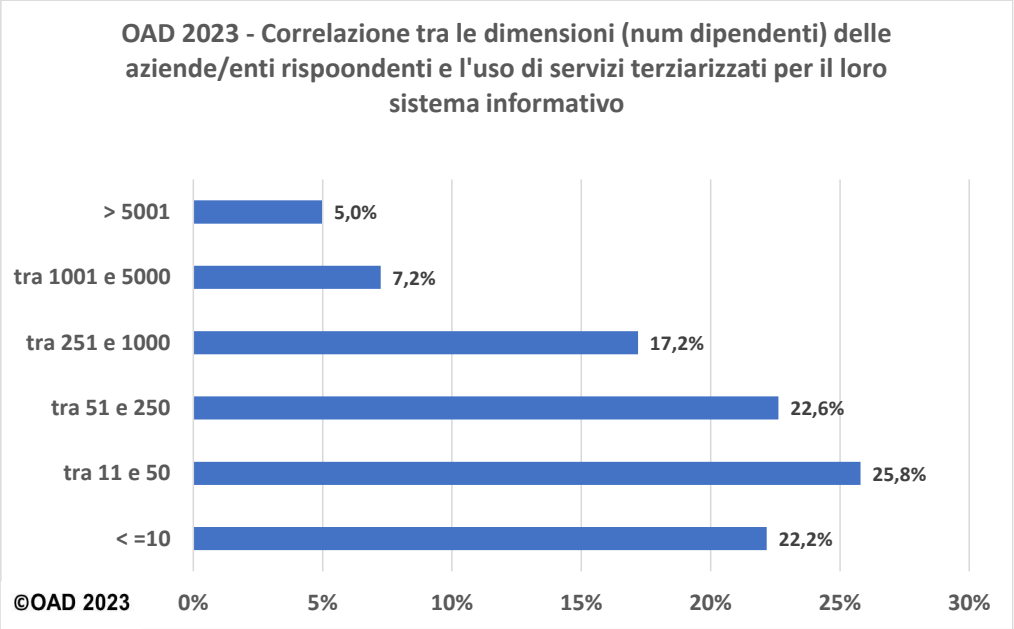


Fig. 6.1-7

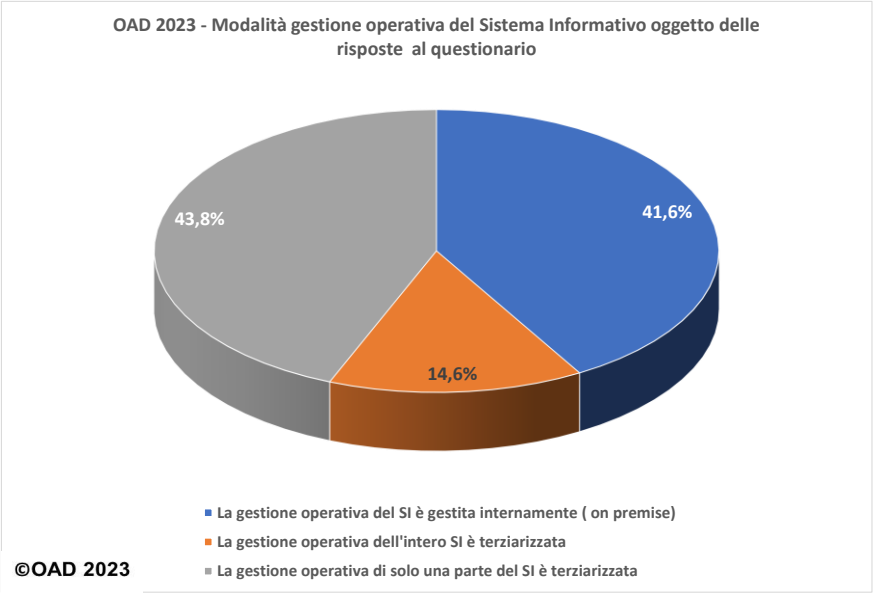


Fig. 6.1-8

La gestione operativa terziarizzata del SI include tipici servizi quali (elenco non esaustivo) 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 sistema informativo e della sua sicurezza. Le fig. 6.1-8 e 6.1-9 mostrano la situazione per i sistemi informativi oggetto delle risposte:

- la gestione dell'intero sistema informativo è terziarizzata solo per il 14,6%;
- la gestione della sicurezza digitale è terziarizzata dal 22,4%.

In entrambi i casi una percentuale ben maggiore opta per un mix tra gestione interna e terziarizzata: quest'ultima, molto probabilmente per gli ambienti e le applicazioni usate ed acquisite "as a service".

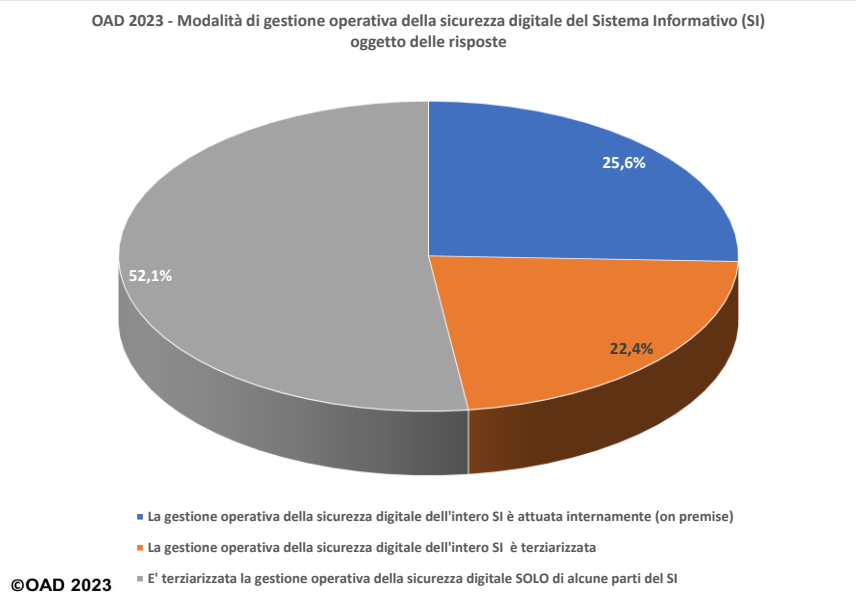


Fig. 6.1-9

Un'ultima considerazione sulla terziarizzazione della gestione operativa della sicurezza digitale: essa può e deve essere terziarizzata, in particolare per le piccole strutture, ma a condizione che sia terziarizzata alle corrette condizioni tecniche, economiche e normative, che sia trasparente e controllabile: in una parola che sia un "right-sourcing", un giusto approvvigionamento.

6.2 L'Azienda/Ente rispondente

La fig. 6.2-1 riporta la tabella con i raggruppamenti dei settori merceologici considerati da OAD: essa fa riferimento alla classificazione ATECO[40], sulla cui base si sono raggruppati alcune classi e alla quale si sono aggiunte le Pubbliche Amministrazioni Centrali e Locali.
Questa classificazione abbastanza dettagliata, pur con vari raggruppamenti, è stata ritenuta utile per ridurre possibili errori di posizionamento dell'azienda/ente da parte delle/dei rispondenti, come era successo nei primi anni dell'indagine OAI/OAD.

La fig. 6.2-2 riporta la distribuzione percentuali dei rispondenti per le macro famiglie di settori merceologici considerati. Dato che l'indagine OAD 2023 è focalizzata sugli ambiti web, che nella maggior parte dei casi sono in Italia terziarizzati, si è voluto evidenziare, tra i servizi ICT, quello dei Fornitori (Service Provider) di hosting e di cloud, separandolo in una

[40] 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

voce a se stante e ponendo tutti gli altri servizi ICT in una altra voce. L'intenzione era anche di "forzare" in questo modo i Service Provider a compilare la parte opzionale del questionario sulle misure di sicurezza in essere. Ma anche quest'anno, come già riferito in §3, AIPSI e l'autore non sono riusciti, nonostante l'effettivo aiuto di qualche associazione patrocinante, ad ottenere un numero significativo di risposte, non solo dai service Provider, ma anche da settori come quello finanziario e assicurativo, quello della sanità (enti sanitari, ospedali, cliniche, studi medici, laboratori d'analisi, etc.), dell'istruzione, delle Pubbliche Amministrazione. Si è comunque riusciti a far compilare il questionario ad almeno alcuni appartenenti ad ogni settore merceologico considerato, più PAL e PAC, anche se per alcuni settori il numero di risposte è stato esiguo.
Le risposte avute dai vari settori merceologici sono state significative per l'analisi complessiva dei trend sul fenomeno attacchi digitali in Italia, oltre che sulle misure di sicurezza in essere, ma non sono stai sufficienti per approfondire l'analisi per settore.

- Settore primario: agricoltura, allevamento, pesca, estrazione (Codici Ateco A e B)
- Industria manifatturiera e costruzioni: meccanica, chimica, farmaceutica, elettronica, alimentare, edilizia, ecc. (Codici Ateco C e F)
- Utility: Acqua, Energia, Gas ecc. (Codici Ateco D ed E)
- Commercio all'ingrosso e al dettaglio, incluso quello di apparati ICT (Codici Ateco G)
- Trasporti e magazzinaggio (Codice Ateco H)
- Attività finanziarie ed assicurative: assicurazioni, banche, istituti finanziari, broker, intermediazione finanziaria, ecc. (Codice Ateco M)
- Servizi turistici, di alloggio e ristorazione: agenzie di viaggio, tour operator, hotel, villaggi turistici, campeggi, ristoranti, bar, etc. (Codice Ateco I e N79)
- Attività artistiche, sportive, di intrattenimento e divertimento: teatri, biblioteche, archivi, musei, lotterie, case da gioco, stadi, piscine, parchi, discoteche, etc. (Codice Ateco R)
- Stampa e servizi editoriali (Codice 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)
- Servizi ICT: consulenza, produzione software, service provider ICT, gestione Data Center, servizi assistenza e riparazione ICT, etc. (Codici Ateco J62, J63, S95.1)
- 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. (Codice Ateco Q)
- Istruzione: scuole e università pubbliche e private (Codice Ateco P)
- Associazioni, associazioni imprenditoriali e sindacati (Codice Ateco S94)
- PAC, Pubblica Amministrazione Centrale
- PAL, Pubblica Amministrazione Locale

Fig. 6.2-1

La fig. 6.2-3 mostra la ripartizione del tipo di PAL rispondenti. Purtroppo AIPSI non è riuscita a coinvolgere, come avrebbe voluto, un ben maggiore numero di PAL: molte di quelle contattate hanno rifiutato di rispondere al questionario per le policy interne. Comunque si è risusciti ad ottenere qualche risposta dai vari tipi di PAL, tranne che per i Comuni tra 5.000 e 15.000 abitanti.
Volutamente non si è voluto considerare un dettaglio analogo per le PAC, perché sostanzialmente avrebbe leso il principio di anonimità garantito da OAD.

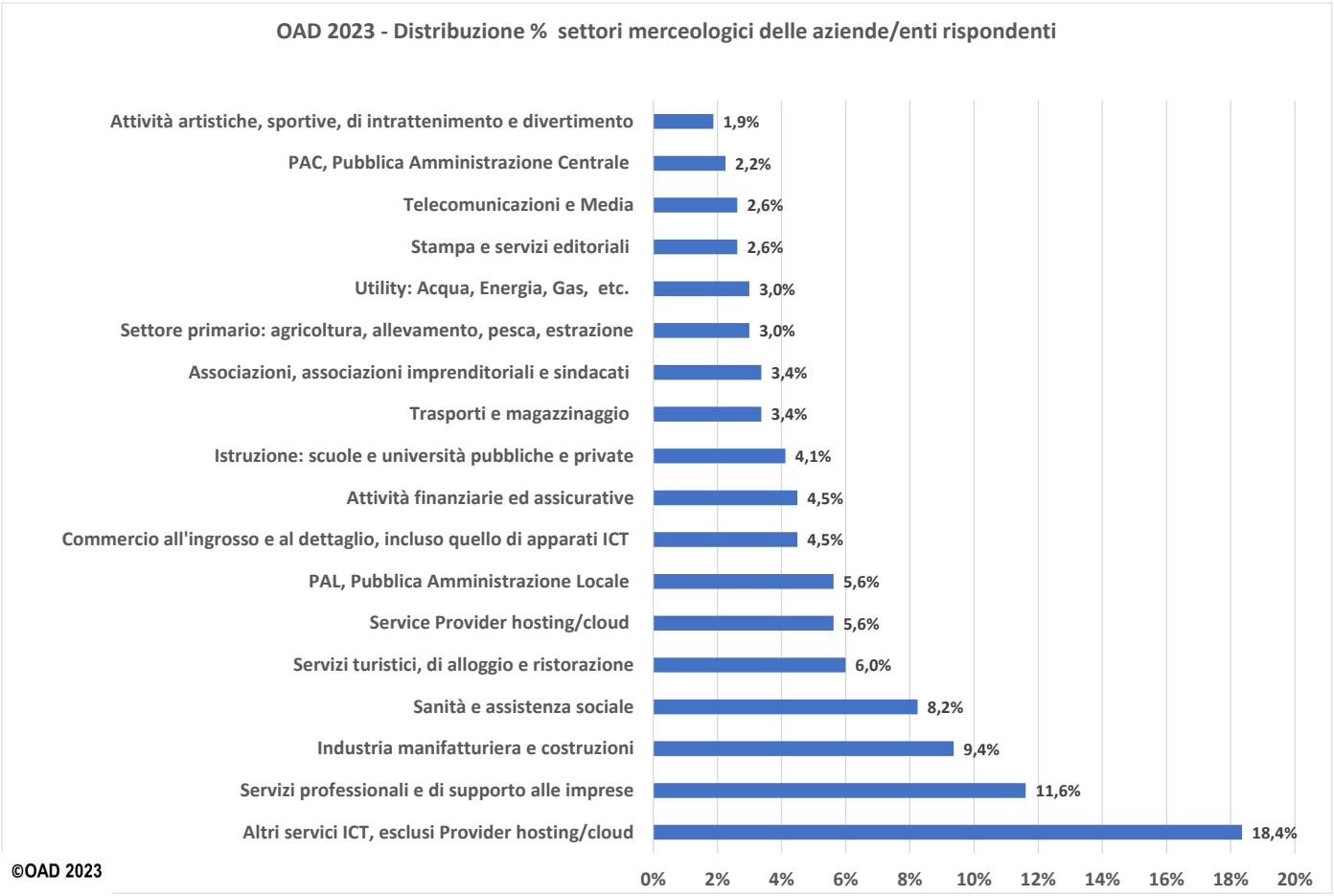


Fig. 6.2-2

Per le dimensioni di un'organizzazione per numero di dipendenti, come per le ultime edizione di OAD il questionario 2023 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

La fig. 6.2-4 mostra la ripartizione percentuale delle aziende/enti rispondenti in base al numero di loro dipendenti. Hanno risposto il 67% di piccole e medie organizzazioni, ossia quelle con meno di 250 dipendenti (le PMI, Piccole Medie Imprese, in ambito aziende private). Significativa, con un 21,6%, la presenza tra queste delle piccolissime organizzazioni con meno di 10 dipendenti, che, come già indicato in §3.4.5, costituiscono la stragrande maggioranza delle imprese, private e pubbliche, in Italia.

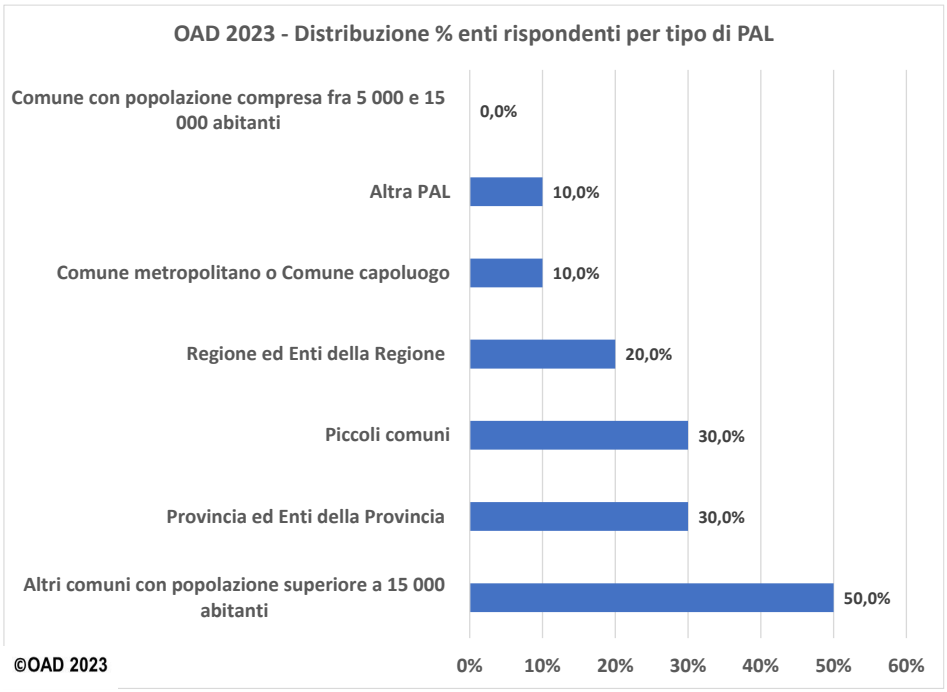


Fig. 6.2-3

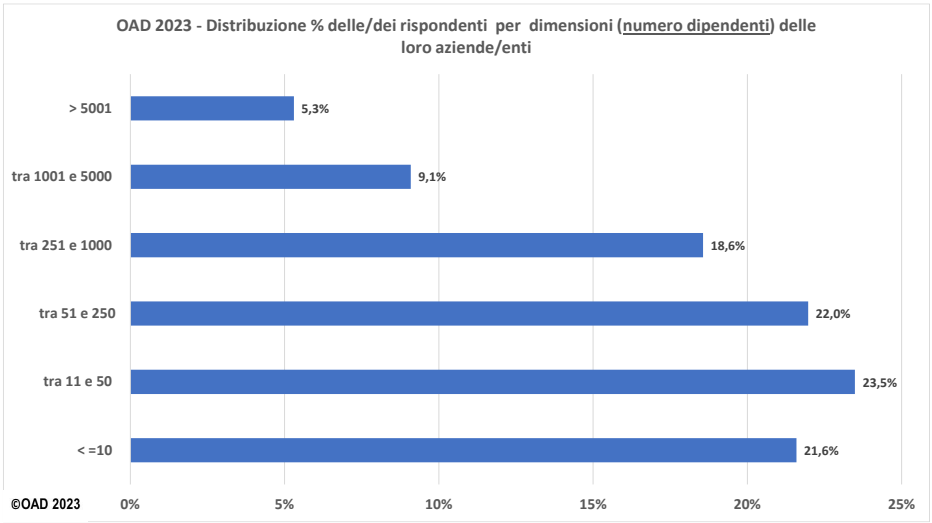


Fig. 6.2-4

La fig. 6.2-5 mostra la ripartizione percentuale delle aziende/enti rispondenti in base al loro ultimo fatturato, e per le PA le entrate del loro ultimo bilancio. Come nell'edizione precedente, OAD 2023 ha considerato nel questionario le seguenti 5 classi di fatturato/attivo di bilancio: fino a 1 Mlne €, da 1 a 5 Mlni €, da 5 a 10 Mlni €, da 10 a 50 Mlni €, oltre i 50 Mlni €.

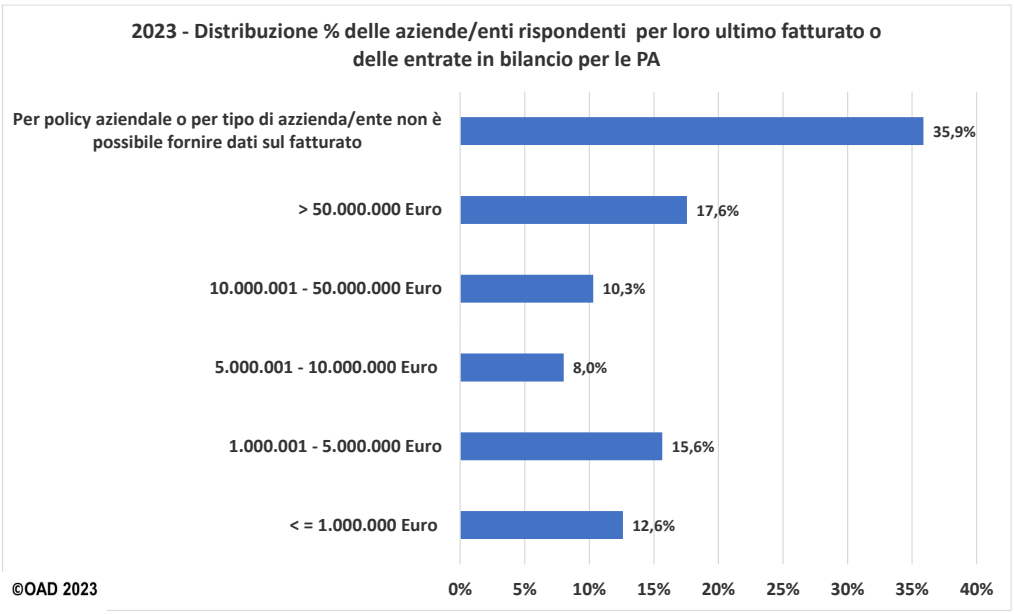


Fig. 6.2-5

Nell'attale indagine 2023 la percentuale più alta, 35,9%, è data da aziende/enti che non possono/vogliono fornire queste dato, pur con l'elevata anonimità garantita da OAD. Per questo motivo in OAD 2023 la maggior parte delle correlazioni tra dati su specifiche tematiche ed aziende/enti rispondenti è stata effettuata sulla classe per numero di dipendenti, e non per fatturato/entrate.
Un ulteriore dato caratterizzante un'azienda/ente è la copertura geografica delle sue attività e/o del suo business, da non confondere con la sede a livello regionale del polo principale del sistema informativo, di cui in fig. 6.1-2.

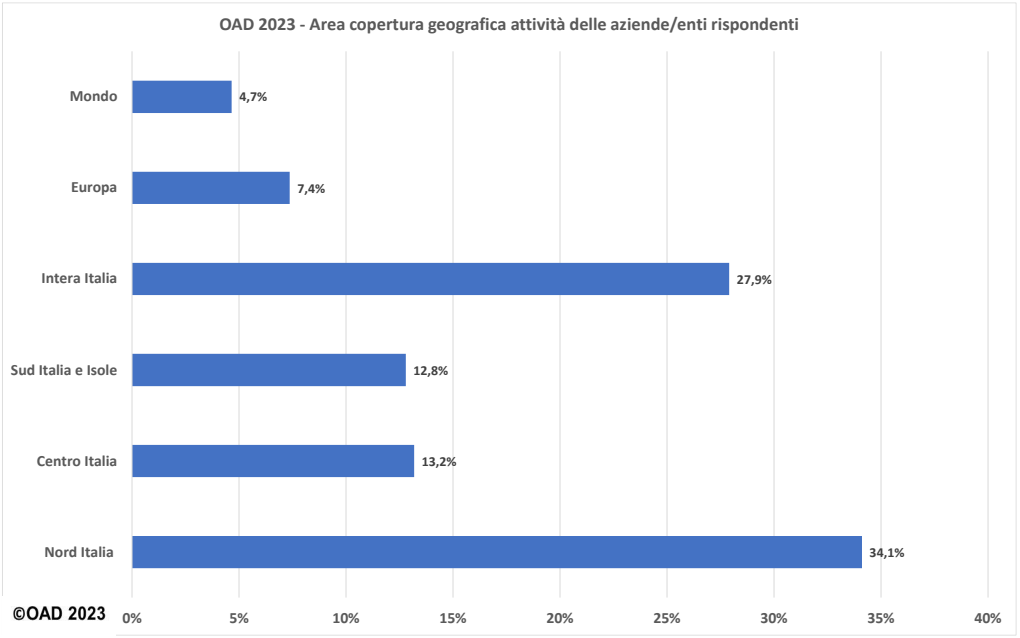


Fig. 6.2-6

La fig. 6.2-5 mostra la copertura geografica dell'azienda/ente. L'88% opera solo in Italia, e la figura dettaglia in quali aree. Di questi più di 1/3 opera al Nord, con percentuali simili, poco sopra e poco sotto il 13%, le organizzazioni che operano al Centro e al Sud. Alcune aziende, con percentuali più basse ma non trascurabili, operano a livello europeo e a livello mondiale.

6.3 Ruolo della persona rispondente

La fig. 6.3-1 mostra la ripartizione % dei ruoli nelle loro strutture organizzative di chi ha compilato il questionario OAD 2023

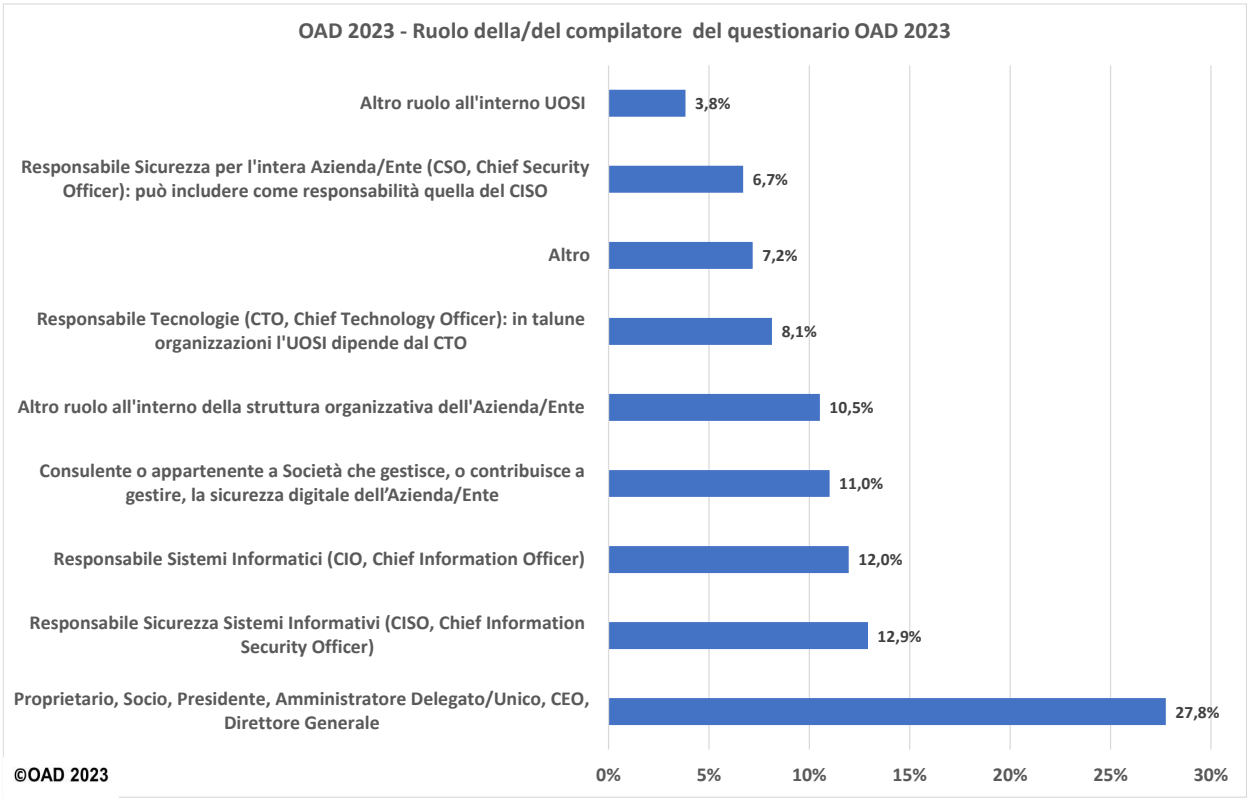


Fig. 6.3-1

Al primo posto, con il 27,8%, il proprietario/socio o i vertici manageriali dell'azienda/ente, cui seguono con percentuali nella fascia del 12%, il CISO ed il CIO (che rappresenta anche l'Amministratore di sistema interno per le piccole-piccolissime organizzazioni). L'alta percentuale di proprietari/soci deriva dall'alta percentuale di organizzazioni con meno di 50 dipendenti, come negozi, studi professionali, piccole PAL, dove chi decide sul sistema informativo, per quanto piccolo possa essere, è la proprietà o il top manager (C-level Executive). Relativamente basse le percentuali di CISO e di CIO, figure professionali presenti in Italia prevalentemente nelle medio-grandi organizzazioni: ed in molte di queste il ruolo di CISO non è definito, ed è attuato de facto dal CIO, da amministratori di sistema, da consulenti esterni.
Al quarto posto, con l'11%, 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 dl sistema informativo e della sua sicurezza, con i già citati servizi MSS e CSaaS.
Per la voce "Altro" molti delle/dei rispondenti hanno indicato la figura di DPO, Data Privacy Officer, altri quella di "Responsabile delle compliance", altri di auditor, altri di Preside per alcuni istituti scolastici. Percentuali ancora inferiori

per due figure, il CTO, Chief Technology Officer, il responsabile delle tecnologie, ed il CSO, Chief Security Officer, il Responsabile della Sicurezza fisica e delle persone per l'intera azienda/ente., ruoli che sono definiti ed operativi soprattutto nelle grandi organizzazioni.

7. Le misure di sicurezza digitale nei sistemi informativi delle aziende/enti rispondenti

Nell'indagine OAD 2023 le domande sulle misure di sicurezza erano opzionali, si potevano cioè saltare, anche se erano raccomandate per i fornitori di hosting/cloud e per le piccole/medie organizzazioni perché queste ultime, soprattutto, 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 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 **42,2%** delle/dei rispondenti complessivi (fig. 7-1).

La fig. 7-2 correla percentualmente quanti hanno risposto alle domande sulle misure di sicurezza per settore merceologico, incluse le PA. Pur avendo risposto a queste domande meno della metà delle aziende/enti, la loro distribuzione copre tutti i settori merceologici, a parte le PAC.

Percentualmente al primo posto, con un **30,6%**, sono le **aziende ICT**, nell'indagine OAD 2023 volutamente suddivise tra i fornitori di hosting/cloud (dato che l'indagine è verticalizzata sugli attacchi alle applicazioni ed ai siti web che nella maggior parte dei casi sono in cloud) e tutte le altre aziende dell'offerta ICT. Questi due gruppi si suddividono esattamente a metà questa percentuale: in proporzione al numero di aziende del settore in Italia, OAD 2023 ha avuto più compilazioni dai fornitori di servizi web, quali IaaS/PaaS, SaaS, che da tutte le altre aziende ICT. Seguono, con percentuali gradualmente inferiori, le aziende del settore manifatturiero, gli enti e le aziende del settore sanitario, gli studi per i servizi professionali (legali, commercialisti, etc.), e così via.

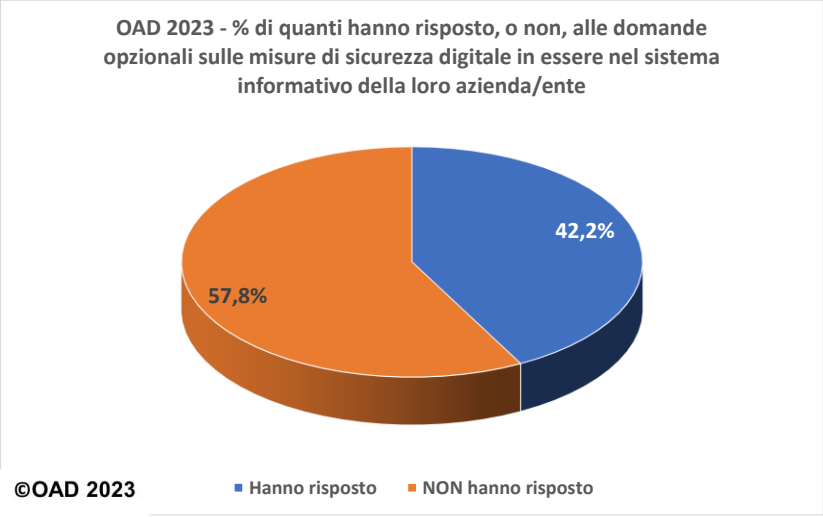


Fig. 7-1

Il presente capitolo descrive gli strumenti di sicurezza in uso nei sistemi informativi delle aziende/enti rispondenti, e le cui macro caratteristiche sono riportate nel precedente §6, così da poter meglio comprendere in quali ambiti e contro quali livelli di sicurezza digitale sono stati attuati gli attacchi rilevati ed analizzati in §4.

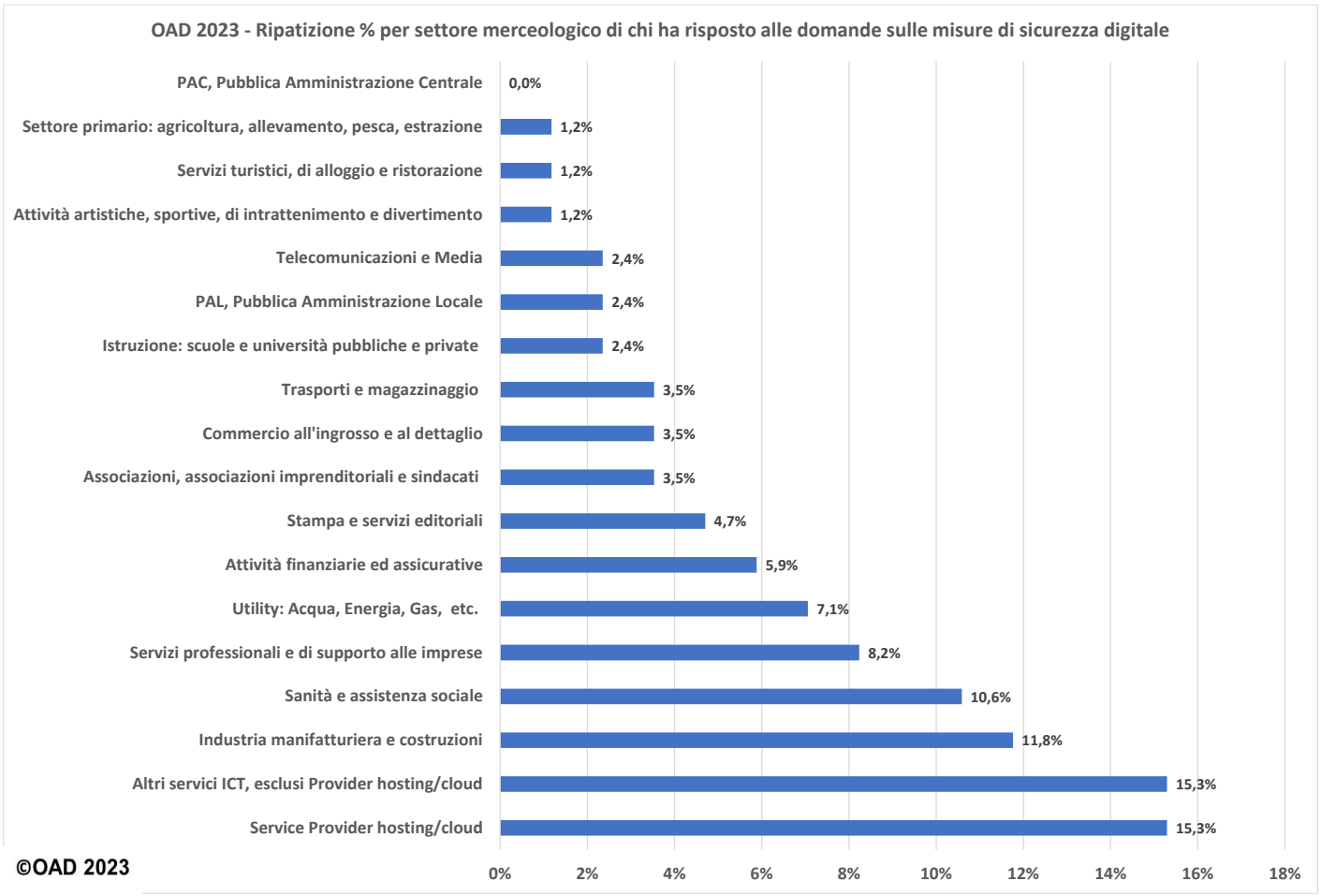


Fig. 7-2

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 (NIS2, DORA, CER, etc), a partire dal GDPR per la privacy, richiedono tutti l'attuazione di gran parte delle misure organizzative considerate in OAD 2023. 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 ed una 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[41], 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 la relativa struttura organizzativa, piccolo o grande, interna o esterna.
La fig. 7.1.1-1 mostra che poco meno dei ¾ delle aziende/enti rispondenti hanno posto in esercizio una struttura organizzativa per la sicurezza digitale con a capo un responsabile, il CISO. Tale struttura è presente nelle organizzazioni di ogni dimensione, come indica la fig. 7.1.1-2.

Fig. 7.1.1-1

Pur tenendo conto che la correlazione tra l'attuazione della struttura con CISO e le dimensioni delle aziende/enti rispondenti è influenzata dal numero di compilazioni ricevute da parte di organizzazioni di varie dimensioni, la fig. 7.1.1-2 conferma che il ruolo e la struttura dedicata del CISO è presente anche nelle piccole organizzazioni rispondenti: un altro elemento che evidenzia come il campione emerso dall'indagine OAD 2023 si colloca in una fascia medio-alta per l'adozione delle misure di sicurezza digitale.

[41] 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.

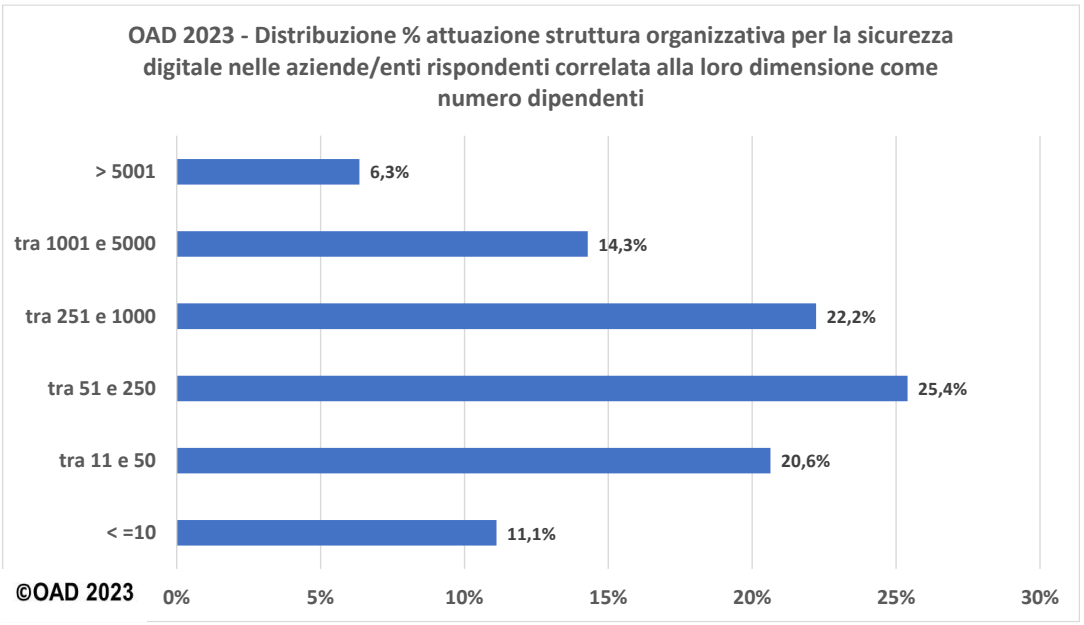


Fig. 7.1.1-2

La fig. 7.1.1-3 indica da chi dipende il CISO e la sua struttura organizzativa, per le realtà che hanno definito ed attuato ufficialmente tale ruolo.

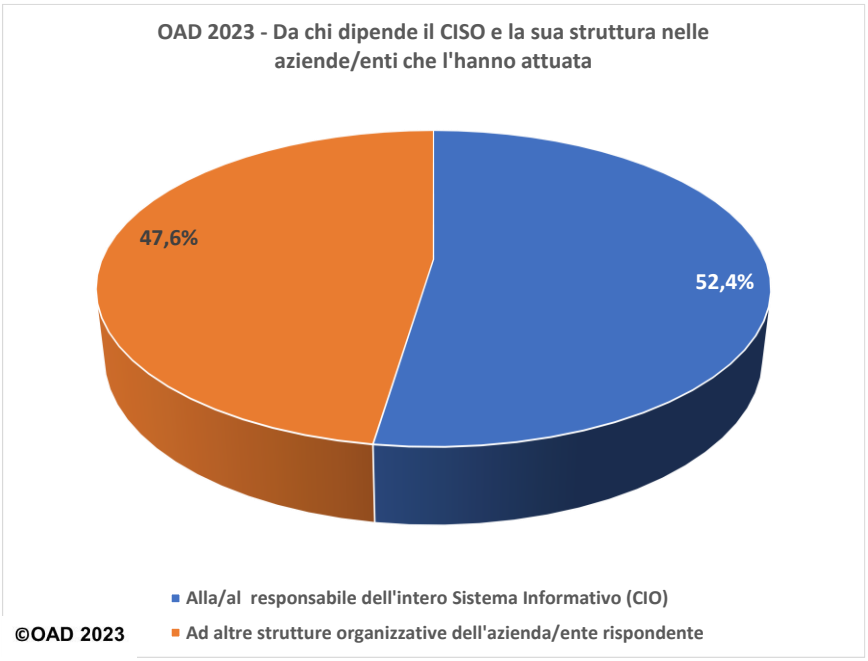


Fig. 7.1.1-3

Per semplificare la riposta al questionario da chi può dipendere il CISO e la sua struttura, oltre al CIO ed alla sua UOSI, Unità Organizzativa Sistemi Informativi, l'alternativa era una generica voce "altre strutture organizzative", che possono

essere la Direzione Generale, il Personale e l'Organizzazione, l'Ufficio legale, oppure le strutture di cui sono responsabili il CSO o il CTO. La figura mostra che le due opzioni quasi si pareggiano, in percentuale, pur con una leggera prevalenza del "tradizionale" riporto del CISO al CIO. Per meglio approfondire questo aspetto, si è correlata tale dipendenza alle dimensioni delle aziende/enti. Il risultato è riportato nella fig. 7.1.1-4.

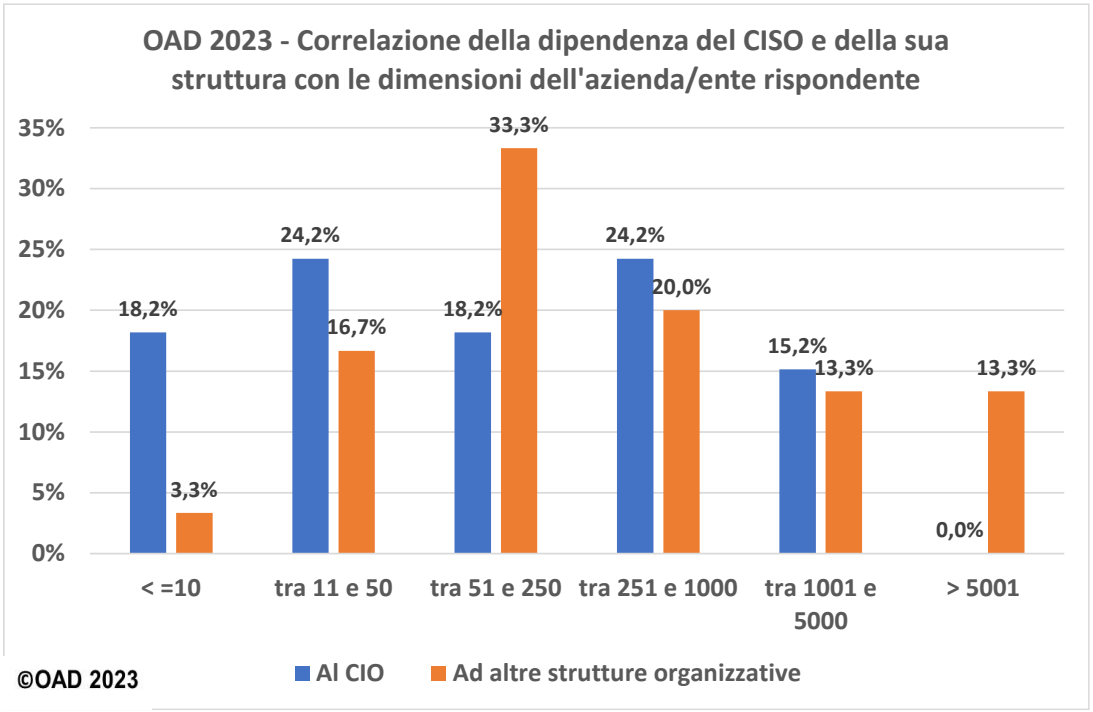


Fig. 7.1.1-4

Nelle piccole e piccolissime organizzazioni prevale ancora la tradizionale dipendenza del CISO dal CIO, ma nelle organizzazioni grandi e grandissime il ruolo del CISO aumenta fortemente e la tendenza è di porlo al di fuori dall'UOSI e dalla dipendenza del CIO. Nella figura, le organizzazioni più grandi rispondenti, > 5000 dipendenti, hanno tutte il CISO rispondente ad altre strutture organizzative e non a quella del CIO.
Come già ricordato in precedenza, i dati emersi dalle correlazioni dipendono anche dal numero di rispondenti per i vari temi considerati, in primis le classi di aziende/enti per numero di dipendenti: devono essere pertanto considerati come indicatori delle tendenze considerate nella correlazione stessa.

E' bene evidenziare che il posizionamento del CISO in ambito UOSI, e quindi sotto il CIO, di fatto lede il principio della separazione delle responsabilità (la "*separation of duties*"): infatti il controllato, ossia il CIO, controlla il controllore, ossia il CISO. Molte delle più recenti leggi e normative europee impediscono la mancanza della separazione dei compiti e delle responsabilità. In alcune multinazionali, il CISO ha un'importanza anche maggiore di quella del CIO, e può far parte del "board of director", il Consiglio di Amministrazione, del Gruppo.

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 o è ben dettagliato o 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 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 un' 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[42], così come richiesto ad esempio dal GDPR, ed ora anche dalle altre normative dell'Unione Europea nell'ambito della sicurezza digitale, le principali descritte in §3.4.

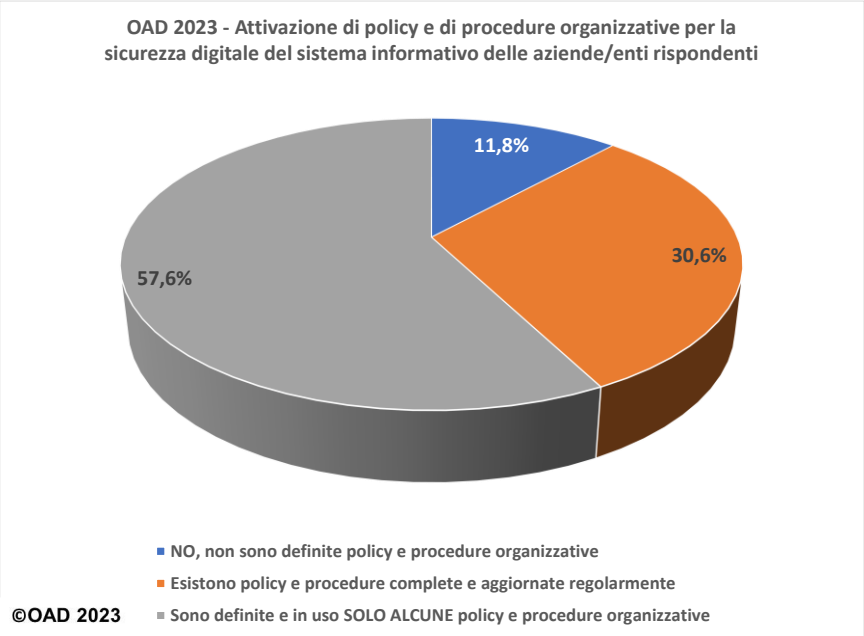


Fig. 7.1.2-1

La fig. 7.1.2-1 evidenzia che la stragrande maggioranza delle aziende/enti rispondenti, l'**88,2%** ha definito ed usa policy e procedure organizzative per la sicurezza digitale, ma di questi il **57,6 %** lo ha fatto solo per alcune attività e funzioni di sicurezza, tipicamente per quelle più necessarie e critiche; esempi includono la gestione degli incidenti e dei problemi, la gestione dell'identificazioni ed autenticazione degli utenti, finali e/o privilegiati (che include anche la gestione delle password), la gestione dell'help desk e del "trouble ticketing".[43]
A conferma di questo, OAD 2023 ha posto la domanda sull'esistenza di policy, e soprattutto di procedure, per la gestione di incidenti sul sistema informativo e sulla sua sicurezza. La fig. 7.1.2-2 fornisce la risposta, ed evidenzia che il **78,9%**

[42] Il termine "accountability" significa responsabilizzazione nei 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.
[43] 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.

dichiara di aver definito ed attuato queste misure organizzative. La figura mostra anche che il 2,7% ammette di non saperlo. A seconda di chi ha compilato il questionario OAD 2023, conoscenze specifiche su aspetti tecnici o organizzativi o legali possono mancare: se questi non ha potuto chiedere a colleghi, ha onestamente ammesso di non saperlo. Si vedrà, nelle pagine di questo capitolo (ma anche in altri del presente Rapporto OAD 2023), il ripetersi di queste risposte "non so" per alcune domande più specialistiche: questo è un elemento che comprova la serietà dei molti che hanno risposto al questionario, e non si sono inventati risposte su argomenti che non conoscevano; ed aumenta la validità e l'autorevolezza dell'intera indagine.

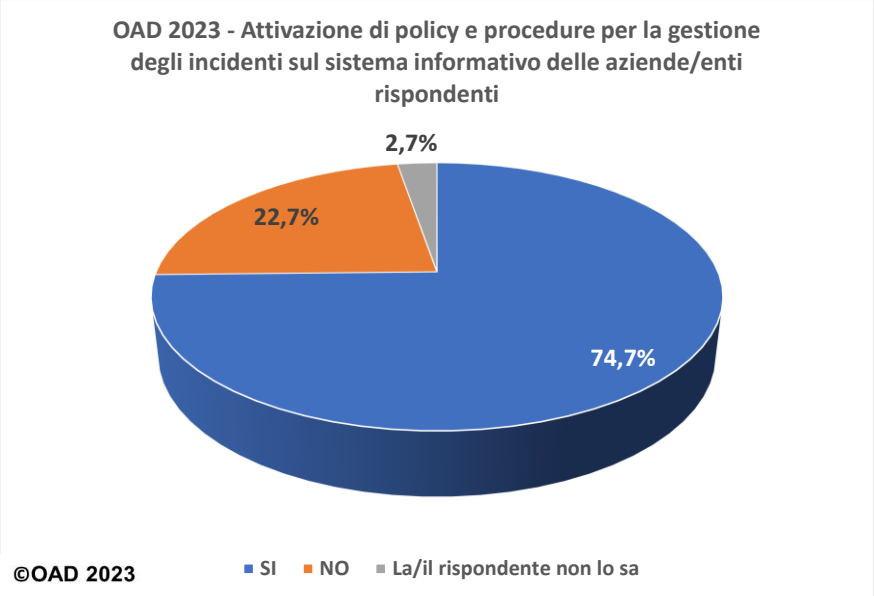


Fig. 7.1.2-2

Un'altra procedura organizzativa nella gestione del sistema informativo e della sua sicurezza è **l'assistenza agli utenti**, fondamentale soprattutto per i sistemi con centinaia o migliaia di utenti. 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 a diversi livelli di approfondimento[44] e in logica multicanale, nella maggior parte dei casi anche con applicazioni di "trouble ticketing". Per la sicurezza digitale, l'help desk è la prima interfaccia con l'utente finale del sistema informativo, 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 fig. 7.1.2-4).
La fig. 7.1.2-3 mostra che il **65,3%** delle aziende/enti rispondenti ha servizi di assistenza agli utenti, ed il **34,7** % le ha in parte o in toto terziarizzate.

[44] 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 oggetto della richiesta.

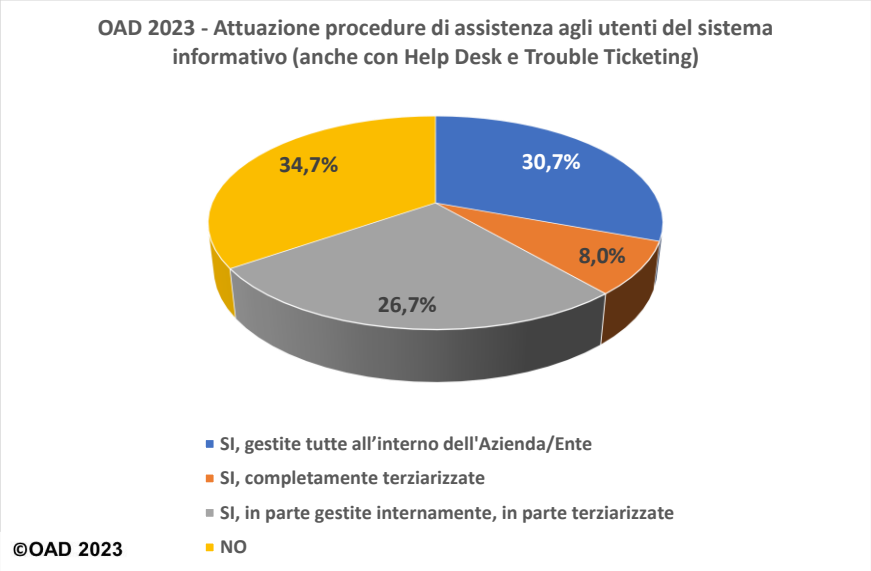


Fig. 7.1.2-3

Per la gestione degli incidenti gravi, e non solo riguardanti il sistema informativo, le grandi organizzazioni dedicano uno specifico team, l'ERT, 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 (si veda &7.2.7). Il **45,3%** delle aziende/enti rispondenti dichiara di avere un ERT con definite e in uso le relative procedure organizzative, come mostrato in fig. 7.1.2-4. Di questi solo il 20% effettua periodicamente prove e simulazioni di casi di emergenza: ed è quindi solo questo nucleo di aziende/enti in grado realmente di attivare un Disaster Recovery del sistema informativo (SI).

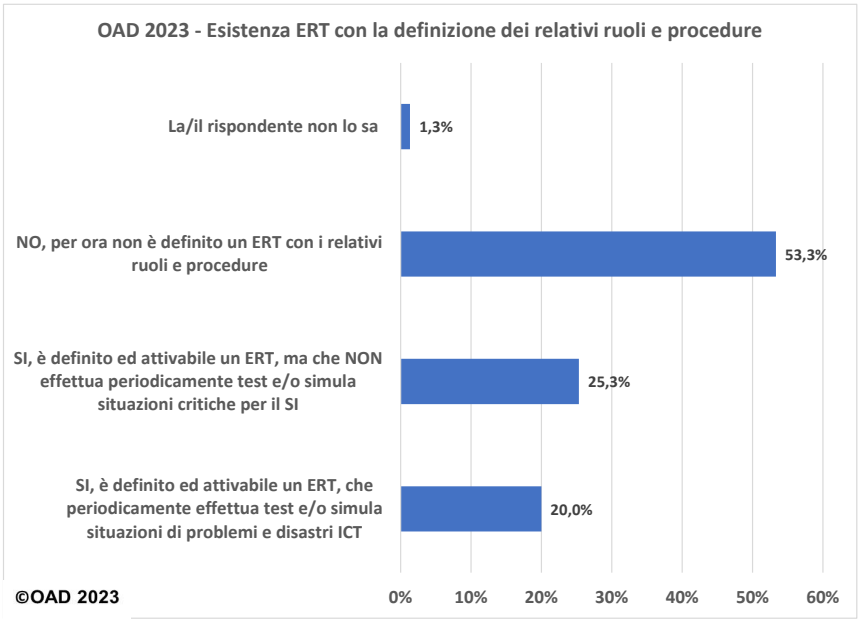


Fig. 7.1.2-4

Un altro aspetto importante nella gestione dell'ERT, oltre alle periodiche prove e simulazioni dei possibili "disastri", è il periodico aggiornamento delle sue procedure organizzative e del personale che lo compone. Le risposte in merito fornite dalle aziende/enti che dispongono di un ERT sono riportate in fig. 7.1.2-5, che evidenzia che più dei ¾ aggiorna componenti e procedure ERT o periodicamente o a seguito di importanti riorganizzazioni e/o importanti modifiche evolutive del sistema informativo.

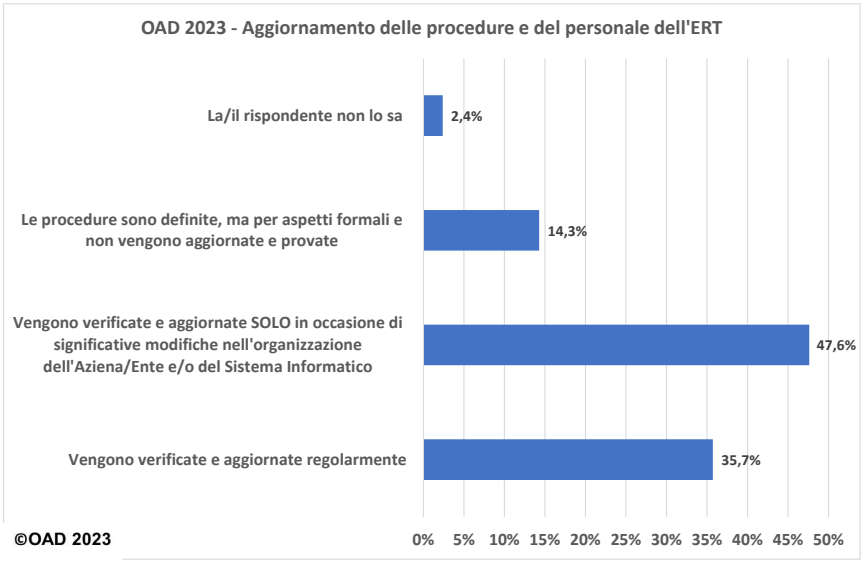


Fig. 7.1.2-5

7.1.3 Analisi dei rischi digitali e dei possibili impatti

L'analisi dei rischi digitali e dei lori impatti sul sistema informativo, 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.
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 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[45] grazie all'uso di tecniche di intelligenza artificiale. Uno strumento gratuito che aiuta nell'analisi predittiva è il **MITRE ATT&CK**, AdversarialTactics, Techniques, and Common Knowledge (https://attack.mitre.org/), che fa riferimento alla banca dati CVE delle vulnerabilità (§3.3.1) 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) e nei SOC.

Il **90,8%** delle aziende/enti rispondenti **effettua l'analisi dei rischi**, come evidenzia la fig. 7.1.3-1 con un risultato veramente positivo: di questi il 48,2% la effettua solo se richiesta e/o in casi specifici, ad esempio dopo aver subito un grave attacco digitale.

[45] 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.

A questo risultato ha sicuramente contribuito la compliance alle normative sulla privacy, obbligatorie in Europa e in Italia dal 1995,ed ulteriormente rafforzate dall'attuale GDPR. Anche le nuove normative europee sulla sicurezza digitale, dal NIS 2 a DORA (si veda §3.4), richiedono una seria e periodica analisi dei rischi digitali.

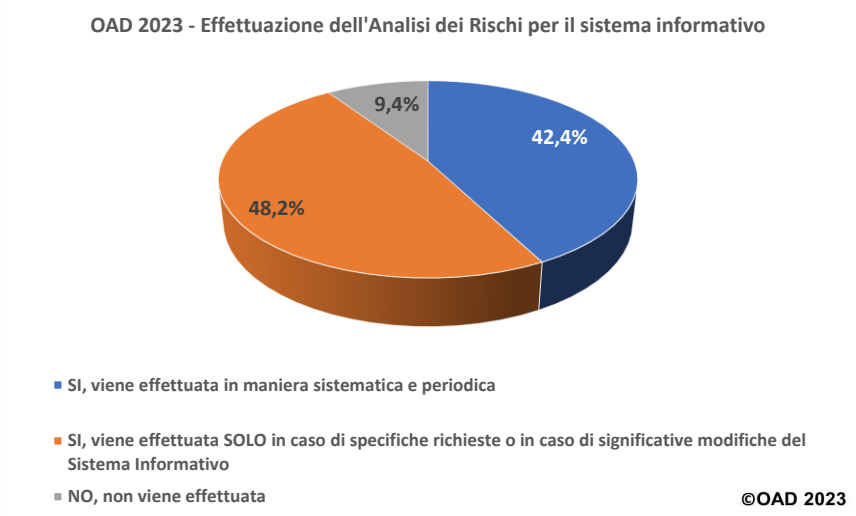


Fig. 7.1.3-1

Data l'importanza dell'analisi dei rischi, OAD 2023 ha voluto approfondire chi la effettua o non correlando questo dato con le dimensioni, come numero di dipendenti, delle aziende/enti rispondenti. La fig. 7.1.3-2 mostra tale correlazione e conferma, come prevedibili, che le grandi organizzazioni rispondenti effettuano tutte l'analisi dei rischi. Il dato positivo è che anche le piccole e piccolissime organizzazioni rispondenti effettuano tale analisi, e conferma che il bacino emerso dall'indagine OAD 2023 è nella fascia medio-alta per il livello di sicurezza digitale implementato. Come già ricordato in precedenza, i dati emersi dalle correlazioni dipendono anche dal numero di rispondenti per i vari temi considerati, in primis le classi di aziende/enti per numero di dipendenti: devono essere pertanto considerati come indicatori delle tendenze considerate nella correlazione stessa.

Un'ulteriore approfondimento riguarda "il come" viene effettuata l'analisi dei rischi, domanda che il questionario ha posto solo ai rispondenti che in precedenza avevano dichiarato di farla. Le tradizionali metodiche si basano su standard e best practice consolidati a livello mondiale, quali ad esempio NIST, CRAMM, Mehari, Octave Allegro, etc. Le metodiche, i framework e gli strumenti per l'analisi predittiva sono al momento quasi tutti proprietari, e si vanno consolidando per l'analisi dei rischi informatici, essendo per lo più usati attualmente per analisi predittive in altre aree del business. L'uso di algoritmi e di automatismi basati su intelligenza artificiale e machine learning pone una serie di problemi sulla loro effettiva validità in ogni campo, e al di là delle grandi discussioni in merito anche in Italia, si è in attesa delle regole per il loro buon uso che stanno per essere emesse da vari stati, e in particolare dall'Unione Europea con il suo AI Act[46] che dovrebbe essere completato e pubblicato entro i primi mesi del 2024.

[46] https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

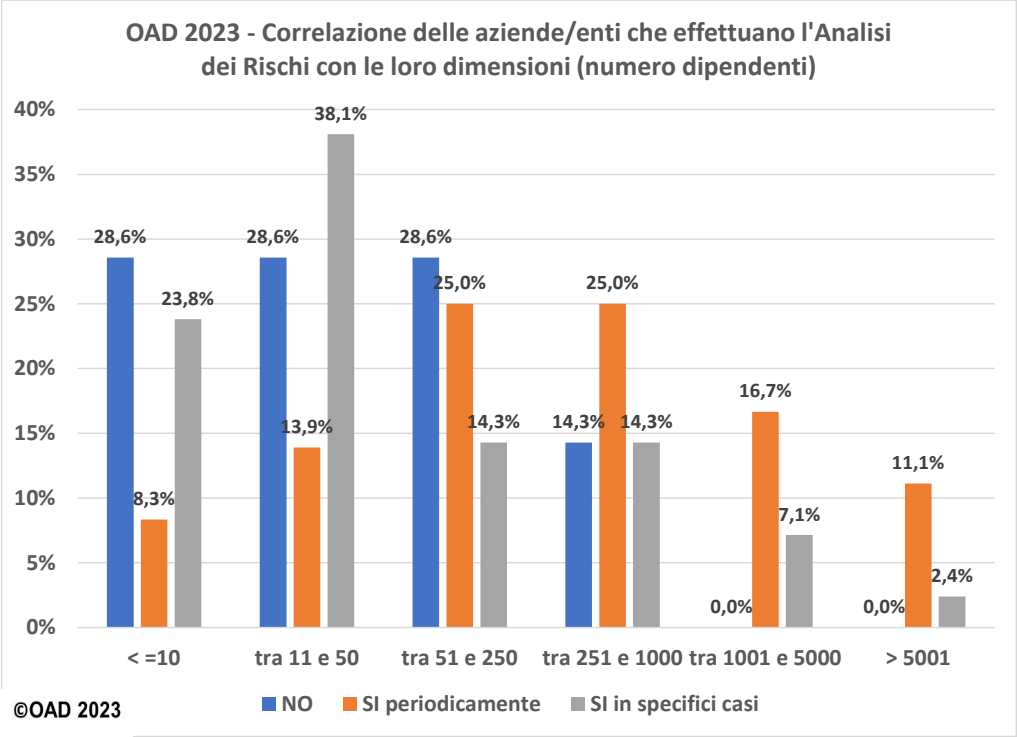


Fig. 7.1.3-2

Come indicato nella fig. 7.1.3-3, più della metà delle aziende/enti che effettuano l'analisi dei rischi fa uso delle citate best practice e standard. Un ulteriore approfondimento sull'analisi dei rischi digitali è posto dalla domanda sull'utilizzo, e quale, degli standard della famiglia ISO 27000, richiesti per varie certificazioni aziendali e dei sistemi informativi.

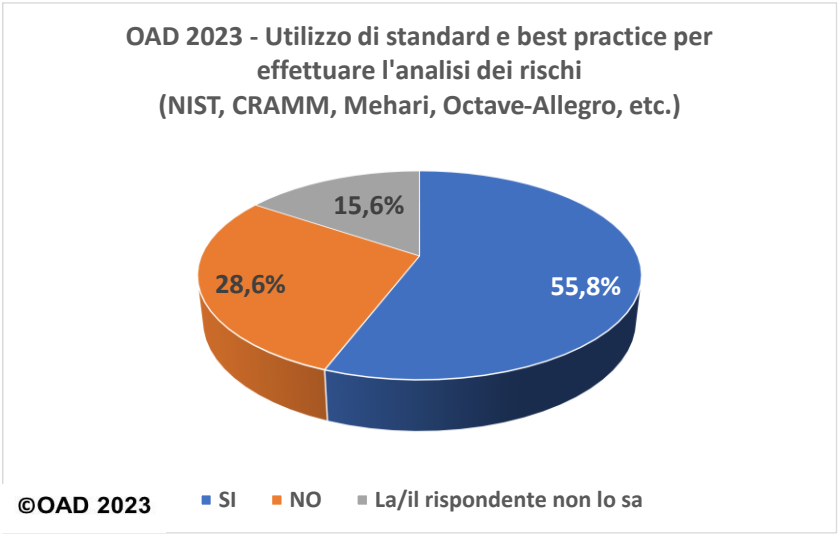


Fig. 7.1.3-3

Tra le aziende/enti rispondenti che effettuano l'analisi dei rischi digitali, circa i 2/3, il **66,2%,** fa riferimento agli standard ISO, in particolare all'ISO 27001 e all'ISO 27005, e di questi quasi la metà ha anche ottenuto la relativa certificazione aziendale.

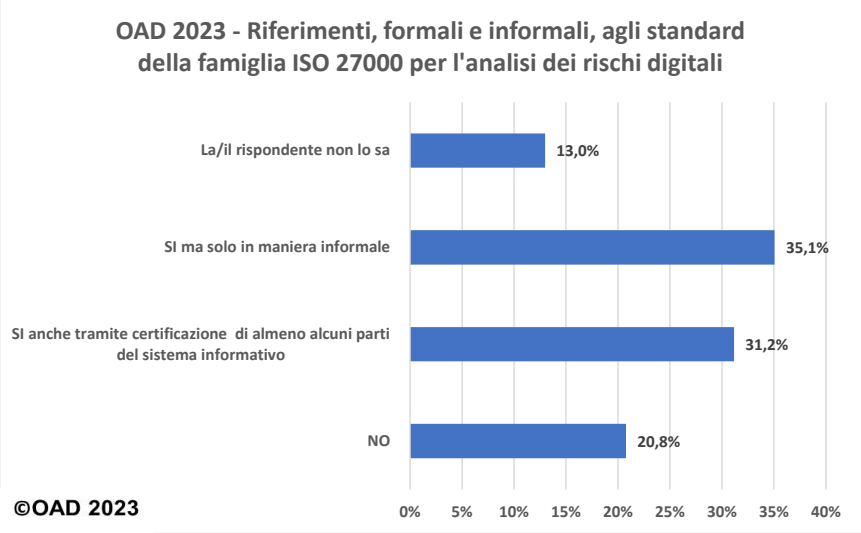


Fig. 7.1.3-4

Una analisi dei rischi del sistema informativo comporta, o dovrebbe comportare, anche l'analisi dei possibili impatti sui processi ed attività dell'azienda/ente, analisi chiamata **BIA**, Business Impact Analysis: tale analisi, si basa normalmente sui rischi digitali più probabili e più gravi per un dato contesto. Su questo tema, nell'indagine OAD 2023 per chi effettua l'analisi dei rischi digitale, la fig. 7.1.3-5 evidenzia che circa i ¾ effettua anche una BIA.

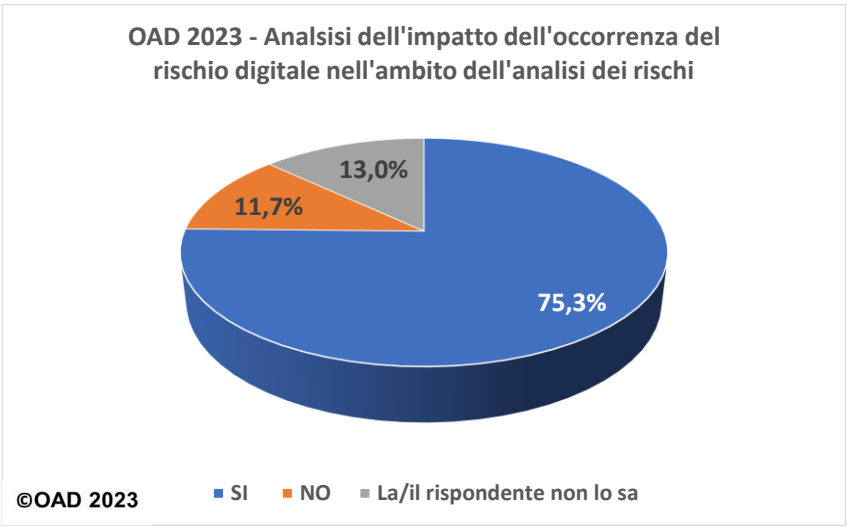


Fig. 7.1.3-5

Nell'ambito della gestione dei rischi digitali, l'unica domanda del questionario OAD 2023 riguardava la stipula di una polizza assicurativa sui rischi digitali per l'intero sistema informativo, o per le sue parti che trattano i dati più critici: domanda aperta a tutti, non solo a chi ha effettua l'analisi dei rischi digitali.
Come mostrato nella fig. 7.1.3-6, quasi 1/3 delle aziende/enti rispondenti ha stipulato una simile polizza, ma di questi il 28,2% solo per alcune delle parti del sistema informativo. 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'assicurazione infatti richiede, e

verifica con suoi esperti, che siano in atto le misure di sicurezza idonee, e allo stato dell'arte dell'informatica, altrimenti non stipula il contratto o chiede premi altissimi.

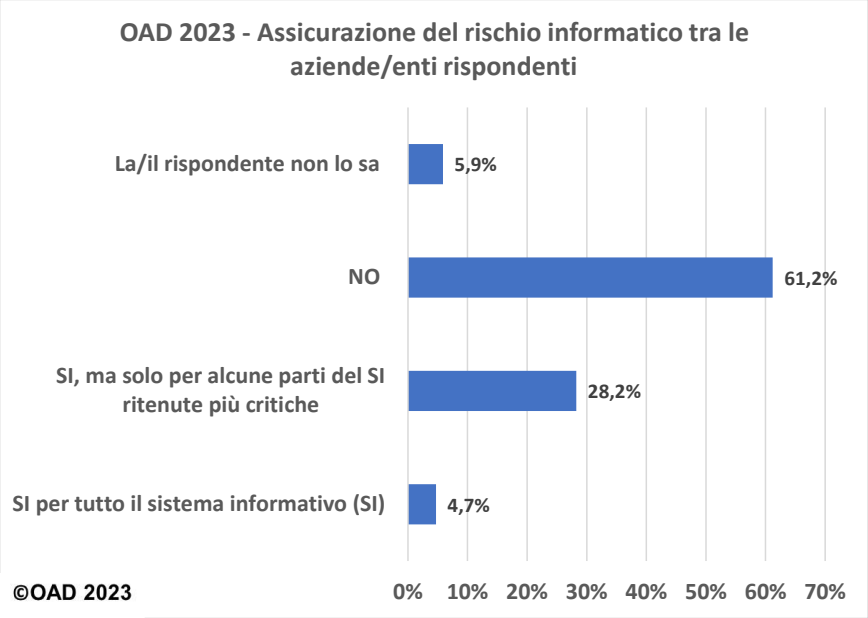


Fig. 7.1.3-6

Come già sottolineato nei precedenti capitoli, ad alcune domande "specialistiche" la/il rispondente ha selezionato "non si sa", riportato nelle figure con la voce "La/il rispondente non lo sa"; in taluni casi questa voce ha valori percentuali non trascurabili, ed è un aspetto in qualche misura positivo per l'indagine OAD. A domande specialistiche, è ragionevole, ed apprezzato, che chi ha compilato il questionario non sapesse come rispondere, e correttamente non ha selezionato a caso una risposta ma abbia onestamente selezionato che non sa rispondere.

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 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.

La fig. 7.1.4-1 indica che il **71,8%** dei rispondenti effettua **auditing per la sicurezza digitale**, e più della metà di questi, il 41,2% lo effettua sistematicamente e periodicamente. Valori percentuali alti, soprattutto considerando le numerose piccole organizzazioni rispondenti, e per le quali, se non sono del settore dell'ICT, l'auditing della sicurezza digitale non è prioritaria.
La fig. 7.1.4-2, indica chi effettua l'auditing per le aziende/enti che hanno risposto affermativamente nella domanda precedente, quindi per il 71,8% del totale. La maggior parte, 46,3%, effettua l'auditing in maniera mista (mix), con

personale interno e con esperti esterni. I valori percentuali delle aziende/enti che effettuano l'auditing della sicurezza digitale solo esternamente o solo internamente quasi si equivalgono, intorno ad un quarto del totale ciascuno, con un piccolo vantaggio per l'auditing interno.

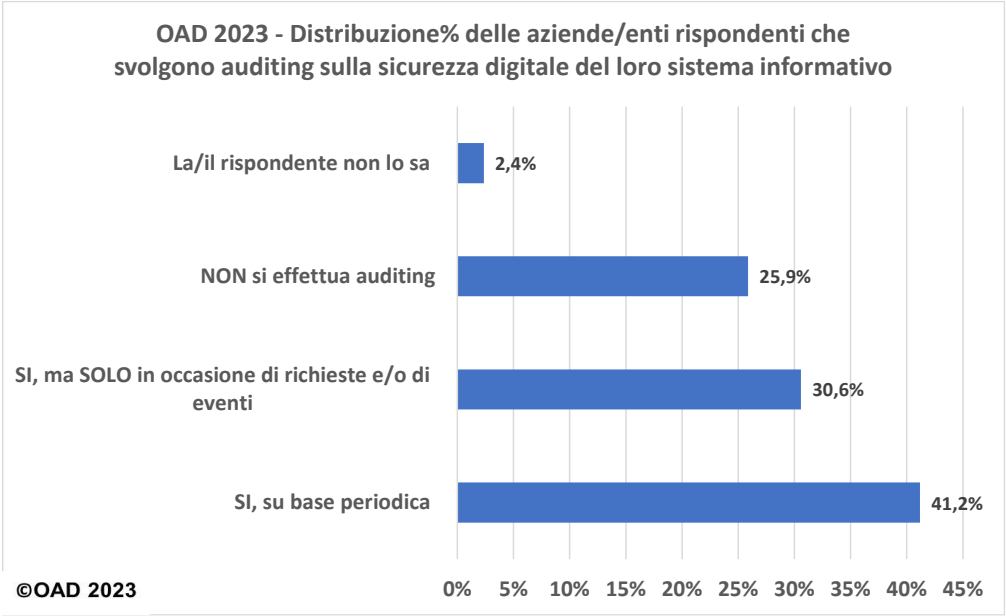


Fig. 7.1.4-1

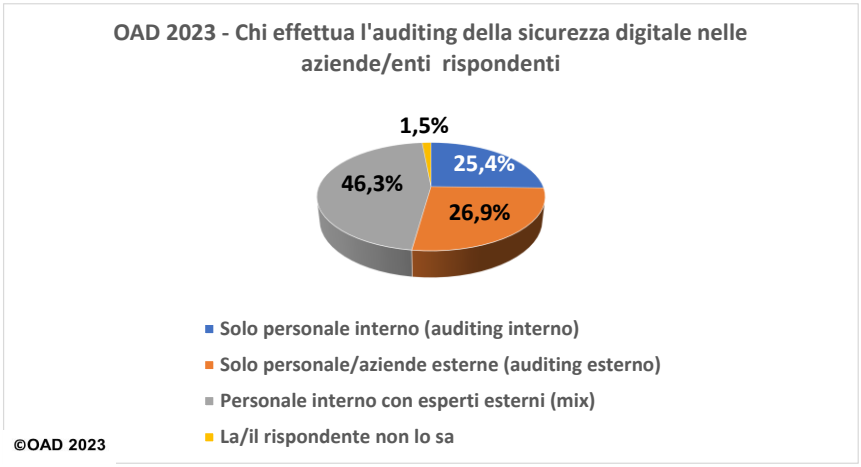


Fig. 7.1.4-2

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. Per i produttori di dispositivi informatici o che realizzano prodotti con sistemi digitali al loro interno, l'Unione Europea con il Cybersecurity Act (si veda $3.4) richiederà nel prossimo futuro la certificazione del livello di sicurezza digitale implementato, una specie di "Common Criteria" a livello europeo, così come specificato nel Titolo III dell'EU Cybersecurity Act (https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32019R0881).

La fig. 7.1.5-1 riporta la richiesta di specifiche certificazioni sulla sicurezza digitale da parte dell'azienda/ente per il suo personale interno, che se ne occupa. Il **60%** delle aziende/enti rispondenti non le richiede per il proprio personale; le richiede più di 1/3 dei rispondenti, una elevata percentuale, ma solo per i ruoli e le figure professionali più importanti e di riferimento nella sicurezza digitale dell'azienda/ente rispondente, quali ad esempio il CISO. Da sottolineare come nessuna azienda/ente rispondente richieda certificazioni individuali per tutto il suo personale coinvolto nella sicurezza digitale.

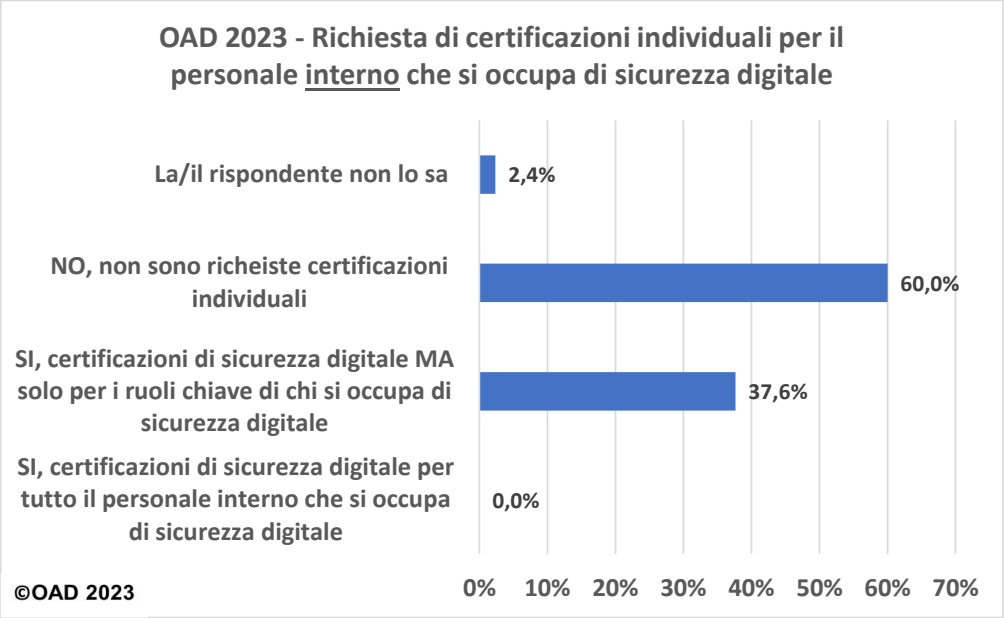


Fig. 7.1.5-1

Nei capitoli e nei paragrafi precedenti si è più volte evidenziata la tendenza a terziarizzare, in tutto in parte, la gestione della sicurezza digitale, il più delle volte con più fornitori. Questa terziarizzazione multipla, spesso indicata come "multi cloud", 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. 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.

La fig. 7.1.5-2 mostra che il **57,7%** dei rispondenti le richiede alle aziende/ente coinvolte, lato fornitori e clienti, nella sua supply chain, ed il **35.7%** di questi le richiede sia a livello aziendale che delle singole persone che interagiscono con il personale dell'azienda/ente.

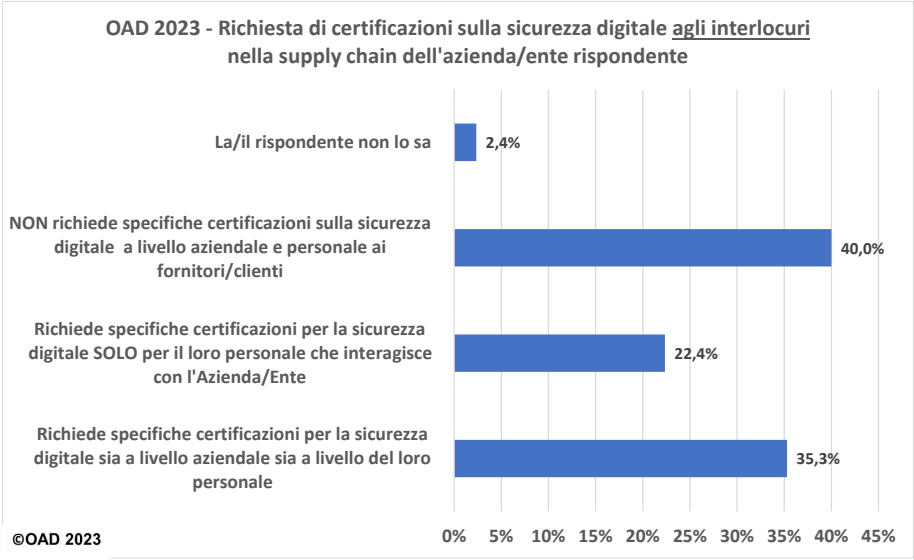


Fig. 7.1.5-2

Importante avere certificazioni aziendali sulla sicurezza digitale soprattutto per aziende/enti di specifici settori che forniscono servizi digitali essenziali per il funzionamento del sistema paese: per queste, che gestiscono infrastrutture critiche, talune certificazione saranno obbligatorie per poter soddisfare le norme delle già citate normative europee sulla cybersicurezza.
Quante sono tra le aziende/enti rispondenti a OAD 2023 quelle che già hanno certificazioni sulla sicurezza digitale? La fig. 7.1.5-3 fornisce la risposta: il **57,6%** non ne ha, ma di questi il 17,6% ha a piano di acquisirne a breve almeno una. Il **41,2%** ha certificazioni sulla sicurezza digitale ed il **34,1%** per l'intera organizzazione ed il suo sistema informativo.

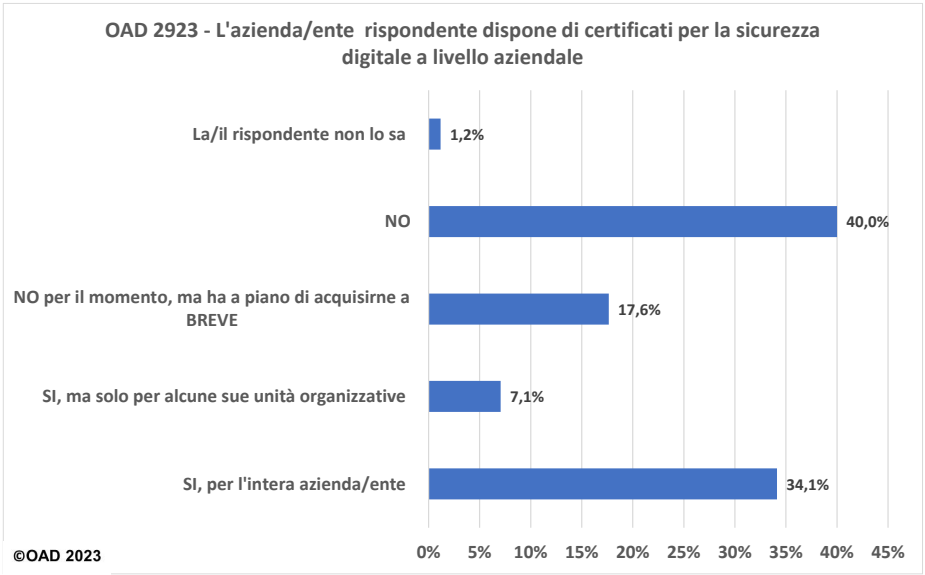


Fig. 7.1.5-3

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 compila il questionario troppo tempo e troppe specifiche competenze tecniche.

7.2.1 Architetture per la sicurezza digitale

La fig. 7.2.1-1 mostra le risposte al questionario relative alle architetture per la sicurezza digitale[47] definite ed implementate nei sistema informativo oggetto delle risposte: l'architettura è definita ed implementata nel **68,5%** dei sistemi informativi delle aziende/enti rispondenti, ma di questi il 37% solo per le sue parti più critiche.

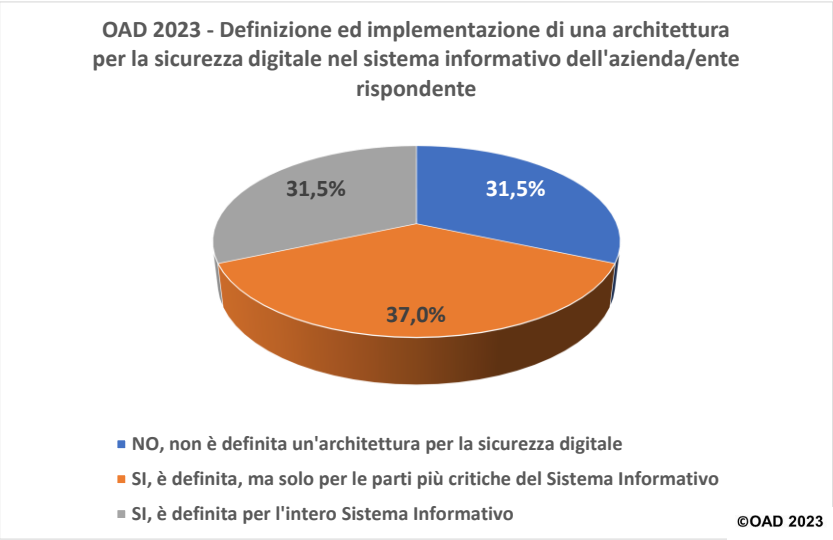


Fig. 7.2.1-1

[47] Le architetture per la sicurezza digitale si basano su standard e framework internazionali quali gli standard della famiglia ISO 27000, NIST, OSA (Open Security Architecture), CIS (Center for Internet Security), etc. Per le varie sigle/acronimi si rimanda al Glossario in Allegato B.

La fig. 7.2.1-2 mostra quali sono le architetture per la sicurezza digitale implementate nei sistemi informativi dei rispondenti.

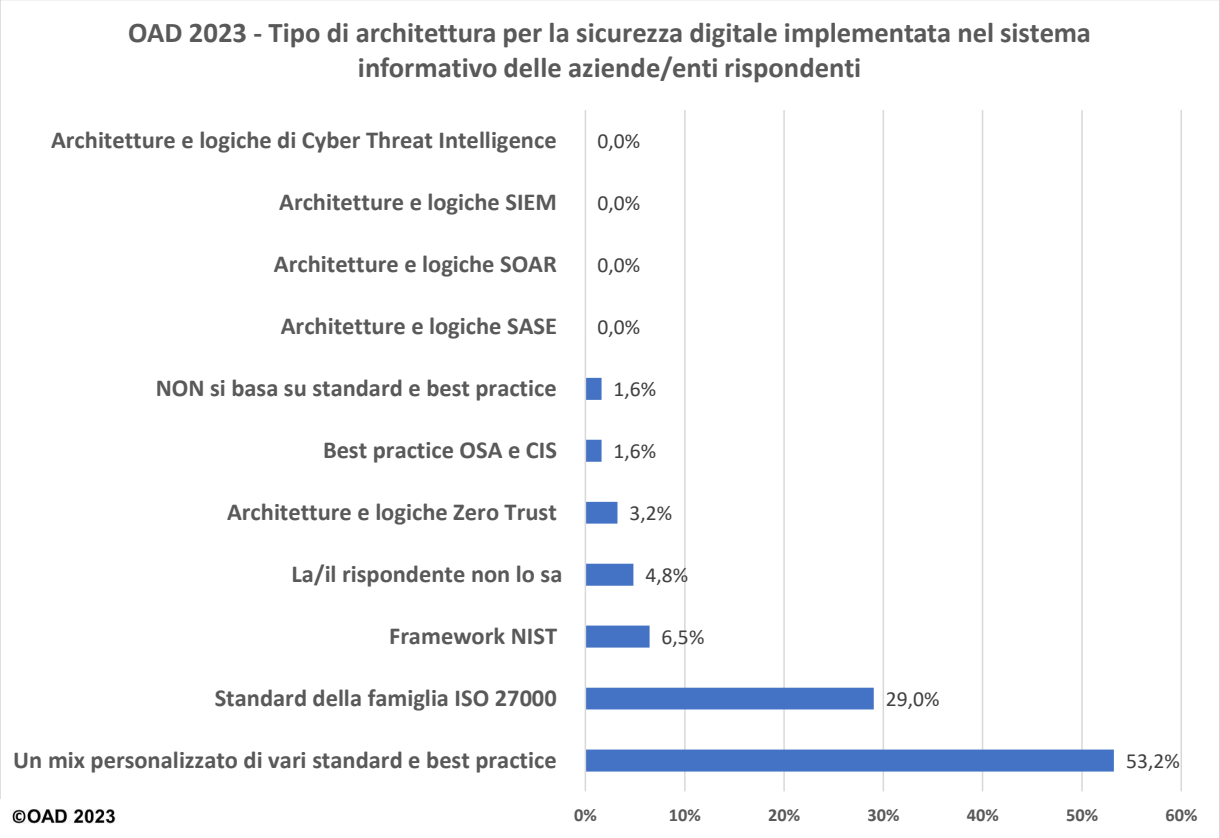


Fig. 7.2.1-2

Più della metà, il **53,2%**, ha adottato e personalizzo soluzioni che includono diverse logiche e architetture per la sicurezza. Al secondo posto, con un 29%, il riferimento agli standard della famiglia ISO 27000. Tutte le altre architetture di riferimento hanno percentuali nulle o minimali, anche perché nel questionario, per questa domanda, non si potevano selezionare risposte multiple. Quindi, per la maggior parte, SIEM, SASE, SOAR, e le altre architetture, se prese a riferimento, sono state incluse con altre nella voce "mix" di soluzioni che integrano più architetture.
L'architettura della sicurezza digitale gioca un ruolo basilare per garantire l'alta affidabilità e disponibilità del sistema informativo che la implementa. Più dei ¾ , il **76,1%**, dei sistemi informativi delle aziende/enti rispondenti sono in alta affidabilità, ma di questi meno della metà, il 31,5%, garantisce l'alta affidabilità a tutte le risorse ICT , mentre il 44,6% la garantisce solo alle risorse ICT più critiche ed importanti (fig. 7.2.1-3).

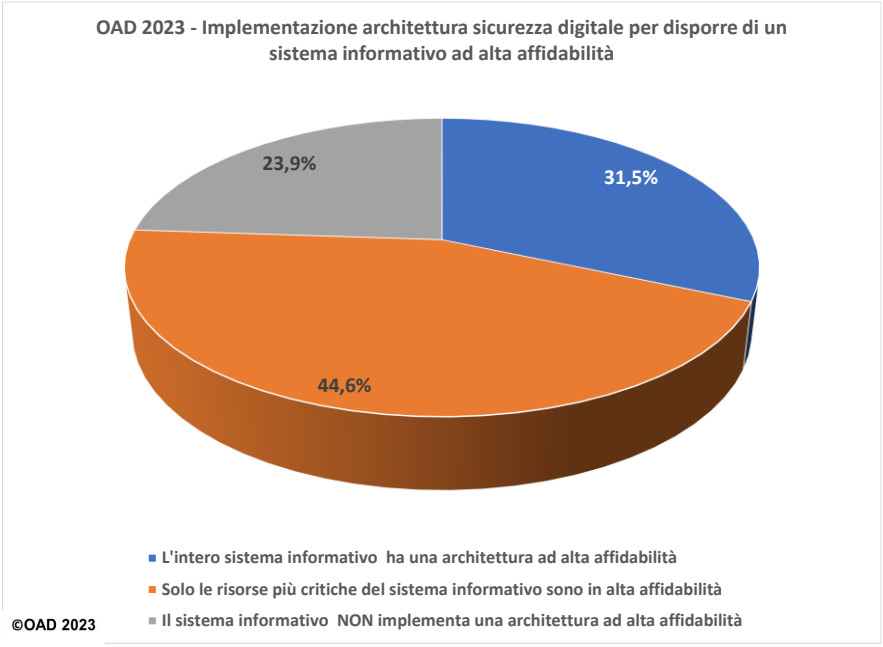


Fig. 7.2.1-3

Ulteriore domanda è il livello di affidabilità secondo lo standard ANSI/TIA 942[48] nelle architetture di sicurezza del sistema informativo con almeno un Data Center in Italia, oltre alla eventuale certificazione TIA di questo livello.
La fig. 7.2.1-4 mostra i livelli di affidabilità del principale Data Center in Italia secondo lo standard ANSI/TIA 942: la metà dei sistemi informativi delle aziende/enti che hanno risposto alle domande sulle misure tecniche dichiara che il principale Data Center in Italia del proprio sistema informativo è al Tier III, mentre per il 23,1% è di livello massimo, al Tier IV. In pratica i ¾ dei rispondenti hanno i loro principali Data Center in Italia con un elevato ed elevatissimo livello di affidabilità. Questo alto livello di affidabilità emerso dall'indagine è congruente con il settore merceologico delle aziende/enti rispondenti (si veda fig. 7-2) ed il ruolo del sistema informativo, 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. 3.4-1 e §3.4).
La fig. 7.2.1-5 indica che solo il 13,5% dei principali Data Center in Italia dei sistemi informativi delle aziende/enti rispondenti è certificato ANSI/TIA 942.

[48] 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.

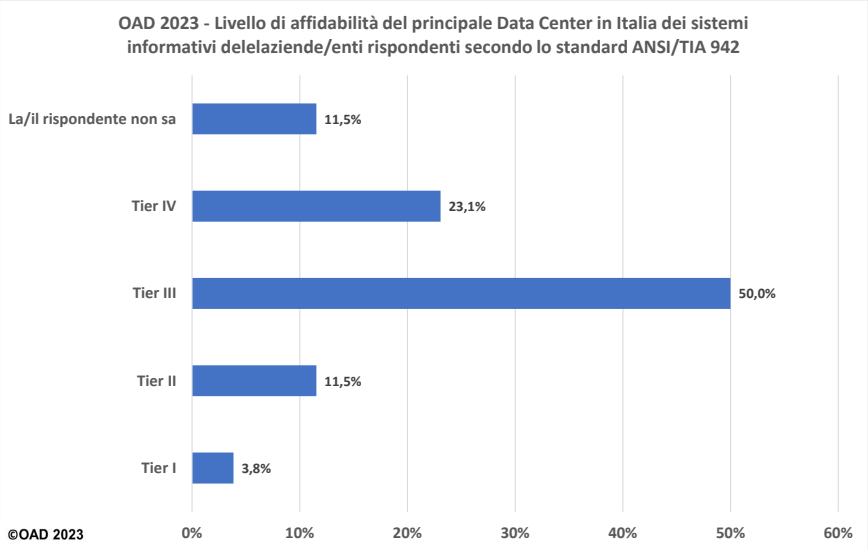


Fig. 7.2.1-4

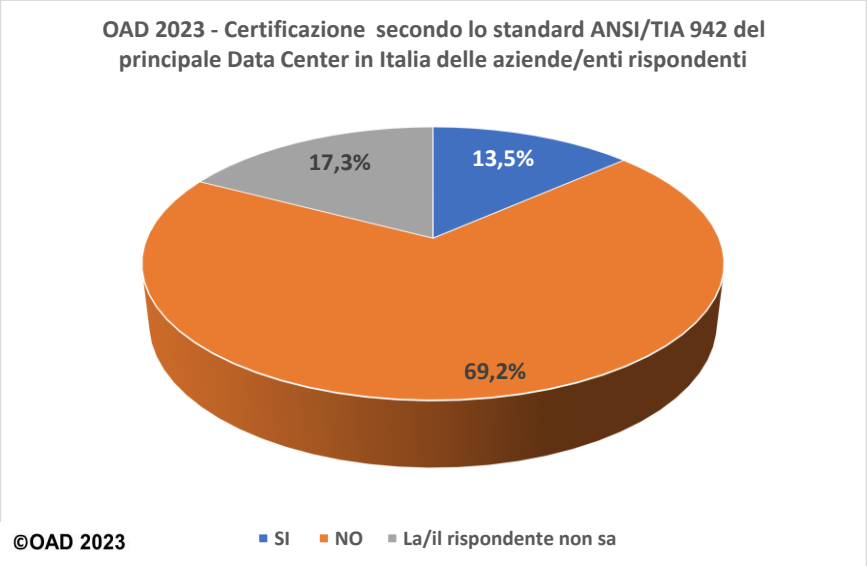


Fig. 7.2.1-5

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 nel seguito viene chiamata da OAD computer room[49], e alla quale possono, o dovrebbero poter accedere solo un numero ristretto di persone, tipicamente l'amministratore dei sistemi ICT ed il personale esterno per la manutenzione dei dispositivi; 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 fig. 7.2.2-1 mostra la situazione emersa dalle aziende/enti rispondenti per la **sicurezza fisica ed i relativi controlli**: nella maggior parte dei casi, il **71,7%**, sono previste misure per il controllo dell'**accesso fisico** di persone nei locali con sistemi ICT, a parte l'eventuale Data Center.

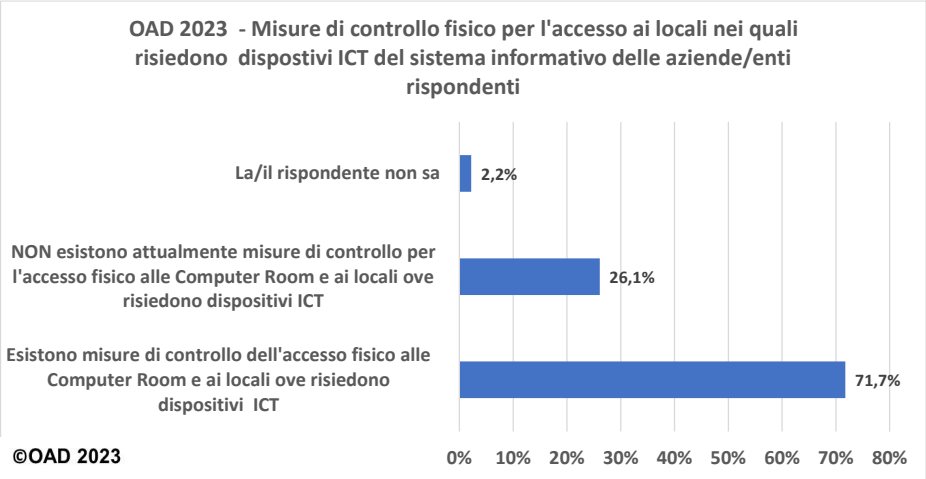


Fig. 7.2.2-1

Sempre escludendo i Data Center, la fig. 7.2.2-2 mostra che nell'**83,5%** dei casi emersi dall'indagine sono in funzione sistemi di controllo perimetrale[50] nei locali/computer room ove risiedono sistemi ICT, e di questi il 35,2% li ha in funzione **in tutti** i locali/computer room con sistemi ICT (esclusi i dispositivi d'utente quali i PC) , mentre il 48,4 % li ha in funzione **solo** per i locali/computer room con i sistemi ICT **più critici**, ad esempio quelli che supportano applicazioni di gestione del personale, sistemi AFC o ERP, CRM, SCM.

Dopo il controllo fisco degli accessi ed i controlli perimetrali, un'altra importante misura che OAD fa rientrare nella sicurezza fisica è quella dei sistemi di controllo e prevenzione di interruzioni dell'energia elettrica (black out energetico) per l'alimentazione dei sistemi ICT nelle computer room e negli altri locali (non dell'eventuale Data Center per il quali si dà per scontato che esistano queste misure di sicurezza) con l'attivazione di gruppi di continuità, indicati per brevità con l'acronimo UPS (Uninterruptible Power Supply).

[49] Le computer room, nel caso di sistemi informativi distribuiti sul territorio, sono gli ambienti dipartimentali dei sistemi informativi di medie o grandi dimensioni.
[50] 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.

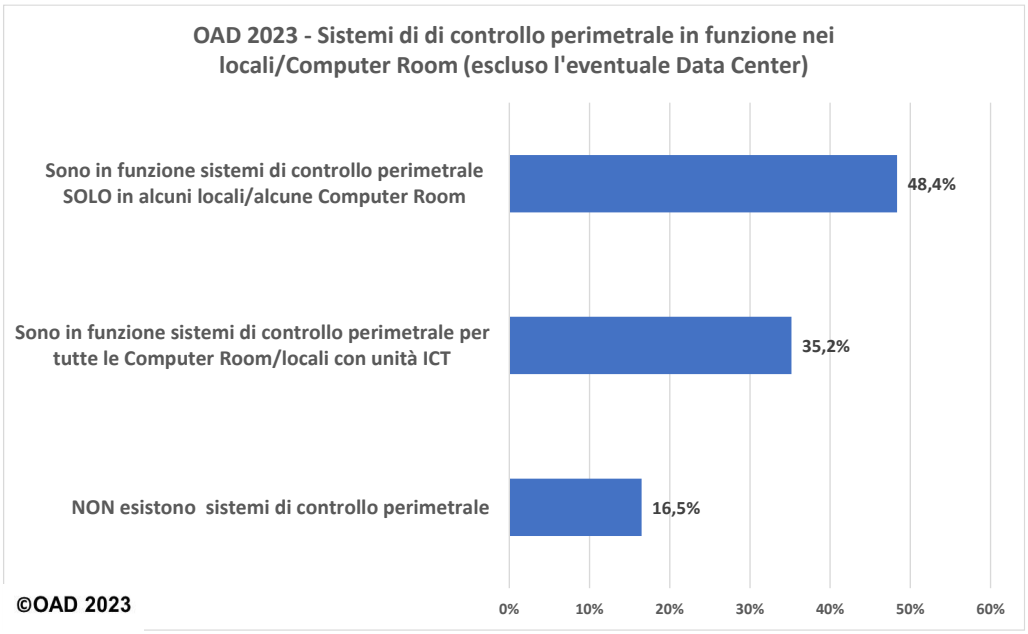


Fig. 7.2.2-2

Per i Data Center, specie quelli di maggiori dimensioni, sono anche usati generatori alternativi di corrente, con UPS che mantengono la corrente fino a che il generatore alternativo non si è attivato. Come indicato nella 7.2.2-3, a parte i Data Center, più di 2/3 delle aziende/enti rispondenti, il **77,8%**, dispone di UPS nei locali/computer room, ma di questi il 44,4% li ha in funzione solo nei locali con i sistemi ICT più critici.

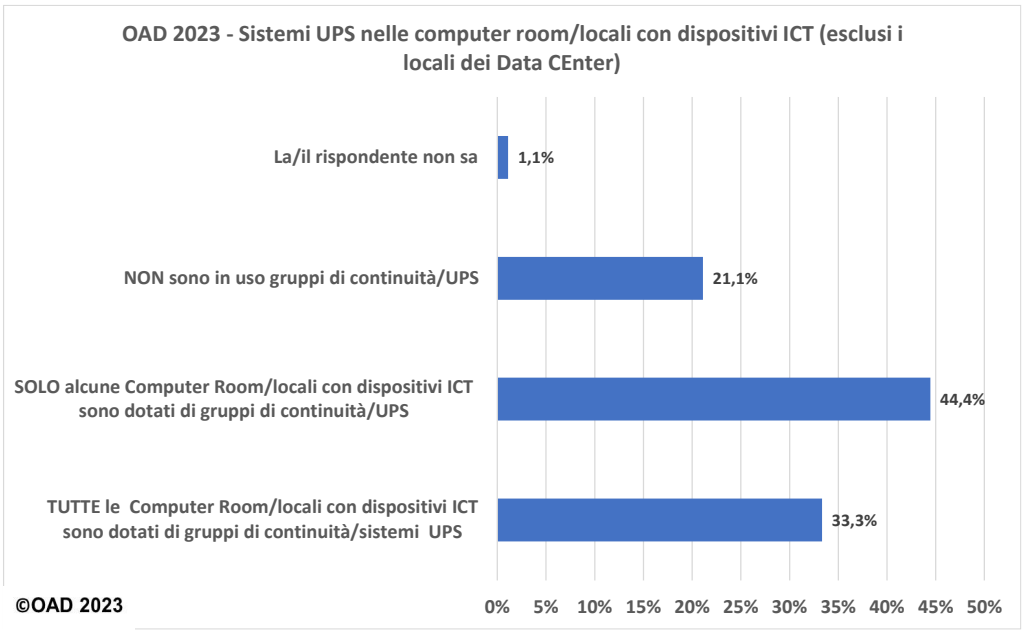


Fig. 7.2.2-3

Oltre che nei Data Center, la sistemazione in rack[51] dei vari sistemi ICT (switch, router, server, 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. **Più del 90%** delle aziende/enti rispondenti utilizza rack nelle computer room e negli altri locali nei quali sono allocati dispositivi ICT, a parte l'eventuale Data Center. La fig. 7.2.2-4 dettaglia le varie modalità d'uso dei rack, ed è significativo che la percentuale più alta di questi, il 35,2%, li ha attivati in tutti i locali e computer room.

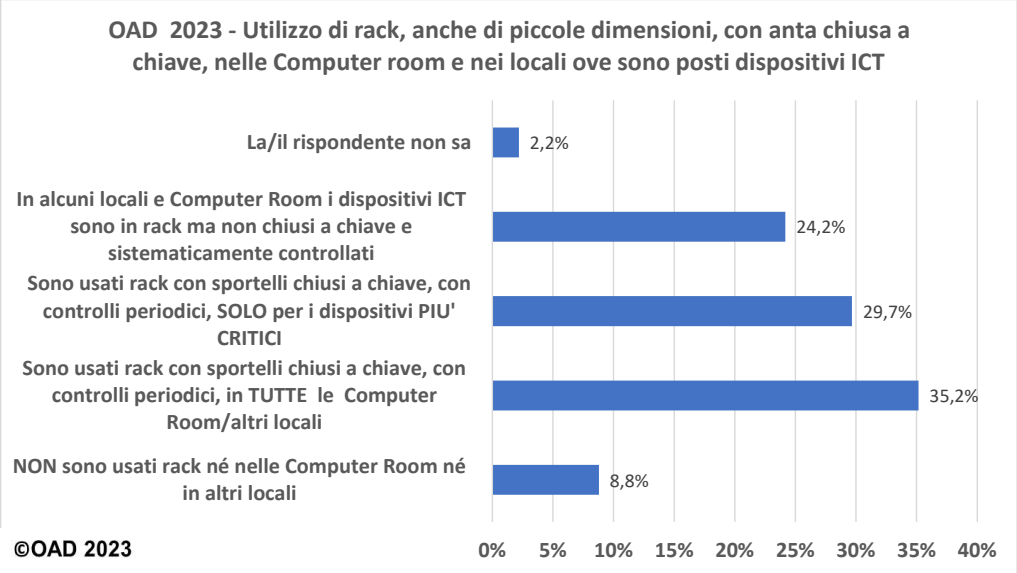


Fig. 7.2.2-4

Per ridurre la possibilità di furto dei PC, soprattutto i lap top, e delle 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, l'**83,3%**, come riportato nella fig. 7.2.2-5. Solo il 16,7% utilizza questi strumenti, ma di questi 13,3% solo per PC e workstation più critici e più costosi.

[51] 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.

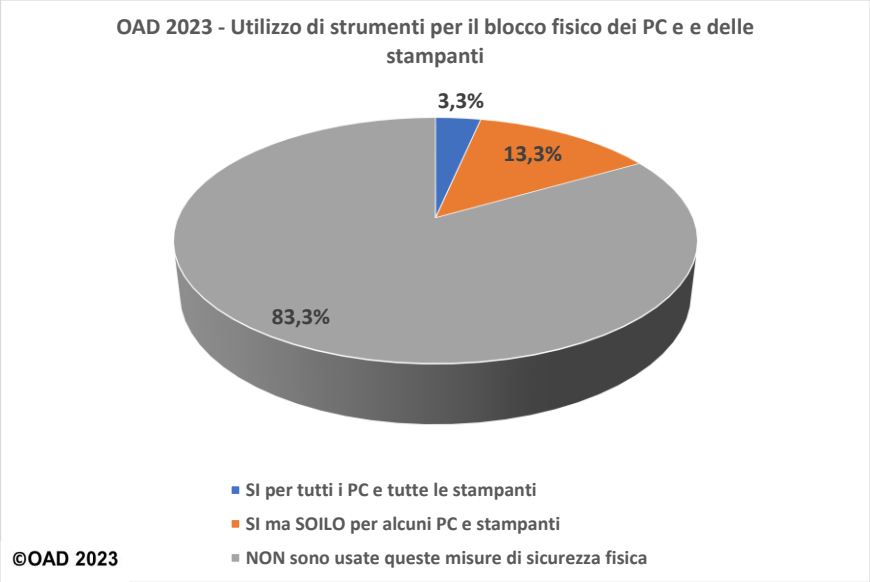


Fig. 7.2.2-5

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[52] (questi ultimi sono gli amministratori-operatori ICT, i manutentori, gli sviluppatori software, che hanno tutti dei particolari privilegi di accesso) sono fondamentali per l'effettiva protezione di un sistema informativo, tenendo anche conto che gli attacchi digitali all'IAA sono i più diffusi per OAD 2021 (si veda §4) ed anche nelle indagini dei quattro anni precedenti (20220, 2019, 2018 e 2017).

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[53], 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 prima domanda nell'ambito IAA di OAD 2023 è relativa all'uso dell'autenticazione forte/quasi forte per gli utenti privilegiati, ed i risultati emersi sono raffigurati nella fig. 7.2.3-1.

[52] 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.

[53] 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.

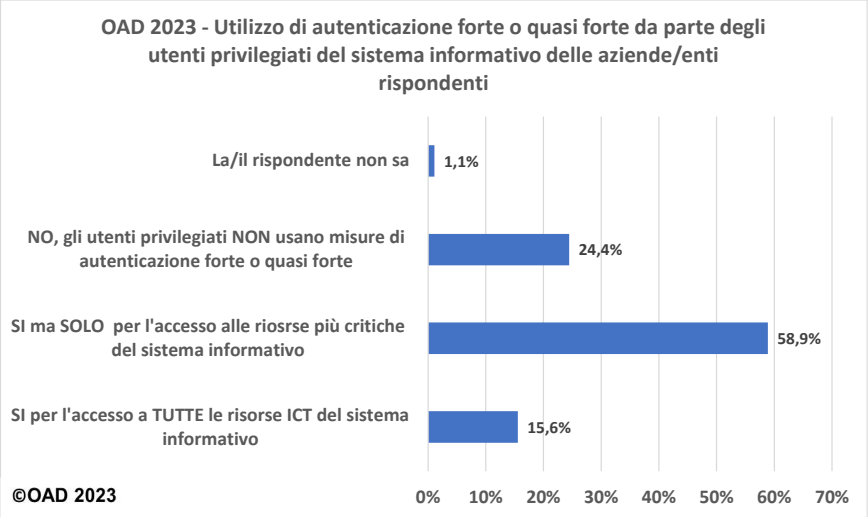


Fig. 7.2.3-1

Quasi i 2/3, **74,4%,** dei sistemi informativi rispondenti obbliga gli utenti privilegiati ad usare tecniche di autenticazione forte o quali forte, ma di questi solo il 15,6% per ogni risorsa ICT, ed il restante 58,9% solo per le risorse ICT più critiche. Per l'autenticazione degli utenti finali, come mostrato nella fig. 7.2.3-2, la maggior parte dei sistemi informativi, il **61,1%**, consente l'utilizzo di diverse tipologie a seconda del tipo di applicativo, prevalentemente in funzione della sua criticità e riservatezza per le informazioni trattate, e in certi casi per il ruolo dell'utente finale. Un terzo circa dei sistemi informativi delle aziende/enti rispondenti, *32,2%*, utilizza solo autenticazione debole. Trascurabili le percentuali di chi utilizza per ogni ambiente applicativo l'autenticazione forte, o lo SPID (questo anche per il limitato numero di PA rispondenti), o di chi delega l'autenticazione ai servizi dei principali service provider come Google, o infine di chi sta introducendo autenticazioni biometriche, quali Fido2, anche per il sostanziale loro divieto in Europa da parte dei vari Garanti nazionali della privacy.

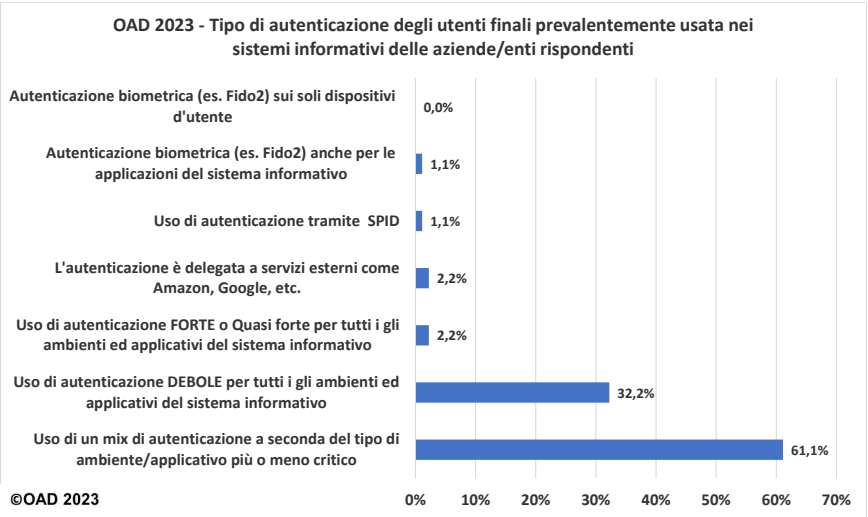


Fig. 7.2.3-2

.

Il tipo e la gestione delle password degli utenti finali e privilegiati è un annoso problema, di fatto per la gran parte ancora aperto. Problema parzialmente rimediabile con autenticazioni forti/quasi forti e con l'uso di PIN[54], che sono codici più facili e corti da ricordare rispetto ad una password alfanumerica, con caratteri speciali, e che dovrebbe essere lunga come minimo 12-14 caratteri, con l'uso di token (smart card, chiavette USB, etc.) e in prospettiva con l'identificazione biometrica, una volta superati i forti ostacoli in Europa per la privacy, che già è in grado di implementare sistemi "senza password" (passwordless)[55]. Nonostante un elevato numero di piccole e piccolissime organizzazioni rispondenti ad OAD 2023, i risultati dell'indagine su questo argomento sono sorprendentemente positivi.
Come mostrato in fig. 7.2.3-3 la gestione delle password è **centralizzata** per tutti gli utenti nel **53,3%** dei sistemi informativi, ed è invece lasciata alle decisioni del singolo utente, privilegiato o finale, nel **26,7%**. Nel **18,9%** dei sistemi informativi è centralizzata solo la gestione delle password degli utenti privilegiati. Un piccolo numero di sistemi informativi sta usando/provando tecniche passwordless.

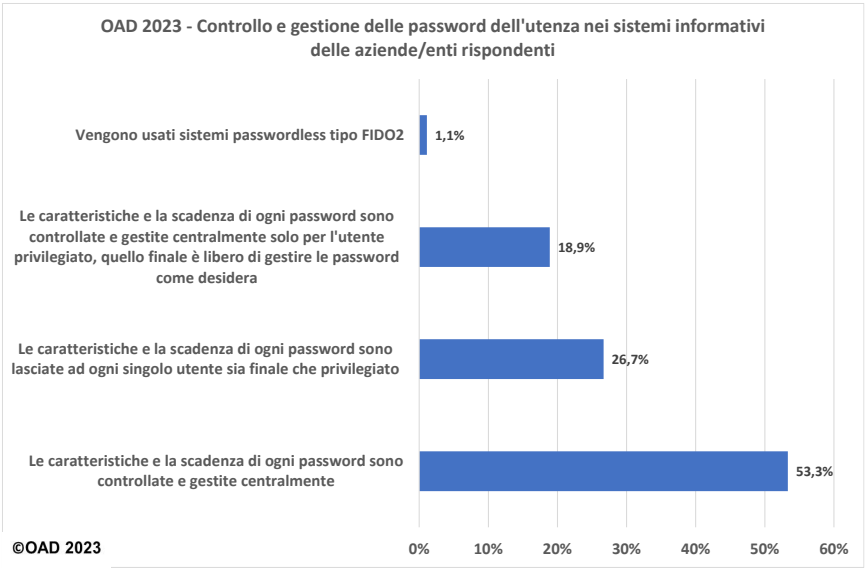


Fig. 7.2.3-3

Data l'importanza e l'ancora forte criticità per la gestione delle password, si sono correlati i dati di cui sopra con le dimensioni (numero di dipendenti) delle aziende/enti rispondenti: il risultato è rappresentato in fig. 7.2.3-4. Le barre verticali blu rappresentano la distribuzione percentuale dei sistemi informativi che lasciano la gestione delle password ai singoli utenti: e come prevedibile, queste barre si addensano sulle piccole organizzazioni, ma ce ne sono anche in organizzazioni tra i 251-1000 dipendenti. Le barre grige rappresentano la distribuzione percentuale dei sistemi informativi che controllano e gestiscono centralmente le password: sono presenti in tutte le classi di dipendenti, e chiaramente prevalenti nei sistemi informativi anche di medio piccole dimensioni, dai 50 dipendenti in su, e non solo nelle grandi e grandissime.

[54] 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 (Wikepidia).
[55] 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, che ovviamente ne frena fortemente l'uso e la diffusione. Tra le principali tecniche e metodiche per l'autenticazione biometrica è di riferimento il Progetto open source FIDO2, https://fidoalliance.org/fido2/

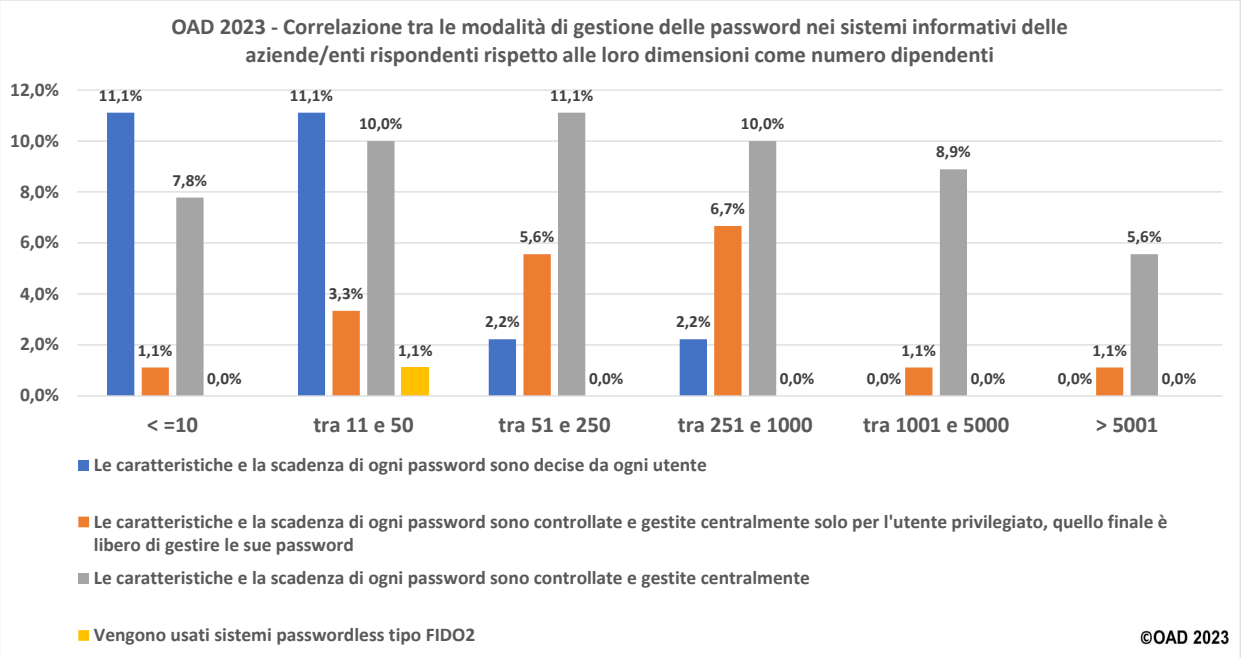


Fig. 7.2.3-4

Anche le barre marroni, che rappresentano il controllo centralizzato solo degli utenti privilegiati, sono presenti in tutte le classi di dimensione, ma con percentuali ben più piccole. Da evidenziare come le poche aziende/enti che stanno utilizzando sistemi passwordless rientrano tutte nella classe 11-50 dipendenti, si veda l'unica barra gialla presente in figura: sono probabilmente start up o piccoli centri di ricerca che stanno provando e utilizzando tali soluzioni.
Come già ricordato in precedenza, i dati emersi dalle correlazioni dipendono anche dal numero di rispondenti per i vari temi considerati, in primis le classi di aziende/enti per numero di dipendenti: devono essere pertanto considerati come indicatori delle tendenze considerate nella correlazione stessa.

7.2.4 Misure tecniche di sicurezza delle reti dei sistemi informativi

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.

La fig. 7.2.4-1 evidenzia come più di un 1/3, **35,6%**, dei sistemi informativi dei rispondenti hanno **tutte** le connessione ad Internet dupplicate/ennuplicate per garantirne una alta affidabilità e disponibilità, mentre il 22,1% dei sistemi informativi, prevalentemente di piccole organizzazioni, non ha connessioni multiple. Il rimanente dei sistemi informativi ha connessioni multiple solo per quelle più importanti e critiche.
Come riportato nella fig. 7.2.4-2, 2/3 dei sistemi informativi, il **66,7%,** monitora e controlla centralmente funzionalità, prestazioni e livelli di sicurezza digitale delle proprie reti "interne", con l'utilizzo di specifici strumenti quali DMZ, FireWall, IPS/IDS, VPN, e così via. Il **33,3%** non controlla centralmente le proprie reti, ma di questi solo il 10% non utilizza specifici strumenti di sicurezza digitale come quelli indicati. Interessante sottolineare come **nessuno** dei sistemi informativi con controllo centralizzato delle proprie reti **non** utilizza specifici strumenti di sicurezza.

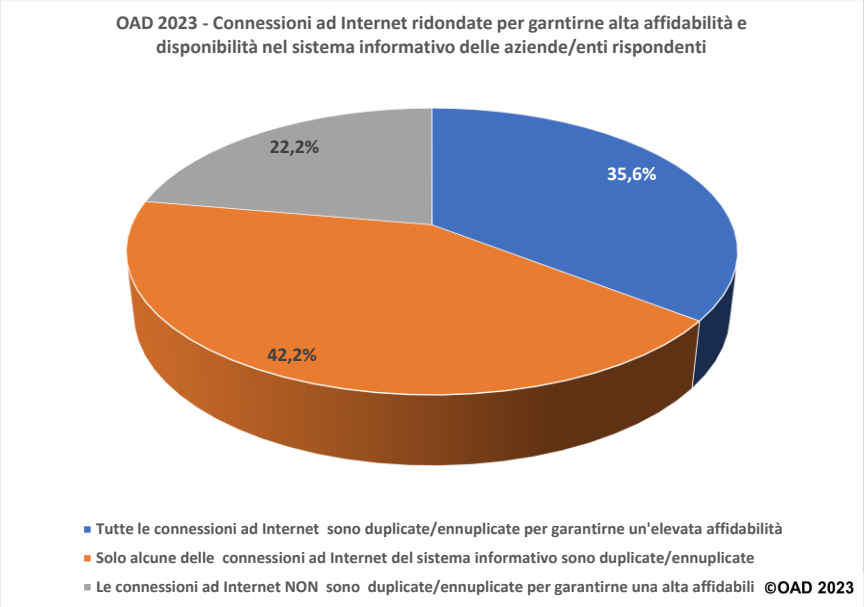


Fig. 7.2.4-1

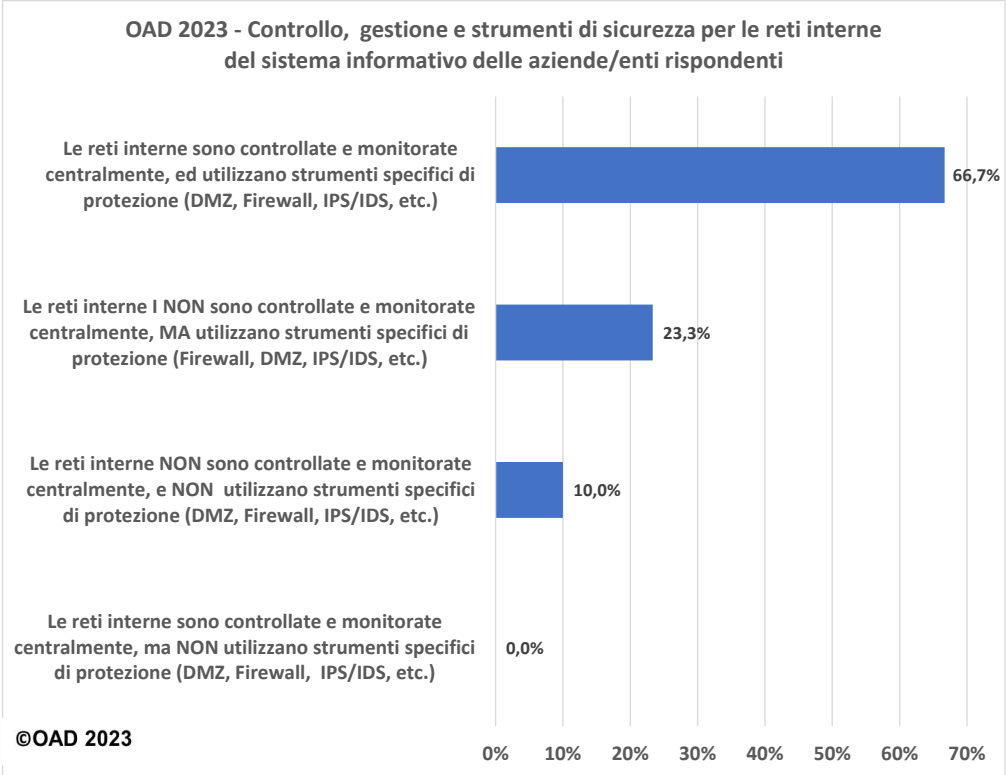


Fig. 7.2.4-2

La fig. 7.2.4-3 evidenzia che per quasi il **90%** dei sistemi informativi delle aziende/enti rispondenti il traffico interno e quello con/da Internet **è crittografato**, prevalentemente con IPSec, quindi per i siti web con HTTPS.

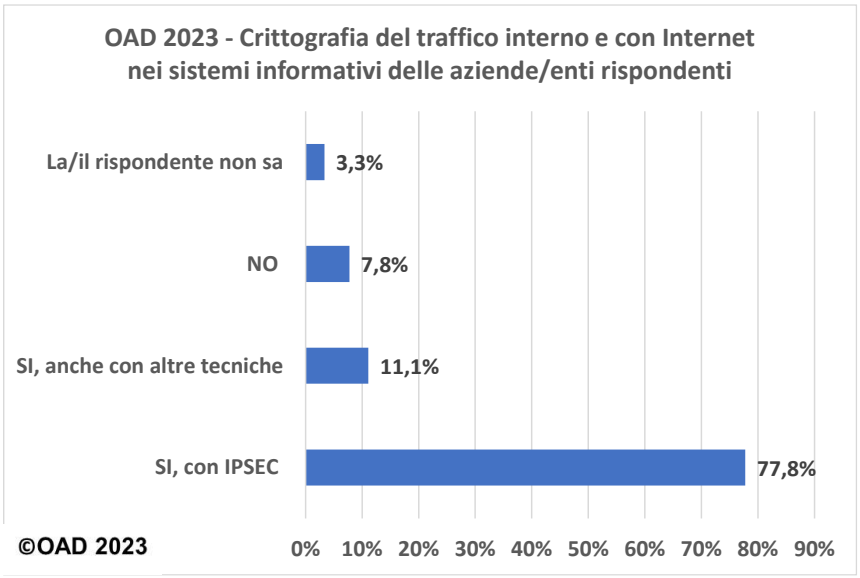


Fig. 7.2.4-3

Interessante il risultato emerso sull'uso di specifici servizi in cloud per potenziare il livello di sicurezza delle reti dei sistemi informativi delle aziende/enti rispondenti, quali ad esempio i servizi delle architetture SASE, che consentono di far fronte ad attacchi tipo Dos/DDos. Il risultato è mostrato nella fig. 7.2.4-4: la maggior parte, il 64%, dei sistemi informativi non utilizza questi servizi, ma il 25,8, ¼ circa, sì. Relativamente alta la percentuale dei "non so", dovuta quasi certamente ad una domanda tecnica su una relativamente nuova tecnica.

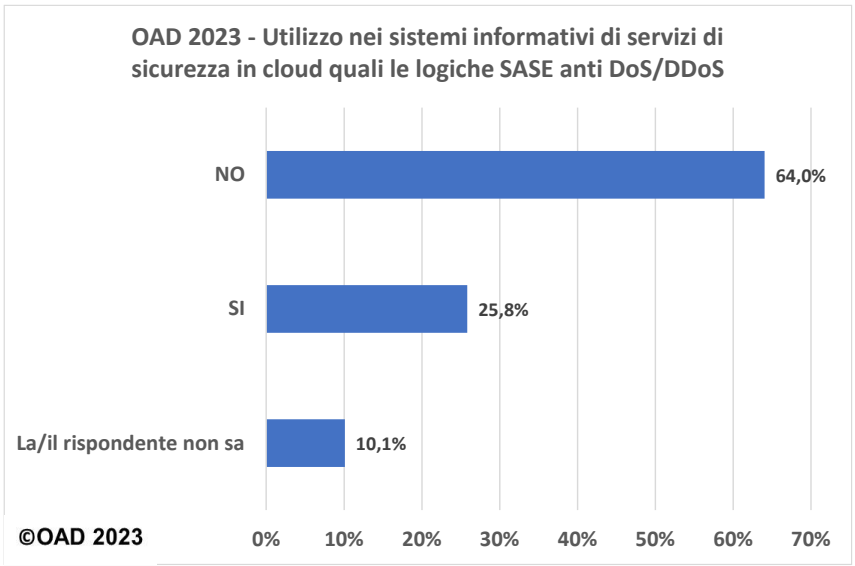


Fig. 7.2.4-4

7.2.5 Misure di sicurezza delle applicazioni nei sistemi informativi

Le contromisure 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 applicazioni commerciali, soprattutto per le PMI, questa dovrebbe essere garantita dal fornitore.
Questa è la volontà dell'Unione Europea che con il già citato Cybersecurity Act (si veda §3.4) intende che ogni prodotto software, o con software interno (emebedded) perché funzioni, sia certificato da appositi enti europei, in un logica tipo Common Criteria di tipo europeo.

La sicurezza del software può essere corrotta da errate installazioni e configurazioni, da aggiunte per l'integrazione e l'interoperabilità con altre applicazioni. Per i software commerciali, poi, in tempi di crisi economica come l'attuale, non vengono talvolta rinnovati i contratti per la loro manutenzione correttiva ed evolutiva, lasciando così in produzione nei sistemi informativi software non aggiornati, e quindi vulnerabili e facile preda degli attaccanti.

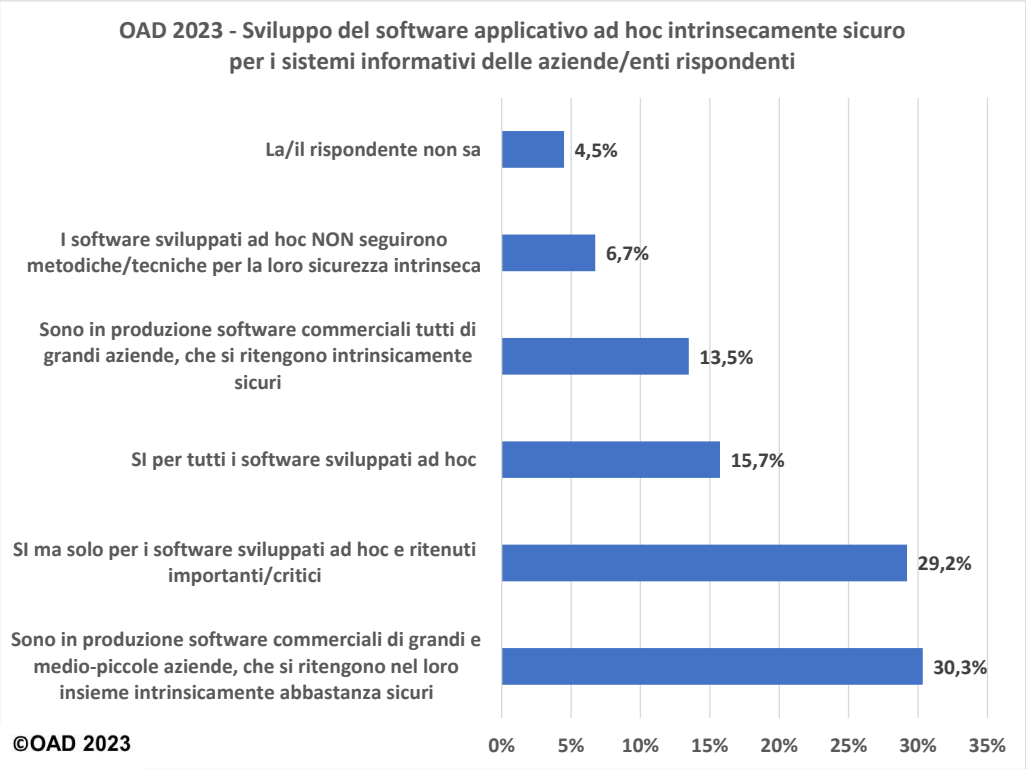


Fig. 7.2.5-1

La fig. 7.2.5-1 mostra che il **43,8%** 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. Di questi, il 29,2% dichiara che tale sviluppo digitalmente sicuro è stato effettuato solo per gli applicativi più importanti e più critici per l'azienda/ente. Una percentuale simile ma leggermente maggiore di un punto circa, il **44,9%,** non ha sviluppato applicazioni software ad hoc, ma ha acquisito e posto in produzione applicativi commerciali di note case produttrici, e che sono ritenuti intrinsecamente sicuri o abbastanza sicuri.

Si ricorda che volutamente, per semplificare e velocizzare la compilazione del questionario OAD 2023, si sono poste poche domande sul complesso ed assai ampio tema della sicurezza delle applicazioni: poche ma tali da poter rilevare su questo argomento la tendenza delle aziende/enti rispondenti, e dei loro sistemi informativi.

La seconda domanda riguarda la verifica ed il test della sicurezza del codice software prima della sua messa in produzione, e le risposte emerse sono nella fig. 7.2.5-2: il **73%** del software viene verificato/testato prima della sua messa in produzione, una percentuale veramente alta, e di questi il 58,4% riguarda verifiche e test solo delle applicazioni considerate più importanti e critiche.

Il controllo degli accessi e delle autorizzazioni nei vari applicativi è un altro elemento basilare per la loro sicurezza. La fig. 7.2.5-3 evidenzia che **in tutti** i sistemi informativi emersi dall'indagine OAD sono attivi strumenti di controllo degli accessi e delle autorizzazioni, ma questi controlli sono effettuati solo per gli applicativi più importanti nel **64%** dei sistemi informativi.

Uno degli strumenti più efficaci nella protezione degli applicativi in produzione è l'uso di **FWA, Firewall Applicativi**. La fig. 7.2.5-4 mostra che il **50,6%** dei sistemi informativi li usa, ma il 39,3 % solo davanti ai server che supportano gli applicativi più importanti e/o più critici per l'azienda/ente rispondente.

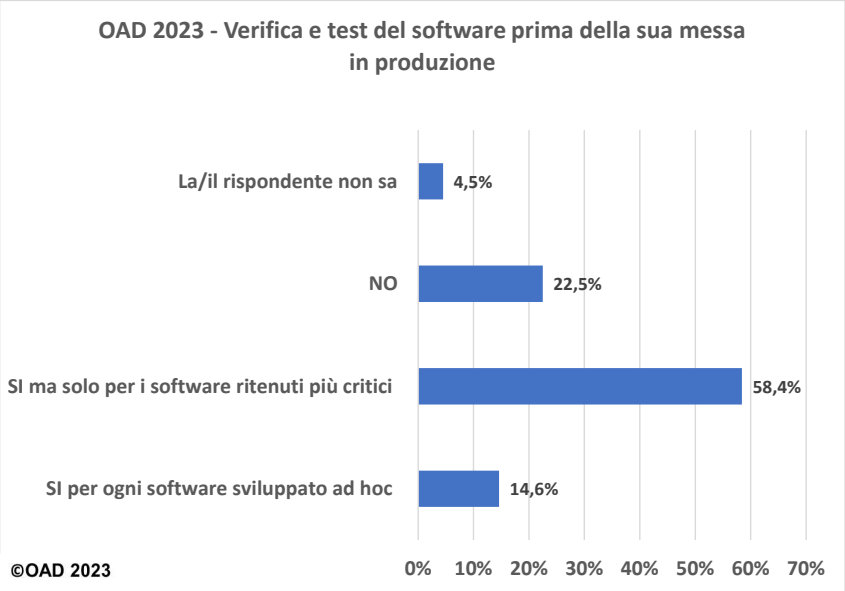


Fig. 7.2.5-2

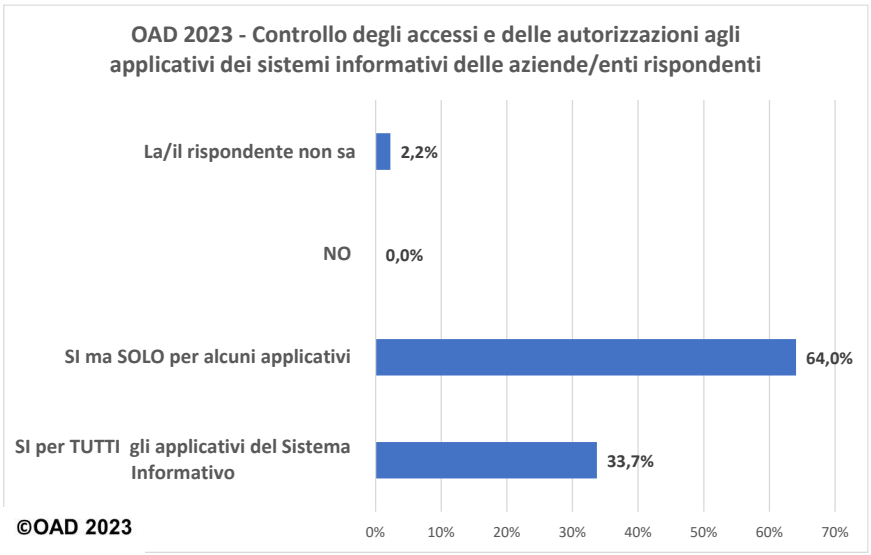


Fig. 7.2.5-3

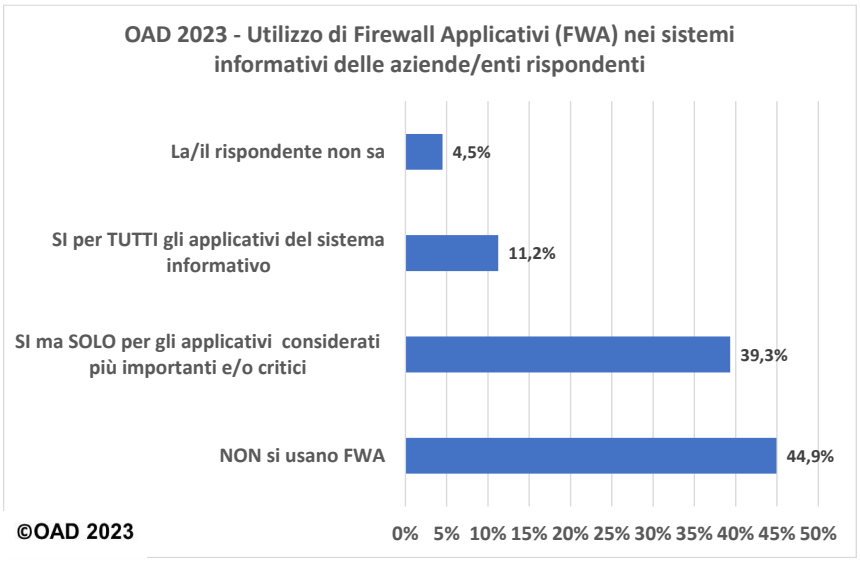


Fig. 7.2.5-4

Un altro aspetto fondamentale per la sicurezza digitale degli applicativi è la loro continua **manutenzione** correttiva: tempestivo aggiornamento delle versioni rilasciate, installazione tempestiva di fix e patch, e così via. La fig. 7.2.5-5 mostra che il **91%** delle aziende/enti rispondenti gestisce la manutenzione correttiva degli applicativi, anche a livello contrattuale con le Terzi Parti di sviluppatori/rivenditori coinvolte: di questi il **55,1%** la effettua per tutti gli applicativi operanti nel sistema informativo.

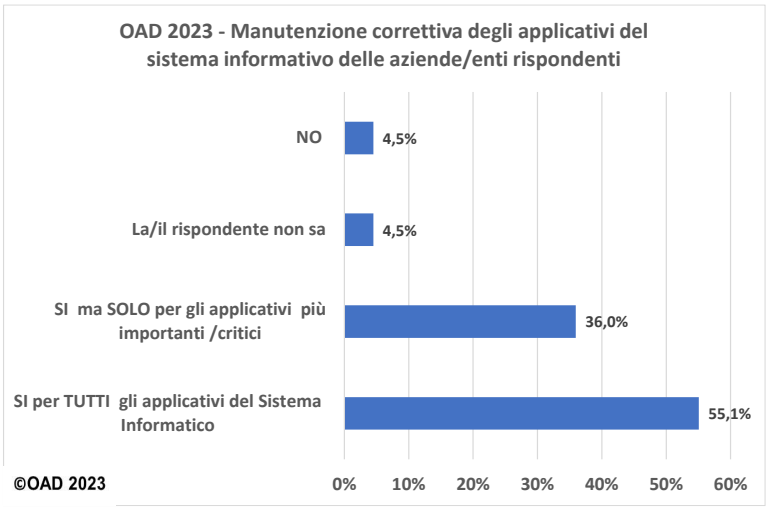


Fig. 7.2.5-5

7.2.6 Misure tecniche di sicurezza digitale per la protezione dei dati

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.

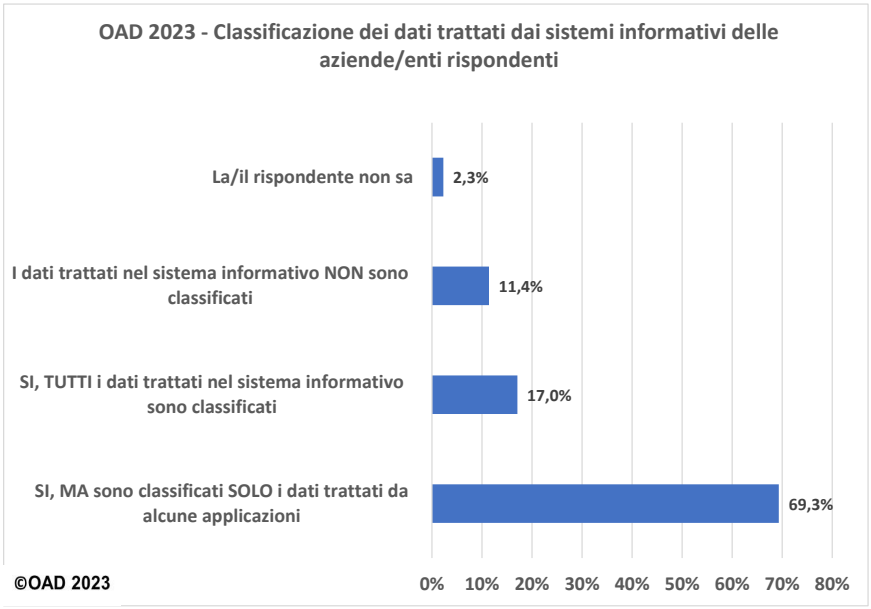


Fig. 7.2.6-1

La situazione della classificazioni dei dati per i sistemi informativi delle aziende/enti rispondenti è evidenziata nella fig. 7.2.6-1. L'**86,4%** dichiara di aver classificato i dati, e di questi il 69,3% dichiara di averlo fatto solo per i dati trattati da

alcune applicazioni: tipicamente dati personali, confidenziali per il business e/o per le attività, etc. L'11,4% non li ha (ancora) classificati, e questo dato, che anche grazie alle norme sulla privacy dovrebbe tendere a zero, è ragionevole nell'indagine OAD 2023 dato l'elevato numero di piccole e piccolissime aziende/enti rispondenti.

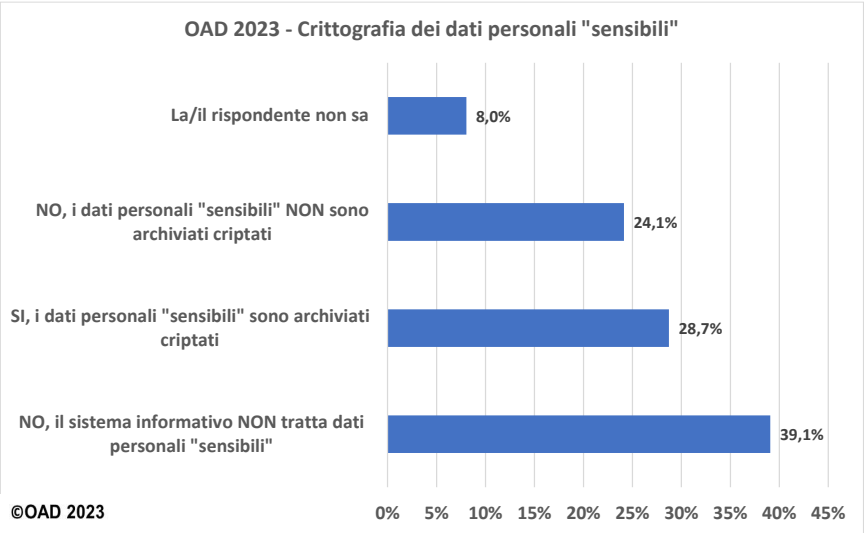


Fig. 7.2.6-2

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. 7.2.6-2 riporta la situazione sul trattamento dei dati personali, in particolare di quelli "sensibili"[56]: il **39,1%** dei sistemi informativi delle aziende/enti rispondenti non trattano dati personali sensibili ed il 28,7 % che li tratta, li cripta anche.
Vengono poi criptati dati ritenuti riservati e confidenziali, non di tipo personale, dal **41,4%** delle aziende/enti rispondenti, come mostrato nella fig. 7.2.6-3.

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

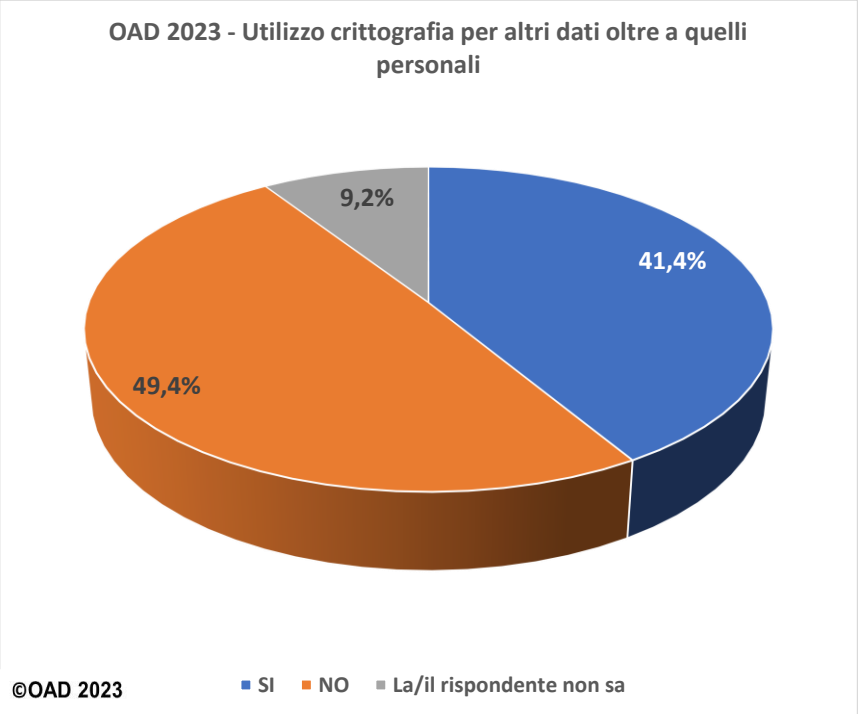


Fig. 7.2.6-3

Le chiavette USB sono un comodo strumento per copiare file, e date le loro attuali grandi dimensioni, 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. Ulteriore rischio è che la chiavetta può essere facilmente persa o a sua volta rubata, e se non ha dati criptati il rischio di perdita di dati è veramente alto.

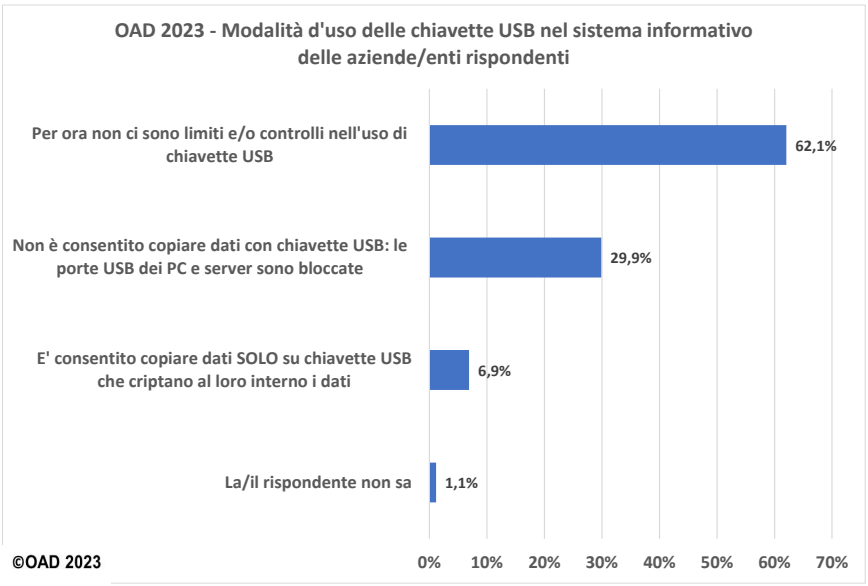


Fig. 7.2.6-4

La fig. 7.2.6-4 mostra che la maggior parte, **il 62,1%**, delle porte USB nei dispositivi ICT dei sistemi informativi emersi dall'indagine sono liberamente utilizzabili, anche se è possibile bloccarle configurando opportunamente lo stesso sistema ICT. Ma **quasi il 30%** dei sistemi informativi delle aziende/enti rispondenti con porte USB bloccate nei dispositivi è un dato significativo, indice che il problema della gestione delle chiavette USB a livello business inizia ad essere affrontato.

Il **backup** è una essenziale misura per la protezione dei dati e dei programmi di un sistema informativo, e nelle precedenti indagini OAD si era rilevato come molte aziende/enti rispondenti lo effettuassero parzialmente e/o in maniera poco professionale.
La fig. 7.2.6-5 riporta i dati emersi dalla presente indagine: il **44,8%** 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 27,6% effettua regolarmente i backup, ma non cripta le copie e non trasferisce questi dati su media removibili, allocandole poi in diverse sedi. Il 18,4% non gestisce in maniera omogenea ed automatizzata il backup, e nessuno ha risposto alla voce "è lascia la responsabilità del backup al singolo utente".

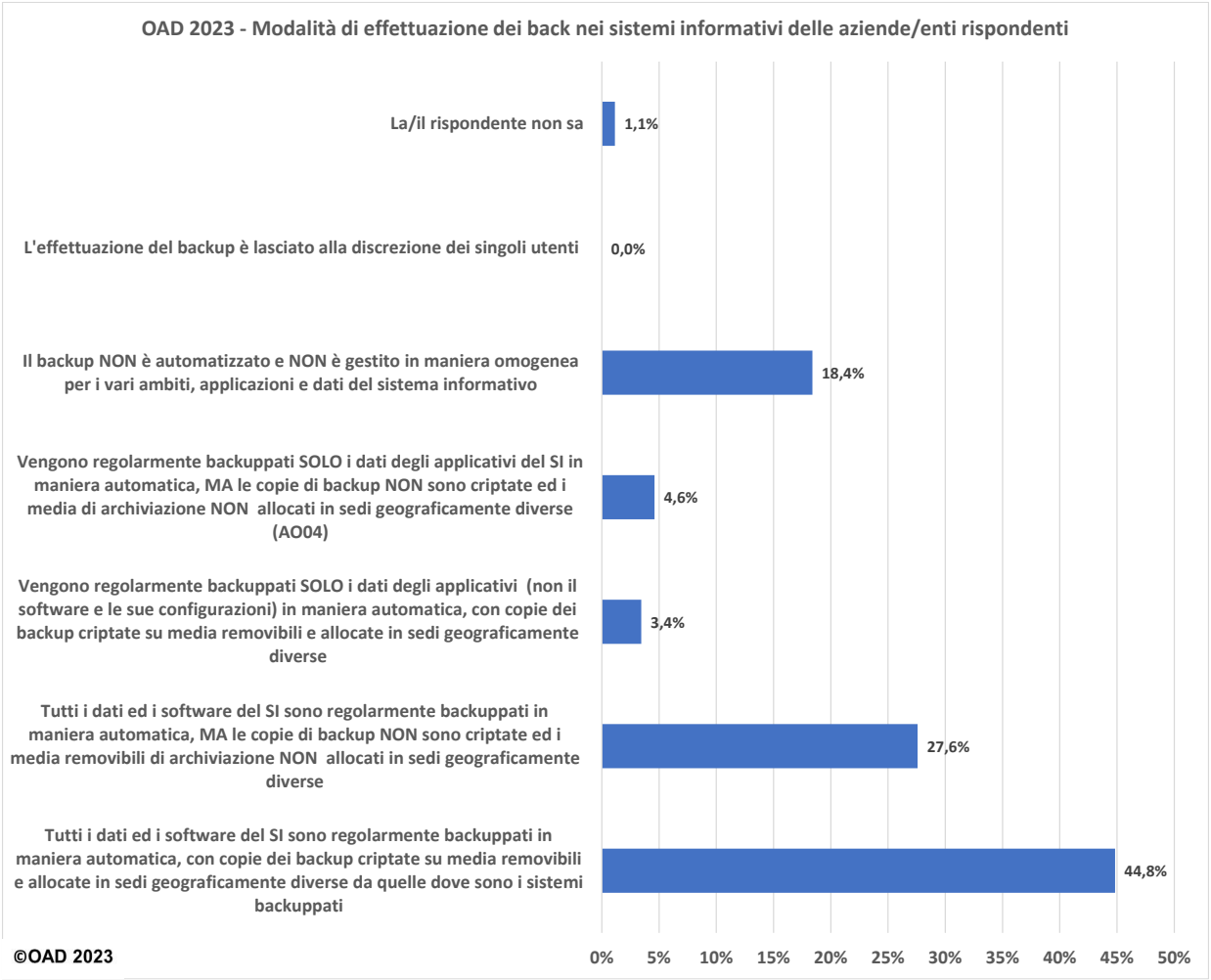


Fig. 7.2.6-5

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.
La fig. 7.2.6-6 mostra che il **81,4%** delle aziende/enti rispondenti ha definito ed utilizza procedure per come ripristinare i vari sistemi dai dati dei backup, ma di questi solo il 47,7% periodicamente le prova con test, rendendosi quindi in grado di usarle correttamente e tempestivamente. Ancora il 18,6% non ha o non utilizza procedure di ripristino. Questa percentuale, non trascurabile, è dovuta al numero elevato di piccole e piccolissime organizzazioni che hanno partecipato all'indagine.

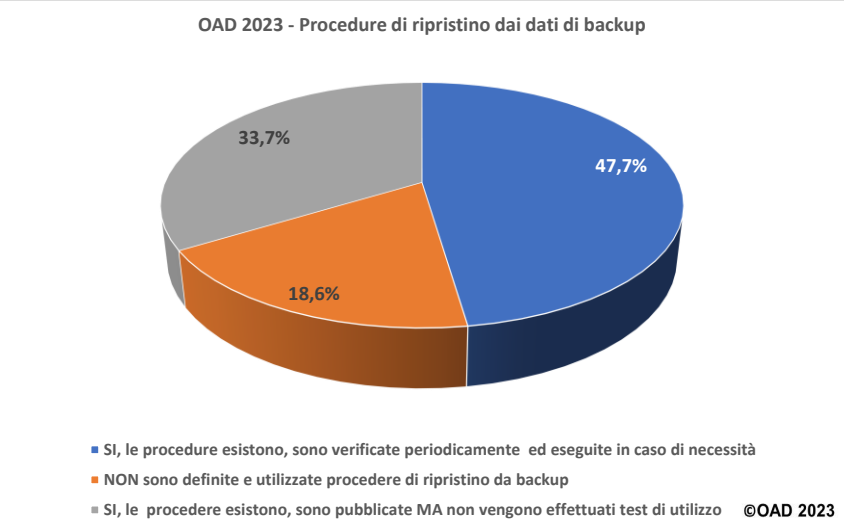


Fig. 7.2.6-6

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

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 specifiche. 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, i sistemi per la raccolta e la gestione dei log dei sistemi ICT e degli utenti, i sistemi SOAR (Security Orchestration, Automation and Response), che consentono di automatizzare e di velocizzare la gestione della sicurezza digitale, i sistemi SASE (SASE, Secure Access Service Edge), i sistemi di analisi comportamentali di utenti e risorse ICT, i sistemi di individuazione e prevenzione di attacchi e data breach.
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 gestire la sicurezza è avere, aggiornato, l'inventario di tutte le risorse hardware, software e terziarizzate.

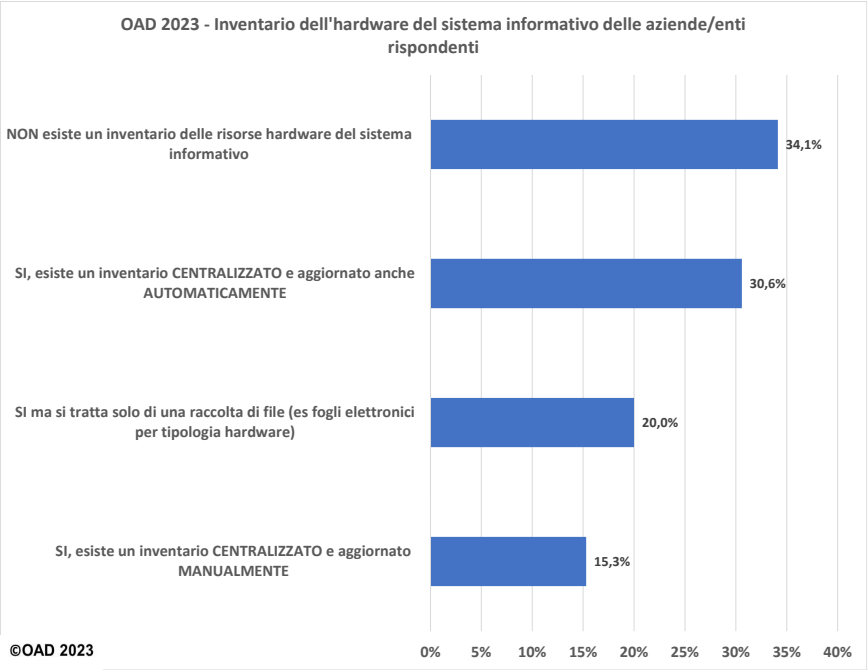


Fig. 7.2.7-1

La fig. 7.2.7-1 mostra la situazione per **l'inventario delle risorse hardware** del sistema informativo dell'azienda/ente rispondente. Più di 1/3, il **34,1%** non ha un inventario delle risorse hardware, mentre i 2/3 ha un inventario, ma realizzato in differenti maniere: il 20% di questi realizza una raccolta manuale dell'hardware esistente in fogli elettronici o in altri tipi di documenti, probabilmente gestito e conservato nelle diverse sedi periferiche dove si trovano i vari dispositivi ICT; il 45,9% ha un inventario centralizzato, e di questi il 30,6% lo alimenta e lo aggiorna automaticamente con appositi software.

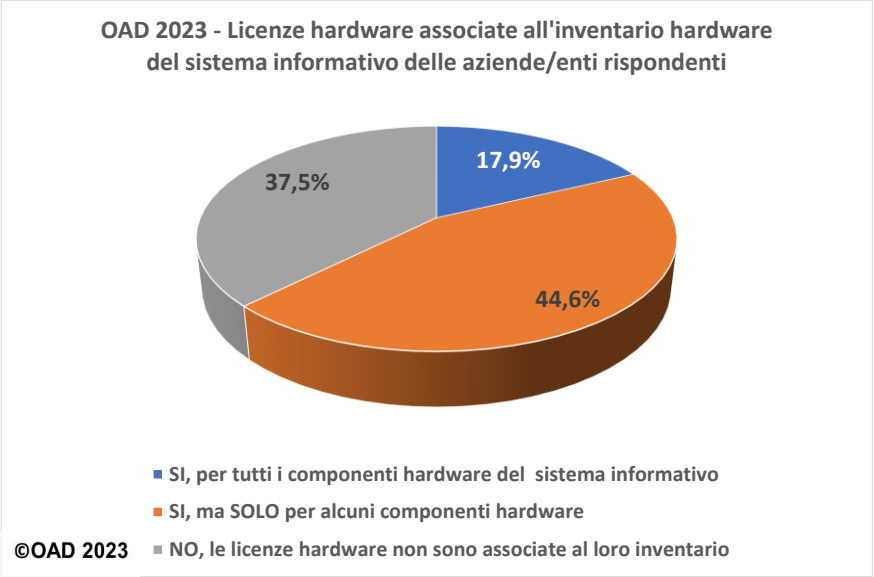


Fig. 7.2.7-2

Le **licenze per l'hardware**, in particolare per la sua manutenzione, dovrebbero essere associate all'inventario, per una loro efficace gestione. La fig. 7.2.7-2 mostra la situazione emersa dall'indagine, limitata ai sistemi informativi che dispongono di un inventario dell'hardware: per essi tale associazione esiste per il **67,5%** dei casi, ma di questi solo il 37,7% riguarda tutte le risorse hardware, e nel 28,6% dei casi tale associazione non esiste.

Per quanto riguarda l'**inventario del software** del sistema informativo, sia di base sia applicativo, la fig. 7.2.7-3 evidenzia che il **41,2%** delle aziende/enti rispondenti non ha un inventario del software, il rimanente **58,8%** ha un inventario, ma realizzato in differenti maniere: il 17,6% realizza una raccolta manuale dell'hardware 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 41,% ha un inventario centralizzato, ma di questi solo il 28,26% lo alimenta e lo aggiorna automaticamente.

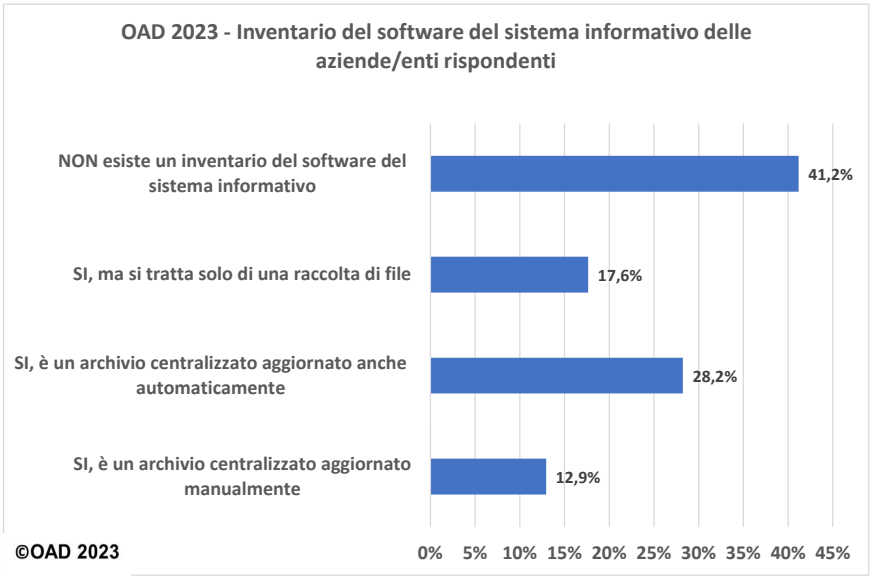


Fig. 7.2.7-3

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.
La fig. 7.2.7-4 mostra la situazione emersa dall'indagine per l'associazione tra le licenze del software ed il loro inventario, limitata ai sistemi informativi che dispongono di un inventario del software: il **54%** 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 24% l'ha per tutti i software inventariati, mentre il 22% ha correlato le licenze solo per alcuni software
Gli inventari dell'hardware e del software dovrebbero 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, è mostrata in fig. 7.2.7-5: il **60%** ha i due inventari correlati/integrati tra loro.

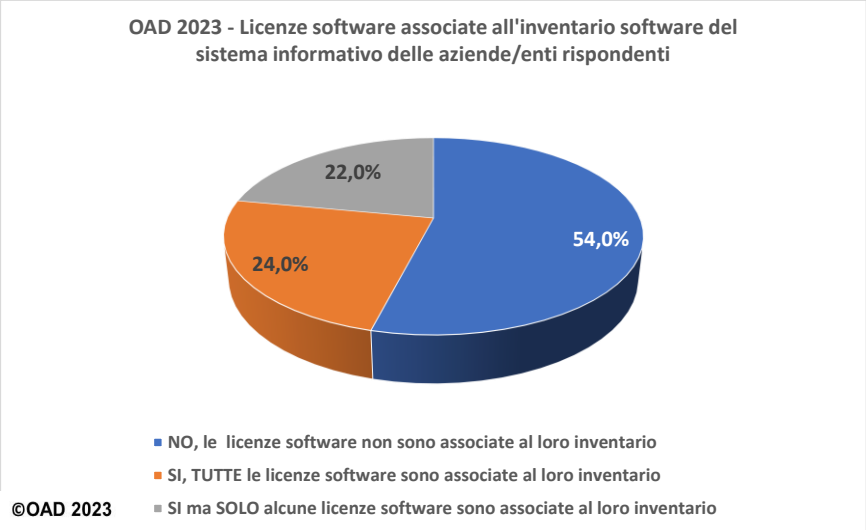


Fig. 7.2.7-4

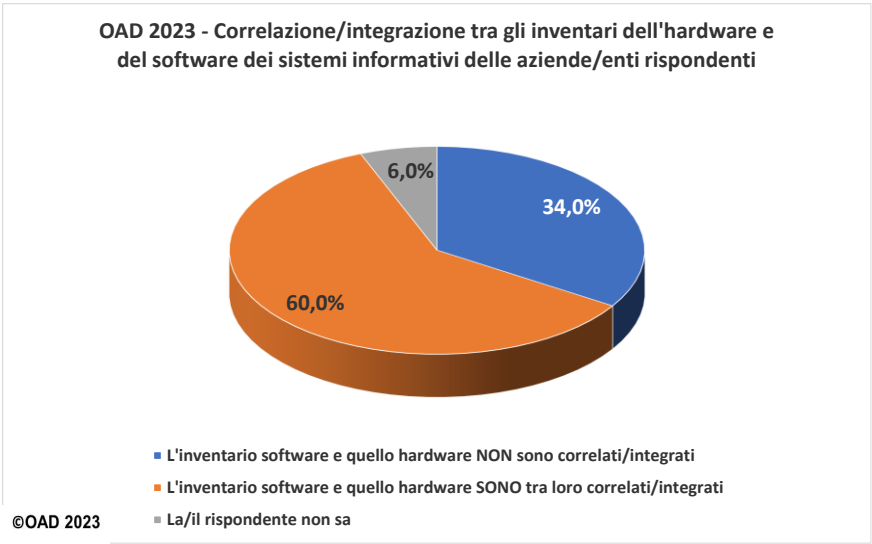


Fig. 7.2.7-5

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 facenti parte del sistema informativo; in alcuni soluzioni questo monitoraggio è integrato con quello dell'intero sistema informativo, 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 2023 si è cercato di semplificare e ridurre le domande su questo argomento, e la fig. 7.2.7-6 mostra i risultati emersi. In generale i sistemi informativi emersi dall'indagine hanno per il **81,2%** un qualche sistema di controllo e monitoraggio per la sicurezza digitale: le due tipologie più diffuse e che rientrano in questa percentuale sono con il 36,5% sistemi centralizzati ed integrati con quelli di controllo e monitoraggio dell'intero sistema informativo, soluzioni tipica per grandi sistemi informativi, e con il 31,8% il controllo non centralizzato ma di ogni singolo sistema ICT, soluzione diffusa nei sistemi informativi di piccole e piccolissime dimensioni. Nel 16,5% dei casi non è (ancora) in funzione alcun sistema di controllo e monitoraggio. Il 7,1% utilizza sistemi di controllo e monitoraggio di Terze Parti.
Un altro aspetto importante per la gestione della sicurezza digitale è la configurazione corretta dei sistemi ICT, in particolare per tutte le opzioni inerenti la sicurezza, che troppo spesso non vengono correttamente settate.

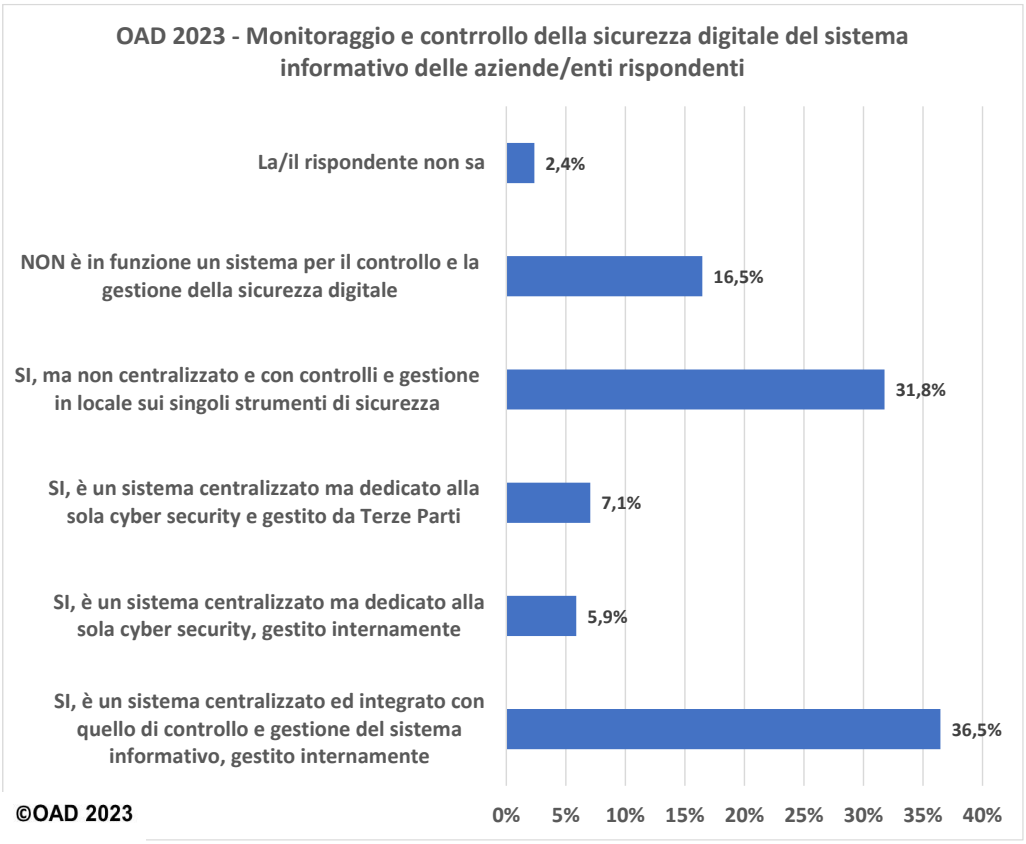


Fig. 7.2.7-6

La fig. 7.2.7-7 sintetizza se e come è gestita la configurazione della sicurezza digitale nei sistemi ICT dei sistemi informativi emersi nell'indagine OAD 2023. Nel **51,8%** dei sistemi informativi delle aziende/enti rispondenti le configurazioni per la sicurezza digitale sono sistematicamente aggiornate, manualmente o in maniera automatica, ma

per più di ¼, il 25,9%, non sono definite metodiche/procedure per correttamente configurare le opzioni di sicurezza all'installazione o successivamente. Il 22% configura alla sola installazione.

Nell'ambito della gestione operativa della sicurezza digitale rientrano anche le periodiche analisi di vulnerabilità ed i penetration test, chiamati per brevità "pentest".
L'analisi dei rischi è considerata da OAD una misura organizzativa, e l'indagine 2023 riporta i dati rilevati in §7.1.3. L'analisi delle vulnerabilità ed i pentest sono invece misure tecniche.

Come mostrato nella fig. 7.2.7-8, solo il **10,6%** delle aziende/enti rispondenti non le effettua. E' un dato positivo, relativo prevalentemente alle piccole organizzazioni, controbilanciato da un ampio **50,6%**, poco più della metà del totale, che effettua l'analisi delle vulnerabilità in maniera sistematica e periodica, e da un **36,5**% 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 **poco meno del 90%** delle aziende/effettua l'analisi delle vulnerabilità tecniche, che è il primo basilare passo per l'implementazione delle idonee misure di sicurezza per ogni specifico sistema informativo.

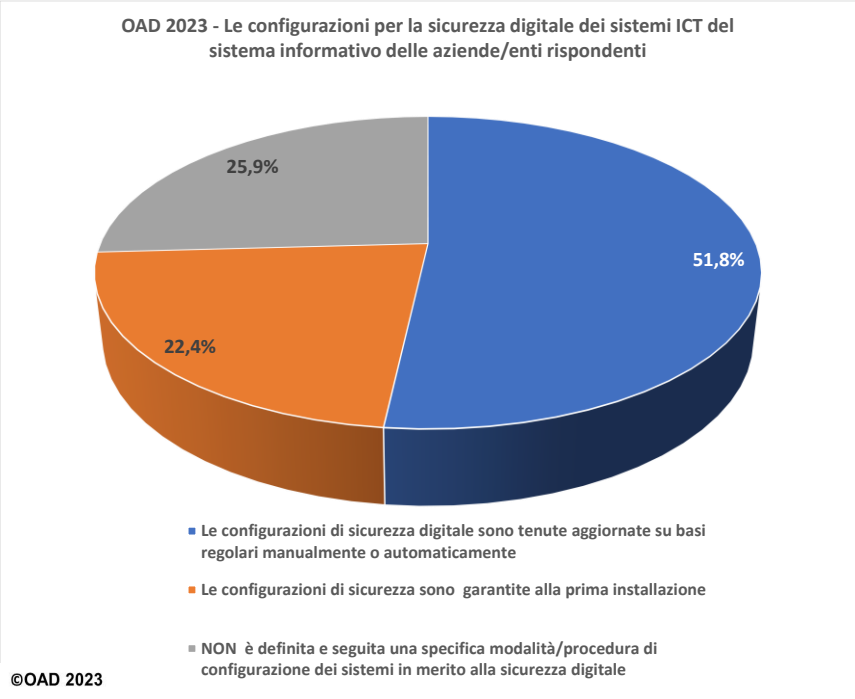


Fig. 7.2.7-7

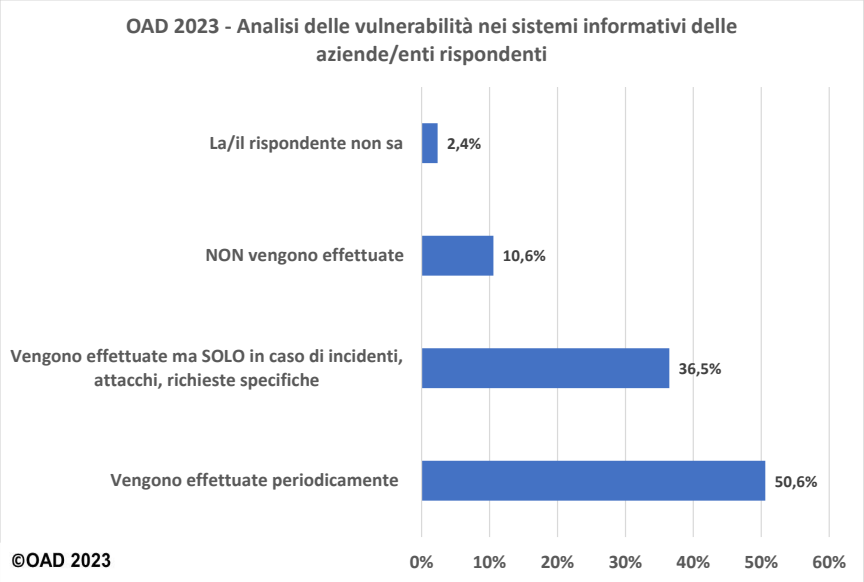


Fig. 7.2.7-8

A fianco dell'analisi delle vulnerabilità, e in particolare dopo aver effettuato opportuni aggiornamenti dei software in uso, è 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.

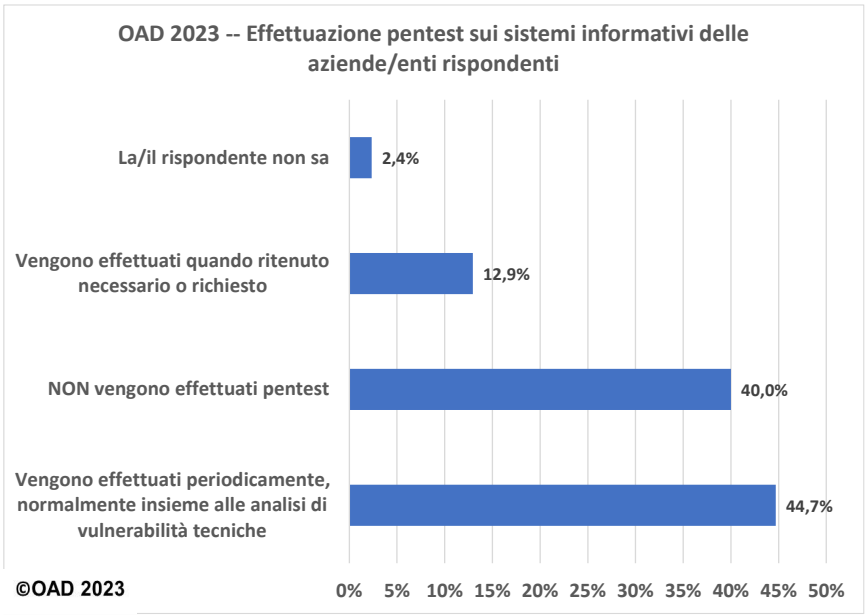


Fig. 7.2.7-9

La fig. 7.2.7-9 mostra che il **57,8%** effettua pentest, e di questi il 44,7% periodicamente e regolarmente, il resto li effettua solo quando ritenuto necessario: ad esempio su richiesta, per contribuire ad una certificazione aziendale, etc. Il 40% non li effettua.

La **raccolta e la gestione dei log** è un'altra misura utile nella gestione operativa del sistema informativo e della sua sicurezza. OAD 2023 nel questionario ha richiesto solo se viene effettuata la raccolta e la gestione dei log degli utenti, sia quelli privilegiati sia quelli finali.
La fig. 7.2.7-10 riassume le risposte raccolte: a parte un 13,3% che non raccoglie ed analizza i log, tutti gli altri lo fanno, seppure con varie modalità. Il **22,2%** raccoglie e gestisce i log di tutti gli utenti, mentre il 34,4% lo fa solo per gli utenti privilegiati ed il 14,4% raccoglie solo i log, così come è obbligatorio per gli amministratori di sistema dal provvedimento del Garante italiano della privacy del 27/11/2008. Proprio per questo provvedimento, lo 84,4 %, archivia i log degli amministratori di sistema, che sono tra utenti privilegiati, che è obbligatorio in Italia dal 2008.

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.

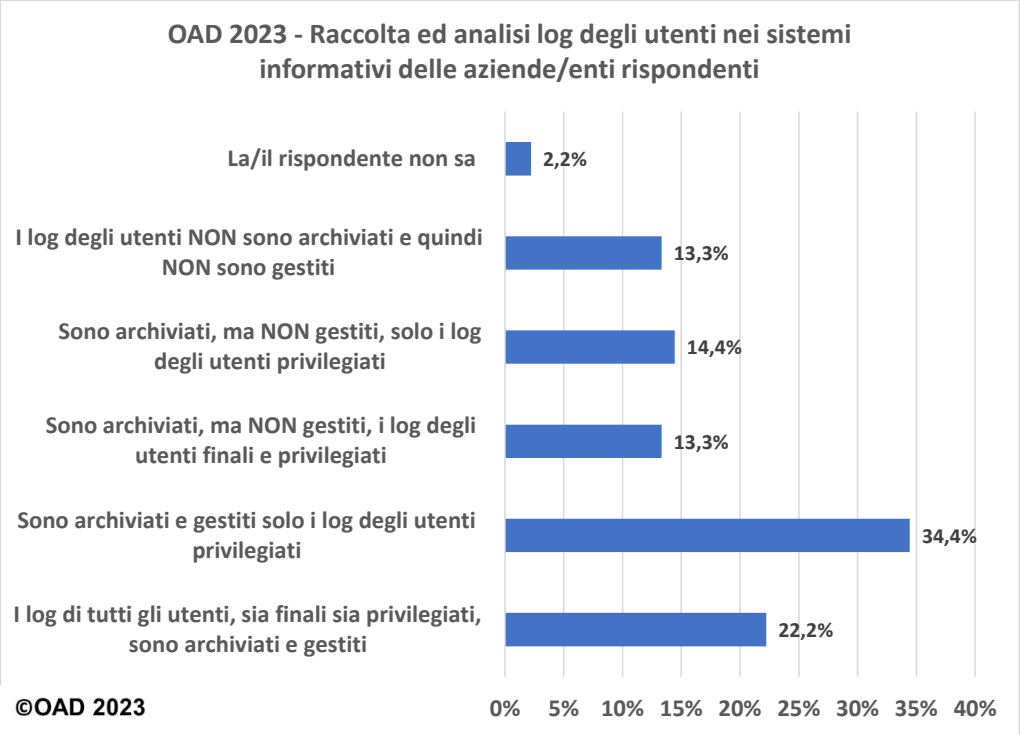


Fig. 7.2.7-10

La figura 7.2.7-11 mostra che un SOC è usato dal **31,8%** delle aziende/enti rispondenti, e di queste il 15,3% usa un SOC fornito da Terze Parte. L'uso di un SOC è tipico di grande organizzazioni e di grandi fornitori di cloud/hosting, il suo limitato uso emerso dall'indagine è pertanto giustificato e ragionevole.

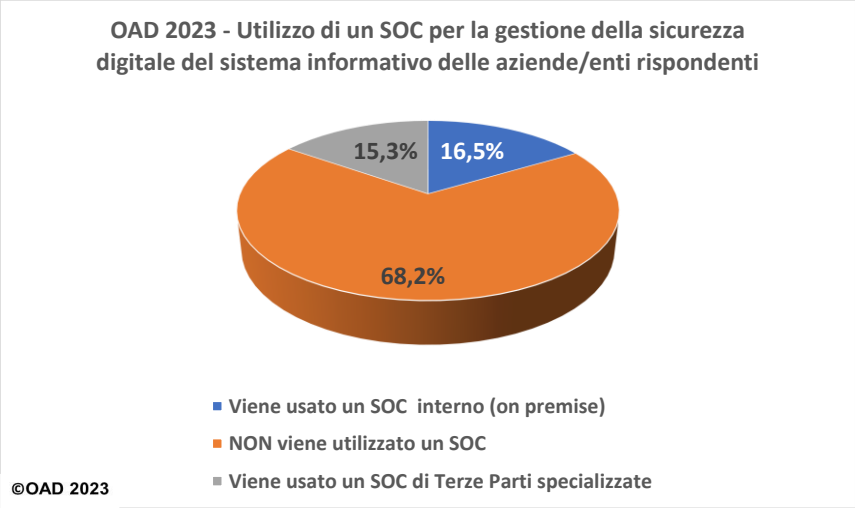


Fig. 7.2.7-11

Nell'ambito della gestione della sicurezza digitale un aspetto importante è la definizione di un Piano di Disaster Recovery (DR) del Sistema Informatico, 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 (si veda in particolare l'ERT in fig. 7.1.2-3 e in fig. 7.1.2-4).
La fig. 7.2.7-12 evidenzia che il **58,8%** dei sistemi informativi delle aziende/enti rispondenti ha un Piano di DR. Data l'importanza dell'argomento, la fig. 7.2.7-13 correla l'esistenza di tale piano alle dimensioni, come numero di dipendenti, delle aziende/enti rispondenti. Come già sottolineato in precedenza, le singole percentuali emerse non sono significative dato che dipendono dal numero di rispondenti per classe di dipendenti. L'informazione più interessante che emerge dalla correlazione è che alcune delle piccole e piccolissime organizzazioni hanno un tale piano.
La barra arancione-bruna dei NO decresce al crescere delle dimensioni dell'azienda/ente, e per le piccolissime organizzazioni (<=10 dipendenti) rispondenti è addirittura percentualmente inferiore alla barra blu del SI. Questo implica che queste piccolissime organizzazioni includono aziende innovative con business per i quali il sistema informativo è essenziale.

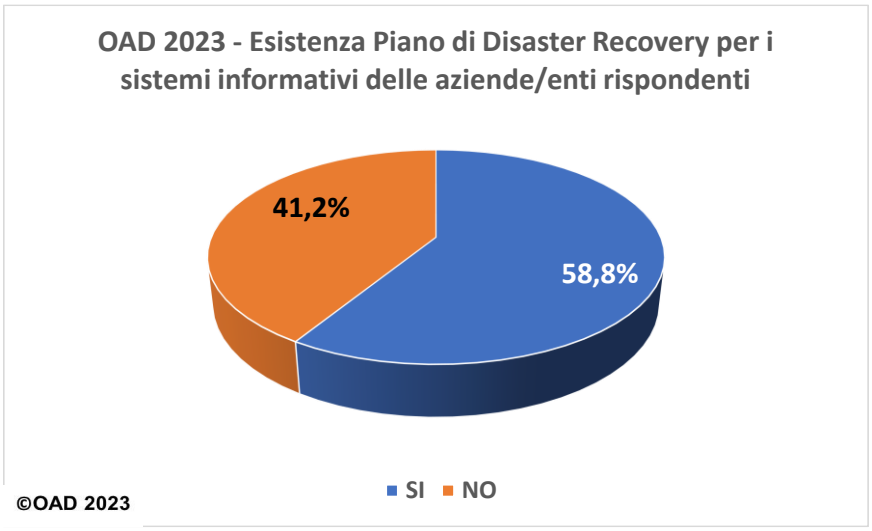


Fig. 7.2.7-12

Come già evidenziato sopra, un Piano di DR deve prevedere le risorse ICT alternative da utilizzare i caso di disastro, e quindi di averle già a disposizione, di averle prenotate o di sapere dove e come poterne disporre in tempi brevi. La disponibilità di IaaS e SaaS favorisce ora questa attivazione anche all'ultimo momento.

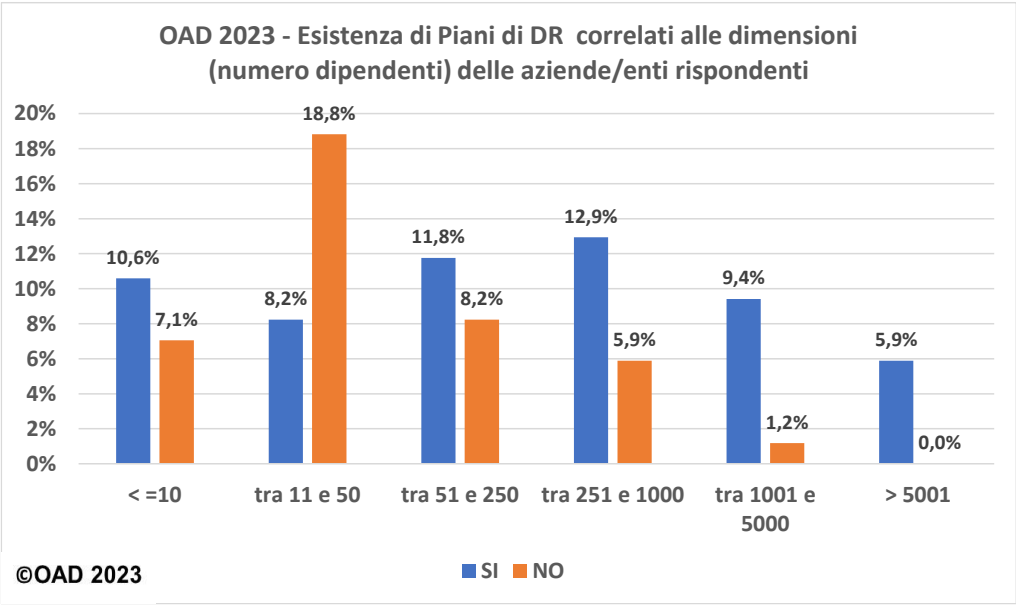


Fig. 7.2.7-13

La fig. 7.2.7-14, mostra che il **90%** delle aziende/enti rispondenti (limitate a quelle che avevano dichiarato di avere un Piano di DR nella precedente domanda del questionario) ha previsto o allocato risorse ICT alternative per poter realmente attuare un DR. Questo dato indica che le organizzazioni rispondenti stanno seriamente considerando l'evenienza di un DR, e migliora nettamente i dati rilevati nelle precedenti edizioni di OAD. Addirittura il 40% delle organizzazioni rispondenti dichiara di disporre di un stand by caldo, ossia disponibilità risorse ICT in tempo reale e probabilmente in replica su risorse remote in una architettura ad alta affidabilità. I percentualmente pochi, 6%, che pur avendo un piano di DR, non hanno previsto alcuna risorsa ICT alternativa da utilizzare, hanno di fatto un DR solo sulla

carta, di fatto attuabile nel momento della crisi per l'occorrenza del disastro con l'attivazione di risorse in cloud: soluzione fattibile ma con ritardi non trascurabili tra il disastro e l'attivazione delle risorse ICT all'ultimo momento ed in una fase di grave crisi.

La gestione di una gravissima emergenza come il recovery di un sistema informativo richiede, sulla base del Piano di DR, l'effettuazione di **esercitazioni periodiche** (normalmente a tavolino, chiamate DTE, Desk Top Exercise), ad esempio su base semestrale, o annuale, per verificare la corretta impostazione delle procedure organizzative e la preparazione del personale da coinvolgere in un DR (si veda ERT in § 7.1.2). 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.

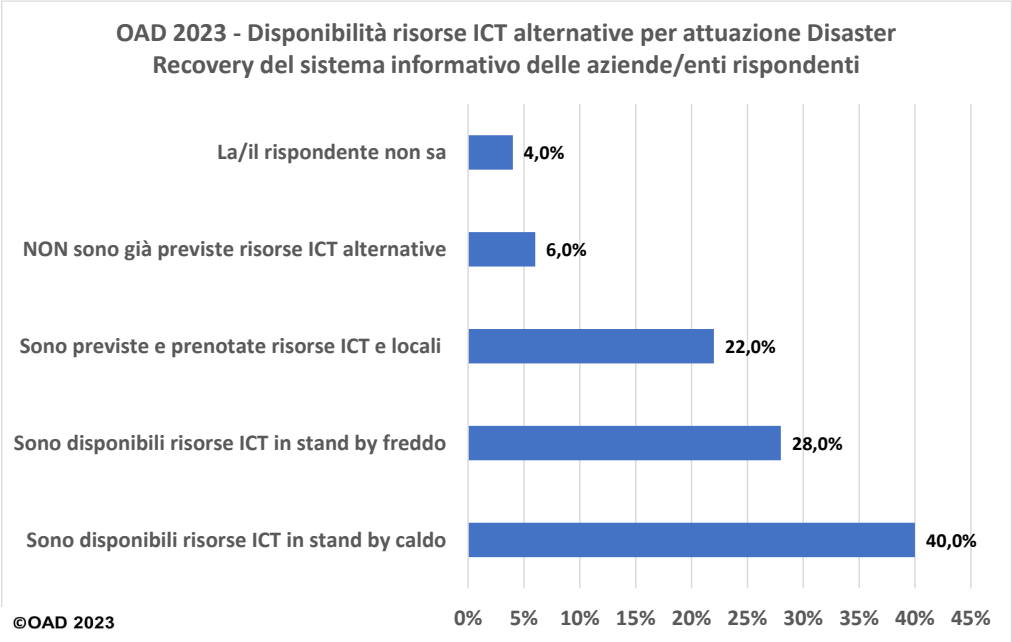


Fig. 7.2.7-14

La fig. 7.2.7-15 mostra che solo il **16%** delle organizzazioni 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. Tra questi, la soluzione più diffusa, per il 34%, è di effettuare prove e simulazioni solo per alcune parti del sistema informativo, quelle più importanti e critiche per business/attività, e solo in specifiche occasioni, quali ad esempio la richiesta del vertice dell'organizzazione, degli auditor, a seguito di un attacco. Il 14% effettua queste prove in maniera periodica e per l'intero sistema informativo.

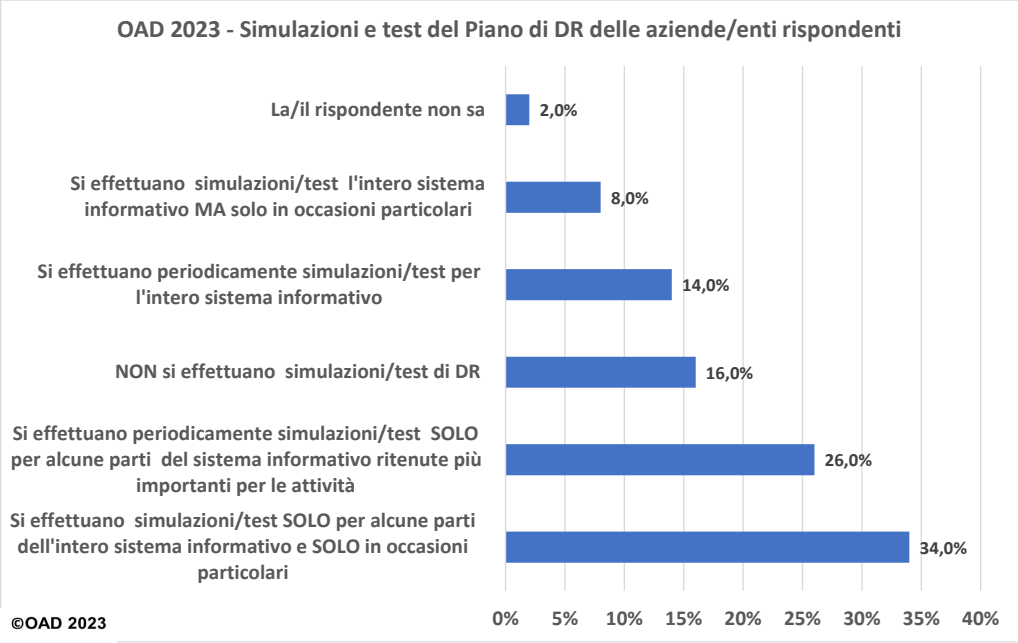

OAD 2023 - Simulazioni e test del Piano di DR delle aziende/enti rispondenti
La/il rispondente non sa
2,0%
Si effettuano simulazioni/test l'intero sistema informativo MA solo in occasioni particolari
8,0%
Si effettuano periodicamente simulazioni/test per l'intero sistema informativo
14,0%
NON si effettuano simulazioni/test di DR
16,0%
Si effettuano periodicamente simulazioni/test SOLO per alcune parti del sistema informativo ritenute più importanti per le attività
26,0%
Si effettuano simulazioni/test SOLO per alcune parti dell'intero sistema informativo e SOLO in occasioni particolari
34,0%
0% 5% 10% 15% 20% 25% 30% 35% 40%
©OAD 2023

Fig. 7.2.7-15

8. Contributo statistico della Polizia Postale e delle Comunicazioni all'indagine OAD 2023

OAD riporta in questo capitolo l'intero contributo della Polizia Postale e delle Telecomunicazioni, mantenendo il formato grafico con cui è stato fornito, da parte dell'Ispettore **Gaetano Martucci** e dell'Agente **Antonio Micello**, che l'autore ed AIPSI ringraziano insieme al **Direttore** della Polizia Postale e delle Telecomunicazioni **Ivano Gabrielli**.
La Polizia Postale e delle Comunicazioni 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.

Per quanto riguarda i dati sulla protezione delle infrastrutture critiche, la Polizia Postale e delle Comunicazioni ha una propria struttura, il **C.N.A.I.P.I.C.**, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche[57], incaricata in via esclusiva della prevenzione e della repressione dei crimini informatici di matrice comune, organizzata o terroristica, che hanno come obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale, soggette alla normativa europea NIS ora aggiornata ed ampliata con NIS 2, ed anche alle altre normative europee sulla sicurezza digitale trattate in §3.4 (si veda in particolare la fig. 3.4-1).

I dati forniti dalla Polizia Postale confermano il drammatico incremento degli attacchi digitali nel 2022. Tale incremento risulta evidente con il confronto dei dati forniti negli ultimi anni per le indagini OAD di AIPSI.
Nella fig.8-1 sono messi a confronto le informazioni ricevute per la protezione delle infrastrutture critiche: gli attacchi rilevati e gli allarmi diramati nel 2022 hanno avuto un forte incremento rispetto ai dati degli anni precedenti.

Protezione strutture critiche	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	13.099	282	509	1181	459	1.032	844
Alert diramati	113.420	24.824	83.416	82.484	80.777	31.524	6.721
Indagini avviate	110	34	103	155	74	72	70
Persone arrestate	n.d	n.d.	n.d.	3	1	3	3
Persone denunciate/indagate	334	n.d.	105	117	14	1.316	1.226
Perquisizioni	n.d.	n.d.	n.d.	n.d.	n.d.	73	58
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	77	17	69	79	108	83	85

Fig. 8-1 (Fonte: elaborazione OAD su dati Polizia Postale e delle Telecomunicazioni)

Nella fig.8-2 sono messi a confronto le informazioni ricevute per il contrasto al cyber terrorismo partendo dal controllo dei siti web : anche in questo caso i numeri nel 2022 sono nell'ordine delle centinaia di migliaia, rispetto alle migliaia nei precedenti anni.

Cyber Terrorismo	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	175.572	11.962	37.081	36.377	36.000

Fig. 8-2 (Fonte: elaborazione OAD su dati Polizia Postale e delle Telecomunicazioni)

Per le altre informazioni fornite sulle "frodi informatiche" e sulle "truffe online", OAD non ha potuto produrre tabelle di confronto con gli anni precedenti, in quanto i dati che seguono non sono dello stesso tipo di quelli ricevuti negli anni precedenti.

[57] https://www.commissariatodips.it/profilo/cnaipic/index.html

Il documento della Polizia Postale e delle Comunicazioni fa riferimento a due frodi indicate come BEC e CEO Fraud. Per una chiara comprensione di questi due termini:

- **BEC**, Business Email Compromise, è la compromissione della posta elettronica di un'azienda/ente. In una logica tipo spear phishing in ambito aziendale, non individuale, vengo inviate da veri, o falsi che assomigliano ai veri, messaggi email che inducono il ricevente a rispondere fornendo dati riservati (la sua password, l'IBAN, etc.) e/o ad effettuare azioni anche economiche che ovviamente non dovrebbe fare, o a ad accedere, involontariamente, a siti malevoli, anche in questo caso lasciando dati riservati o effettuando azioni che non dovrebbe/potrebbe effettuare.
- **CEO fraud** è una frode che può anche non utilizzare strumenti digitali. In essa l'aggressore si finge una figura di rilievo all'interno dell'organizzazione e come tale ha una immediata fiducia dal suo interlocutore che compie le azioni volute dall'attaccante, ad esempio autorizzare acquisti, pagamenti, attivazioni nuovi account, e così via.

Il documento fornisce inoltre dati sulle pedopornografia e sui reati contro la persona che non sono oggetto dell'indagine OAD, ma che per il loro interesse sono stati lasciati.

OAD
Osservatorio
Attacchi Digitali
in Italia

Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

DIREZIONE CENTRALE PER LA POLIZIA STRADALE, FERROVIARIA, DELLE COMUNICAZIONI E PER I REPARTI SPECIALI DELLA POLIZIA DI STATO SERVIZIO POLIZIA POSTALE E DELLE COMUNICAZIONI

POLIZIA POSTALE E DELLE COMUNICAZIONI

Contributo statistico per l'Osservatorio Attacchi Digitali in Italia (indagine AIPSI 2023)

ANNO

2022

(fonte dati: mattinale Polizia Postale e delle Comunicazioni)

Dati aggiornati al 31 dicembre 2022

Roma, 5 giugno 2023

Rilevazione statistica a cura di:
Ispettore della Polizia di Stato Gaetano Martucci
Agente della Polizia di Stato Antonio Micello

PREMESSA

Il 2022 è stato indelebilmente segnato da due eventi di portata globale, le cui ripercussioni si riverberano a livello internazionale e in molteplici ambiti della vita, tra cui la criminalità informatica. Gli strascichi socioeconomici della pandemia da Coronavirus esplosa nei primi mesi del 2020, uniti agli effetti del conflitto militare che vede contrapposte Russia e Ucraina, infatti, hanno continuato ad impegnare quotidianamente gli operatori della Polizia Postale, posti davanti a sempre nuove minacce alla sicurezza cibernetica.

Gli attacchi *cyber* sferrati contro le infrastrutture critiche, i sistemi finanziari e le aziende operanti in settori strategici quali comunicazione e difesa, sono a livello internazionale in preoccupante aumento. In tale scenario è tangibile il ruolo assunto da gruppi schierati di *hacker*, interessati a conquistare il "dominio cibernetico" attraverso campagne di *phishing* sempre più elaborate in termini di *social engineering*, invio di *malware* distruttivi (specialmente *Ransomware*), attacchi Ddos, campagne di disinformazione e *leak* di database.

La prevenzione e il contrasto al CyberCrime, sempre più evoluto ed aggressivo, rappresenta pertanto un impegno notevole in termini di una radicale ma necessaria riorganizzazione delle strutture della Polizia di Stato preposte a tali attività per dare una risposta ancora più incisiva contro la criminalità organizzata che sempre più si avvale delle nuove tecnologie dell'informazione e della comunicazione per perfezionare i propri disegni delittuosi.

Con tali obiettivi, la Polizia di Stato ha dato vita ad una nuova Direzione Centrale, per fronteggiare efficacemente le continue minacce Cyber. La nuova struttura si occuperà da un lato della sicurezza cibernetica, tra cui quella legata alle Infrastrutture del Ministero dell'Interno che ovviamente hanno una criticità propria e strategica in termini di tenuta paese e dall'altro coordinerà le attività di indagini di alto profilo, unendo l'esperienza e le capacità della Polizia Postale con quelle dalla Polizia Scientifica. Il nuovo Polo, quindi, opererà trasversalmente indagando sulle nuove frontiere criminali supportando nelle indagini tecnologiche gli investigatori sul territorio.

L'altro aspetto che ha contrassegnato lo scorso anno è stata la rilevante riduzione delle misure sanitarie dovute alla pandemia da Covid-19 che ha trasformato il 2022 nell'anno del riscatto sociale, caratterizzato dalla voglia da parte di tutta la popolazione di riconquistare, seppur lentamente, quel senso di vita normale che nel biennio precedente si era oramai perso a causa dei lunghi periodi di isolamento sociale forzato, necessari per limitare globalmente la circolazione del virus.

Questo progressivo recupero della normalità, correlato con l'uscita dallo stato di emergenza, non ha ridotto solo quel sentimento di isolamento sociale ma probabilmente ha attenuato l'uso degli strumenti informatici e telematici, che hanno rappresentato nel 2020 e 2021, gli unici supporti per garantire quel minimo (ma indispensabile) rapporto di interazione umana a distanza, soprattutto negli ambiti familiari e lavorativi.

Tali aspetti hanno contribuito alla riduzione del numero dei casi registrati nel 2022 nell'ambito dei reati contro la persona perpetrati Online, riflettendosi anche nella flessione relativa alla circolazione globale di materiale pedopornografico su circuiti internazionali, con una conseguente diminuzione degli eventi delittuosi trattati, che non ha però inciso sull'attività di

contrasto. Infatti, è stato registrato un aumento dei soggetti indagati per violazioni connesse ad abusi in danno di minori.

Da un punto di vista di criminalità informatica strettamente patrimoniale, sono svariate e molteplici le tipologie di truffe *online* che giornalmente vengono rilevate in rete dagli operatori della Specialità durante i continui monitoraggi del *World Wide Web* o segnalate dagli stessi cittadini attraverso l'apposita sezione presente sul sito del Commissariato di P.S. online[58], direttamente proporzionali alle denunce che quotidianamente vengono raccolte dagli Uffici territoriali della Specialità.

L'attività più redditizia ed in preoccupante crescita per la criminalità organizzata, nell'ambito delle truffe online, è rappresentata sicuramente dal falso *trading online*. Negli ultimi anni la diffusione del trading online, grazie anche ad una massiccia campagna promozionale sul web, ha registrato un fortissimo aumento generando interesse anche in coloro che non si sono mai occupati della materia, attratti proprio dal miraggio di cospicui guadagni a fronte di modesti investimenti, ma ignari dei più basilari concetti che regolano il complesso mondo delle contrattazioni finanziarie.

Per consentire agli utenti del web di avere delle risposte in tempo reale su ciò che accade nella rete ed evitare loro di cadere nelle tante insidie della navigazione in Internet, è attivo, ormai da anni, il Commissariato di P.S. Online, portale della Polizia di Stato gestito da investigatori, tecnici ed esperti della Polizia Postale e delle Comunicazioni, che offre agli utenti diversi servizi in materie giuridiche e sociali.

In particolare, il sito è un importante strumento di interazione con i cittadini che, ogni giorno, inviano in media 400 messaggi tra segnalazioni e richieste di informazioni e che viene utilizzato, al contempo, per veicolare loro notizie e consigli utili per un uso sicuro, consapevole e responsabile della rete: un dato che offre un chiaro riscontro al sempre più crescente livello di interazione con i cittadini.

[58] https://www.commissariatodips.it/

CENTRO NAZIONALE ANTICRIMINE INFORMATICO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE (C.N.A.I.P.I.C.) – COMPUTER CRIME – REATI CONTRO LA PERSONA ATTRAVERSO SOCIAL E RETE INTERNET

	1 gen – 31 dic 2022
Attacchi rilevati	13.099*
Alert diramati	113.420
Indagini avviate dal C.N.A.I.P.I.C.	110
Persone indagate	334*
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	77

* 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 2022
Casi trattati pedopornografia e adescamento online	4.618
Persone indagate	1.466
Perquisizioni	1.259
Monitoraggi rete	25.826
Siti presenti in black list al 31/12/2022	2.622

-=oOOo=-

IL COMMISSARIATO DI P.S. ONLINE

	1 gen – 31 dic 2022
Segnalazioni	101.002
Informazioni	25.792
Visite	2.597.545
Accessi	42.494.652
Alert Diramati	33
Interventi finalizzati alla prevenzione di intenti suicidari	64

-=oOOo=-

PREVENZIONE CYBERTERRORISMO

• *Eversione Internazionale Estremismo religioso e politico* • *Eversione nazionale estrema destra, area antagonista, attività in circostanze di emergenza*	**1 gen – 31 dic 2022**
Spazi web monitorati	175.572
Spazi Virtuali con contenuti illeciti rilevati	1.598
Spazi oscurati per attiv. infoinvestigative	338

-=oOOo=-

LE FRODI INFORMATICHE

	1 gen – 31 dic 2022
Casi trattati	5.908
Persone indagate	725
Somme sottratte	€ 35.509.160

BEC e CEO FRAUD IN DANNO DI GRANDI E MEDIO IMPRESE INVESTIGATE DAL SETTORE FINANCIAL CYBER CRIME DEL SERVIZIO POLIZIA POSTALE	**1 gen – 31 dic 2022**
Casi trattati	156
Transazioni Fraudolente	20.502.112 €
Somme Recuperate	4.673.074 €

-=oOOo=-

LE TRUFFE ONLINE

	1 gen – 31 dic 2022
Casi trattai	15.699
Persone indagate	3.570
Somme sottratte	€ 116.454.550

-=oOOo=-

REATI CONTRO LA PERSONA

	1 gen – 31 dic 2022
Casi trattati	9.366
Persone indagate	1.169

-=oOOo=-

ALLEGATI

Allegato A - Aspetti metodologici indagine OAD 2023

L'indagine OAD 2023, come le precedenti, è indirizzata da un lato all'analisi totalmente anonima degli attacchi digitali intenzionali ad aziende/enti in Italia e azioni deliberate e intenzionali rivolte contro i sistemi informatici in Italia, e non ai rischi cui i sistemi sono sottoposti per il loro cattivo funzionamento, per un maldestro uso da parte degli utenti e degli operatori, o per fenomeni accidentali esterni; dall'altro la rilevazione ed analisi, sempre in maniera anonima, delle principali caratteristiche dei sistemi informatici dei rispondenti, e delle loro misure di sicurezza in atto.
Sono considerati gli attacchi che sono stati effettivamente rilevati, e non è necessario che essi abbiano creato danni ed impatti negativi al sistema informativo attaccato, ovvero che l'attacco non ha avuto il successo sperato dall'attaccante.
L'attacco contro un sistema informatico 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 Sistema Informativo (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 riesce puntualmente a fotografare il fenomeno degli attacchi digitali intenzionali in Italia ad imprese pubbliche e private, coinvolgendo nell'indagine anche le piccole e piccolissime realtà, che costituiscono in Italia la stragrande maggioranza (si veda §3.5.1) e che altre indagini nazionali ed internazionali ben difficilmente considerano.
L'indagine OAD è stata scelta tra i progetti di Repubblica Digitale, si veda https://repubblicadigitale.innovazione.gov.it/it/i-progetti/, per la sua importanza in termini di comunicazione, sensibilizzazione e formazione sulla cybersecurity.

L'indagine OAD 2023 si è basata sulle risposte, anonime, ad un questionario online con risposte predefinite da selezionare, con **108 domande raccolte in 14 gruppi**, molte delle quali opzionali e "saltabili" nel corso della compilazione. Il questionario on line era operativo sulla piattaforma LimeSurvey installata sul sito web www.oadweb.it da fine gennaio 2023 a fine agosto 2023.
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 e le competenze specifiche necessarie per completarlo.
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 inoltre la totale riservatezza sulle risposte raccolte.
OAD è un'indagine via web, anonima, cui possono rispondere gli utenti interessati che partecipano su base volontaria tramite un browser ed una connessione ad Internet, senza alcun controllo preventivo da parte del sistema sul web**.** Come già indicato sopra, il bacino dei rispondenti all'indagine non è quindi 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.

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 per poter essere scaricato gratuitamente da tutti gli interessati.
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.

A.1 L'indagine OAD 2023

OAD 2023 ed il relativo questionario si sono focalizzati sugli **attacchi subiti e rilevati nel 2022 ai siti e agli ambienti web,** con due sole domande sulle altre tipologie di attacco rilevate nel 2022 sui Sistemi Informativi dei rispondenti per poter elaborare trend sul fenomeno degli attacchi digitali (che cosa viene attaccato e con quali tecniche) emersi nelle nostre indagini dal **2007.**
Gli approfondimenti sugli attacchi erano richiesti solo per quelli agli ambienti, alle applicazioni ed ai siti web, con riferimento in particolare alle 10 top vulnerabilità elencate da OWASP e dettagliate in §4.2 del presenta rapporto. Solo per questi attacchi sono state poste le domande che nelle precedenti versioni erano riportate per ogni tipologia di attacco, ossia:

- 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.

Le domande sulle **misure di sicurezza digitale in essere** sui sistemi informativi 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 2023

L'edizione 2023 ha ripreso la logica della precedente edizione del 2021-22, migliorando alcune definizioni e considerando le seguenti 14 le tipologie di attacco, che 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 terziarizzatii/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 cloudcl
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, i sistemi per l'automazione industriale ((SCADA, DCS, PLC, ..) e la robotica
14. Nel corso dell'intero 2022 il Sistema Informativo ha subito attacchi digitali la cui tipologia non è stata individuata

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 in §A.2.1.

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

Facendo riferimento principalmente alle tassonomie sviluppate da CERT[59] e da Sandia[60], si sono categorizzate le tecniche di attacco sotto riportate per poter descrivere e richiedere nel questionario 2023 quali sono (o quali si pensa possano essere state) le tecniche usate dall'attaccante per 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.

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

A.2.1.1 Attacco 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, vengo 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 principali per la diffusione malevola di informazioni sono prevalentemente i social network, seguite da spamming e spear phishing oltre che siti malevoli il più delle volte linkati ai precedenti 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.

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 (Cross Site Scripting).

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. 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 nei sistemi 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 la loro individuazione, verifica e realizzazione, anche con l'aiuto di basi di conoscenza contenenti centinaia di exploit.
Questi strumenti non solo sono usati per effettuare attacchi, ma anche per eseguire "penetration test" in sistemi applicativi, middleware ed altri software e prodotti informatici.

A.2.1.6 Botnet e simili

Strumenti distribuiti controllati centralmente da un Command & Control, C&C, il più delle volte anonimo e che continua a spostarsi da un server all'altro 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 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 2023, 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:

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

Il numero IDS calcolato viene posizionato in un range di valori numerici che caratterizzano le seguenti valutazioni qualitative del livello di sicurezza digitale: **buono**, **sufficiente**, **insufficiente**, **molto critico**. Ed è una di queste la valutazione qualitativa fornita a chi completa uno dei due questionari, alla quale si aggiunge l'elenco delle risposte che evidenziano la mancanza o l'insufficienza di misure di sicurezza digitale.

ALLEGATO B - Glossario dei principali acronimi e termini tecnici

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.
ACL	Access Control List. Elenco di regole per il controllo degli accessi a risorse ICT.
ACN, Agenzia Cybersicurezza Nazionale	
Active Directory	Sistema di directory della Microsoft, integrato nei sistemi operativi Windows dal 2000 in avanti. Utilizza SSO, LDAP, Kerberos, DNS, DHCP, ecc.
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.
App	Neologismo ed abbreviazione di "application" (applicazione) per indicare, anche in italiano, le applicazioni operanti localmente sui sistemi mobili, tipicamente su smartphone.
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.
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.
Attacco mirato	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, o di massa	Attacco rivolto ad una grande massa di obiettivi simili, anche dell’ordine di milioni.
AWS	Amazon Web Services.
Backdoor	Interfaccia e/o meccanismo nascosto che permette di accedere ad un programma superando le normali procedure e barriere d’accesso.
BEC	Business Email Compromise. Compromissione posta elettronica dell’azienda/entepuò essere semplice e non sofisticato, ma nella massa qualche attacco va quasi sempre a buon fine. Tipici esempi i phishing ed i ransomware.
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	Per la sicurezza ICT questo termine indica un insieme di computer, 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, etc.
BYOD	Bring Your Own Device Policy aziendale che consente l'utilizzo di dispositivi mobili di proprietà dell'utente anche nell'ambito dei sistemi informativi dell'azienda/ente. Il fenomeno è chiamato anche "consumerizzazione".
Captcha	Completely Automated PublicTuring test to tell Computers and Humans Apart 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.
CDR	Content Disarm & Reconstruction. Strumento di sicurezza informatica per la rimozione di codice potenzialmente dannoso dai file.
CED	Centro Elaborazione Dati Centro di calcolo ove risiedono tutti i sistemi centralizzati di elaborazione, archiviazione e trasmissione dei dati.
CEO Fraud	frode basata sull'aggressore che si finge una figura di rilievo all'interno dell'organizzazione e come fa effettuare all'interlocutore azioni che non dovrebbe e/o potrebbe effettuare.
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
Churn rate	Tasso di abbandono a favore della concorrenza, tipicamente dopo un attacco.
CIO	Chief Information Officer. Il responsabile dell'intero sistema informatico.
CISA	ISACA Certified Information Systems Auditor.
CISA	Cybersecurity Infrastructure Security Agency. In USA
CISO	Chief Information Security Officer. Il responsabile della sicurezza digitale dell'intero sistema informatico.
CISSP	Certified Information Systems Security Professional.
Cyber warfare	Guerra cibernetica, detta anche informatica, digitale, elettronica.
CLOSINT, Close Source Intelligence	Raccolta d'informazioni attraverso consultazione di "fonti chiuse", non accessibili al pubblico. E' l'alternativa a OSINT

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.
C.N.A.I.P.I.C.	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche. Struttura della Polizia Postale e delle Comunicazioni
Consumerizzazione	vedi 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.
CRRT	Cyber Rapid Response Teams and mutual assistance in cyber security. Eente dell'UE.
Cryptojacking	Utilizzo di capacità elaborativa di un inconsapevole traget da parte di un cybercriminale per creare criptovaluta.
CSaaS, Cyber Security as a Service.	
CSIRT, Computer Security Incident Response Team	In Italia sostituisce CERT-PA e Cert Nazionale In ottemperanza alla Direttiva NIS (Decreto legislativo 18 maggio 2018 n. 65).
Cracker	Hacker malevolo, chiamato anche criminale cyber, digitale, informatico …
Crowdturfing	Termine derivato dalla 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.
CSaaS.	Cyber Security as a Service.
CSIS	Center for Strategic and International Studies.
CSO	Chief Security Officer. Responsabile della sicurezza fisica 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. Direttore tecnico di più alto livello, tipicamente per aziende che producono prodotti e servizi. In talune organizzazioni il CIO riporta a questa figura.
CVE	Common Vulnerabilities and Exposures.
CVSS	Common Vulnerability Scoring System.
DAC	Discretionary Access Control.
Darknet	Sistema usato in Internet per monitorare la rete e possibili attaccanti, con funzionalità simili a quelle di un honeypot.
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.
Data Breach	Letteralmente "violazione dei dati", indica l'accesso criminale ad informazioni riservate e alla loro copia: tipico esempio il furto di identità digitali ed informazioni bancarie
Data Center	Centro Dati. Si veda CED.
DB	Data Base

	Banca dati.
DBMS	Data Base Management System.
DCS	Distributed Control System.
Deadlock	Un caso particolare di "race condition", consiste nella 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.
Deepfake	Tecniche basate sull'Intelligenza Artificiale per manipolare video ed audio originali.
Defacing o **defacement**	In inglese significa deturpare, e nel gergo della sicurezza informatica indica un attacco ad un sito web per modificarlo o distruggerlo; spesso con tale attacco viene modificata solo la home-page a scopo dimostrativo.
DESI	Digital Economy and Society Index . Annualmente fornito per tutti i paesi dell'UE sulla digitalizzazione di un paese e le competenze digitali dei cittadini
DoS/DDoS	Denial of Service e Distributed Denial of Service Attacco per saturare sistemi e servizi ed impedire la loro disponibilità, e quindi la loro accessibilità in Internet.
DevOps	Development and Operations. Nello sviluppo di software, stretta collaborazione con il personale della gestione operativa per impostare by design le idonee misure di sicurezza, ed evitare le fasi di test tecnico del software prima della sua messa in produzione.
DevSecOps	Integrazione di specifiche tecniche e procedure per potenziare la sicurezza del software sviluppato e posto in produzione con quelle del tipiche di DevOps.
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.
Digital Twin	Rappresentazione virtuale di un'entità fisica, vivente o non vivente, di una persona o di un sistema anche complesso connessa a una parte fisica e con la quale può scambiare dati e informazioni, sia in modalità sincrona (in tempo reale), che asincrona (in tempi successivi) (definizione di Wikipedia)
DII.	Digital Intensity Index. Indice ISTAT sulla densità del digitale nelle aziende italiane.
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
Docker	Software per la creazione di container
DLP, 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.

Drive-by Downloads	Attacchi causati dallo scaricare (anche inconsapevolmente) codici maligni o programmi malevoli.
Drones	Droni, si veda bots.
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. Recentemente ha cambiato nome in ICDL
eCF	European Competence Framework. Quadro europeo standardizzato sulle competenze digitali e sui ruoli ICT che espletano professionalmente tali competenze.
EDGE	Enhanced Data rates for GSM Evolution.
EDGE Microsoft	Browser che ha sostituito Internet Explorer.
EDR	Endpoint Detection and 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.
Endpoint	Dispositivi fisici che si connettono e scambiano informazioni in una rete di computer, da smartphone a PC, da server a storage e a dispositivi OT quali IoT.
ENISA	European Union Agency for Cybersecurity
ETACS.	Extended TACS
FTP	File Transfer Protocol. Protocollo per il trasferimento di file.
FTPs, FTPS	FTP sicuro con la criptazione dei dati durante la trasmissione
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. Certificazione europea ora sostituita da eCF.
FIRST,.	Forum of Incident Response and Security Teams
Fix	Correzione di un programma software, usato spesso come sinonimo di patch.
Flash threats	Tipi di virus in grado di diffondersi molto velocemente.
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).
FW	FireWall generico, normalmente di rete.
FWA	FireWall Applicativo.
GDPR	General Data Protection Regulation.
GPRS	General Packet Radio Service.
GSM	Global System for Mobile communications.
Hacker	Persona competente su un determinato tipo di risorse ICT che ne studia le eventuali vulnerabilità tecniche per farle conoscere (ad esempio pubblicandole in CVE) e/o per individuare come eliminarle. La sua azione è positiva, da non confondere con cracker.
Hacktivism	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 italiana 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; è quest’ultimo che le gestisce, il provider fornisce oltre allo spazio varie facilities, dall’energia elettrica al condizionamento, alle connessioni in rete, etc. .
HSDPA	High Speed Downlink Packet Access.
HTTP	HyperText Transfer Protocol. Protocollo di comunicazione ed interazione tra browser ed applicazione web
HTTPS	HyperText Transfer Protocol Secure. Protocollo sicuro per le transazioni crittate tra browser e applicazione web, e viceversa.
Hypervisor	Elemento di base, in pratica il sistema operativo, di un sistema virtualizzato, che crea e gestisce sistemi virtuali.
IAA	Identificazione - Autenticazione – Autorizzazione. Sistemi di controllo degli accessi ai sistemi ICT.
IaaS	Infrastructure as a Service.
IAM	Identity & Access Management
ICDL	International Certification of Digital Literacy Traducibile in Certificazione Internazionale di Alfabetizzazione Digitale, è nuovo nome che sostituisce ECDL e le relative certificazioni individuali.
Information Leakage	Diffusione-dispersione non autorizzata di informazioni.
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 dedicati a specifiche e limitate funzionalità .
IIoT	Industrial IoT. IoT in ambito industriale.
ISACA	Information Systems Audit and Control Association
Key Logger	Sistema di tracciamento dei tasti premuti sulla tastiera per poter carpire informazioni quali codici, chiavi, password.
Kerberos	Metodo sicuro per autenticare la richiesta di un servizio, basato su crittografia simmetrica. Utilizzato da Active Directory.
Kubernets	Sistemi per la gestione di carichi di lavoro e servizi containerizzati, 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.
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	Media Access Control. Sub strato del 2° livello datalink del modello ISO/OSI.
MAC	Codice indirizzo assegnato in modo univoco ad ogni scheda di rete.
MAC flooding	Tecnica di attacco ad uno switch per 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 di attacco.
MDR	Managed Detection and Response . Servizi gestiti di rilevamento e risposta ad incidenti sul sistema informative.
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).
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	Replica e sincronizzazione di dati su due o più dischi.
MMS	Multimedia Message Service. SMS con contenuti multimediali.
MR.	Mixed Reality. Realtà mista.
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.
NFT	Non Fungible Token . 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. Normativa europea per armonizzare la sicurezza digitale dei vari paesi.

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, XAquellCML).
OSA	Open Security Architecture.
OSINT	Open Source INTelligence. Raccolta di informazioni attraverso lo sfruttamento delle risorse disponibili al pubblico senza ledere alcuna normativa, in particolare quella sulla privacy.
OT.	Operational Technology.
OTP.	One Time Password.
Outsourcer	Fornitore dei servizi di terziarizzazione.
PaaS	Platform as a Service.
PAC	Pubblica Amministrazione Centrale.
PAL	Pubblica Amministrazione Locale.
PAM.	Privileged Access Management.
Password	Sequenza di caratteri alfanumerici e simboli tenuti segreti da un utente ed usati, dopo un identificativo d'utente, per accedere ad una risorsa informatica. Identificativo d'utente e password costituiscono il tradizionale "account" di un utente.
Passwordless	Tecniche di controllo degli accesi che consentono di non utilizzare password, dato che utilizzano prevalentemente tecniche di identificazione biometrica.
Patch	Piccolo programma per aggiornare e risolvere una vulnerabilità o un malfunzionamento di un software. Spesso usato come sinonimo di "fix".
Payload	Identifica il "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.
PESTEL	Political, Economic, Social (or Socio-cultural), Technological, Environmental and Legal.
Pharming	Attacco per carpire informazioni riservate di un utente basato sulla manipolazione dei server DNS o dei registri del sistema operativo del PC dell'utente.
Phishing	Attacco di social engineering 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.
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. E' un tipo di attacco DoS/DDoS
PLC	Programmable Logic Controller.
PMI	Piccole e Medie Imprese. Aziende sotto i 250 dipendenti.
PNRR	Piano Nazionale di Ripresa e di Resilienza.
Port scanner	Programma 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.
PSN	Polo Strategico Nazionale**.**
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. Codice a barre bidimensionale, ossia a matrice, che è impiegato per memorizzare informazioni generalmente destinate a essere lette tramite uno smartphone.
RA	Realtà aumentata.
RaaS	Ransomware-as-a-Service.
Race condition	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 perpetrato o la sua minaccia vengono usati per ricattare l'attaccato perché paghi per non subirne di altri, magari più perniciosi. Il ransomware ha come tipica motivazione il ricatto, che è un tipo della più generale frode informatica.
Ritorsione	Significa che l'attacco 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.
Rogueware	Falso antivirus. E' a sua volta 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.
RaaS	Ransomware as a Service.
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 industriali, ed in parte per la loro automazione.
Scam	Tentativo di truffa via posta elettronica. A fronte di un millantato forte guadagno o forte vincita ad una lotteria, occorre versare un anticipo o pagare una tassa.
Scammer	Colui che 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 "raschiando", è il termine in informatica usato per 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 motive di sicurezza, tipicamente per analizzarlo, per individuare attività anomale o per sventare attacchi. Può essere realizzato tramite darknet o honeynet.
SI	Sistema Informativo. 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.
Sniffing-snooping	Tecniche mirate a leggere il contenuto (pay load) dei pacchetti in rete, sia LAN che WAN.
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	Con questo termine, traducibile in ingegneria sociale, vengono considerate tutte le modalità di carpire informazioni, quali l'user-id e la password, per accedere illegalmente ad una risorsa informatica. In generale si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni.
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. Sistema di identificazione ed autenticazione pubblico a tre livelli, obbligatorio per accedere on line ai servizi digitali delle Pubbliche Amministrazioni.
SPML	Service Provisioning Markup Language.
Spoofing	Tipo di attacco digitale che falsifica l'indirizzo nell'intestazione 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 di interrogazione di 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.
Supply-chain attack	Attacco ad un sistema target partendo dalle vulnerabilità di un altro sistema collegato ed interoperante con il primo, nella catena di supply dei fornitori.
SYN Flooding	Targeted Attack. Invio di un gran numero di pacchetti SYN a un sistema per intasarlo.
TA	Attacchi mirati, talvolta persistenti, effettuati con più strumenti anche contemporaneamente; rientrano in questa categoria APT e Watering Hole.
TACS	Total Access Communication System.
TLC	Telecomunicazioni.
Trojan Horse	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.aipsi.org
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	Oeratori, 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 informativo 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'adeguato 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.
VR	Virtual Reality.
XACML	eXstensible Access Control Markup Language.

XaaS	everything as a service. Termine generico per indicare l'insieme dei servizi terziarizzati
XR	Extended Reality Termine che include le diverse tecnologie della realtà virtuale (VR), realtà aumentata (RA), realtà mista (MR)
XSS	Cross - Site Scripting. Una vulnerabilità di un sito web 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 non ancora note (non in CVE) e alle quali non è ancora stato trovato rimedio.
Zombies	Zombi, si veda bots.

ALLEGATO C - Profilo SPONSOR GOLD

Qintesi

www.qintesi.com

Il Gruppo Qintesi – con un organico di quasi 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 e Google, implementate con l'utilizzo di metodologie certificate ed il costante riferimento alle *best practices* di settore.

Qintesi è Gold Partner SAP con la qualifica di "Service Partner" e "Build Partner"; ha ottenuto differenti riconoscimenti da parte di SAP.

Qintesi opera su tutto il territorio con sedi a Milano, Bergamo, Venezia, Brescia, Roma e Mantova 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 nelle sedi di Bergamo, Milano, Macon (Venezia).

.
Inoltre, Qintesi ha avviato il percorso per la certificazione della "**Parità di genere**" (UNI/PdR 125:2022), come naturale prosecuzione del rispetto e promozione del valore della sostenibilità e per rafforzare il suo impegno verso lo sviluppo di una leadership equa ed il contrasto di stereotipi, divari, penalizzazioni e disparità a tutti i livelli.

Qintesi ha anche ottenuto recentemente tre importanti riconoscimenti:

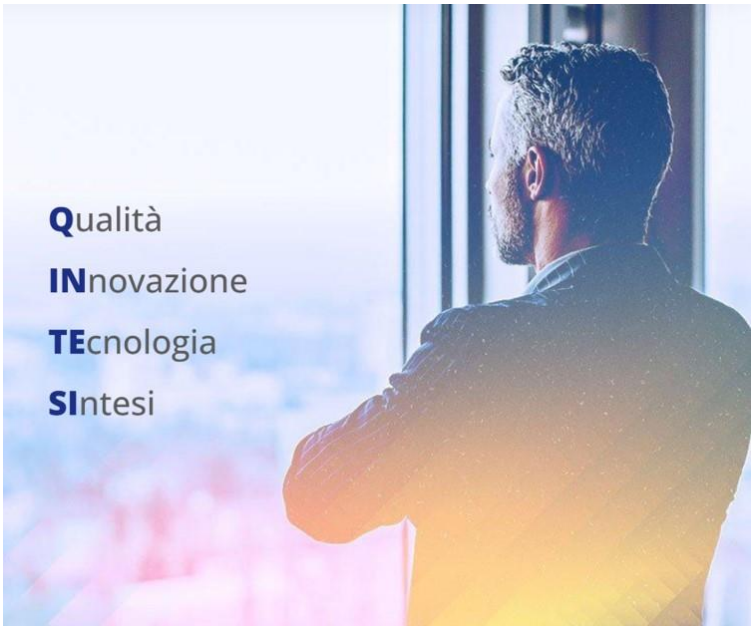
- **Rating della Legalità,** attribuito da **AGCM**, Autorità Garante della Concorrenza e del Mercato, per gli alti standard di qualità di Qintesi e l'attenzione posta sui principi etici nei comportamenti aziendali;
- **Campione della Crescita 2023**, attribuito per il terzo anno consecutivo da uno studio 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.

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/

AIPSA

Associazione Italiana Professionisti Security Aziendale ha come scopo istituzionale di valorizzare l'ordinamento professionale del Security Manager, formare ed aggiornare gli associati, diffondere la cultura della Security ed approfondire lo studio delle sue problematiche di ordine tecnico, funzionale, giuridico e legislativo.

https://www.aipsa.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/

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

Assintel

Associazione Nazionale Imprese ICT, è l'associazione di categoria in ambito Confcommercio: promuove incontri territoriali, gruppi di lavoro tematici e mette a disposizione un portale associativo per fare network tra le aziende che operano nel mercato dell'ICT.

http://www.assintel.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

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 Dirigenti di informatica Torino

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT dell'area torinese- piemontese, che si propone come punto di riferimento e di incontro per chi si occupa di information management. 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://cdtiroma.ning.com/

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

http://www.clubtier.org/

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/

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/

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/

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/cms/index.php

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 - Riferimenti e fonti

E.1 Dall'OCI all'OAI e a OAD: un po' di storia ….

- 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
- Presidenza del Consiglio dei Ministri: "Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico", Dicembre 2013, http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf
- Presidenza del Consiglio dei Ministri: "Piano nazionale per la protezione cibernetica e la sicurezza informatica", Marzo 2017, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf
- NIS, Network and Information Security, *Direttiva EU* 2016/1148, per la sicurezza digitale dei servizi essenziali e delle infrastrutture critiche dei vari paesi europei; sua adozione in Italia col D.Lgs. 65/2018
- Cyber Security Act, Direttiva EU 2019/881, in vigore dal 27/6/2019
- DPCM n. 181 del 30 luglio 2020, entrato in vigore il 5 novembre 2020, sul "Perimetro di sicurezza nazionale cibernetica"
- PNRR, Piano Nazionale Di Ripresa e Resilienza, in Italia: approvazione europea e stato della sua attuazione in https://temi.camera.it/leg18/pnrr.html
- DECRETO-LEGGE 14 giugno 2021, n. 82: Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/SG
- ACN, Agenzia Cybersicurezza Nazionale: https://www.acn.gov.it/
- AGID, Agenzia per l'Italia Digitale: https://www.agid.gov.it/

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.

- 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/
- 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; http://www.weforum.org/issues/global-risks.

ALLEGATO F - AIPSI

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica (https://www.aipsi.org/), capitolo italiano della mondiale **ISSA** (https://www.issa.org/), è una **associazione no-profit solo di persone fisiche** che si occupano a qualsiasi livello e in qualsiasi ruolo professionale di sicurezza digitale.
Il socio AIPSI è contemporaneamente socio ISSA, e gode dei servizi offerti da AIPSI e da ISSA più avanti elencati.

Il principale obiettivo di AIPSI, così come quello di ISSA, è di aiutare i propri soci nella **crescita professionale** e nell'**aggiornamento continuo delle loro competenze** sui diversi temi tecnici, organizzativi, normativi e legislativi della sicurezza digitale.
La crescita professionale è strutturata in varie fasi sull'intero ciclo di vita professionale CSCL, Cyber Security Career Lifecycle, di ISSA, contestualizzata da AIPSI alla realtà italiana (https://www.aipsi.org/aree-tematiche/sig-riservati-ai-soci/crescita-e-percorsi-professionali.html).

Gli elementi che caratterizzano AIPSI includono la reale indipendenza ed autonomia da qualsiasi fornitore ed ente, anche in caso di sponsorizzazioni, la qualità ed il livello professionale sempre ricercato per le proprie iniziative, l'etica professionale dei soci (sottoscritto dal codice etico ISSA), l'internazionalità che consente di avere contatti e di coinvolgere esperti dei vari Capitoli di ISSA a livello mondiale.

L'appartenenza al contesto internazionale ISSA permette ai soci di interagire con gli altri capitoli europei, americani e del resto del mondo. ISSA ed AIPSI sono focalizzate nel mantenere la posizione di "Global voice of Information Security": in tale ottica AIPSI collabora attivamente con altre associazioni italiane per effettuare congiuntamente varie iniziative, ed è socio attivo di FidaInform, la Federazione Nazionale delle Associazioni Professionali di Information Management, che federa varie associazioni a livello prevalentemente regionale (https://fidainform.it/).

AIPSI ha realizzato, e sta realizzando, specifiche iniziative a livello italiano, che si affiancano a quelle erogate a livello internazionale da ISSA.

Le **iniziative AIPSI aperte a tutti** includono:

- **webinar** sui vari temi della sicurezza digitale, si veda la documentazione relativa nell'archivio storico del sito web di AIPSI;
- **la Newsletter AIPSI** mensile inviata ad una mailing list di più di 5.000 utenti registrati;
- l'iniziativa **AIPSI Giovani** per coinvolgere i giovani interessati alla cybersecurity (https://www.aipsi.org/aree-tematiche/aipsi-giovani.html);
- **l'indagine OAD**, Osservatorio Attacchi Digitali in Italia, per la quale è stato realizzato un sito ad hoc, https://www.oadweb.it/, quale punto di riferimento e repository di tutti i rapporti annualmente pubblicati e di tutta la documentazione, ultimamente anche i videostreaming, degli eventi tenuti per presentare e discutere i dati emersi dalle indagini anno per anno;
- **CSWI**, Cyber Security Women's Italy, gruppo di lavoro sul lavoro femminile nella cybersecurity in Italia, che nel 2020 e nel 2021 ha prodotto due indagini, scaricabili, insieme alla documentazione delle altre attività di CSWI, da https://www.aipsi.org/aree-tematiche/cswi-cyber-security-women-s-italy.html.

Le **iniziative AIPSI riservate ai soli Soci** includono. alla data:

- **Mentorship** di indirizzamento e di crescita professionale, https://www.aipsi.org/aree-tematiche/sig-riservati-ai-soci/crescita-e-percorsi-professionali/mentorship-aipsi.html
- il supporto ed un significativo sconto per la **certificazione eCF** (UNI EN 16234-1:2016) per le figure di Security Manager e Security Specialist tramite AICA, accreditata Accredia;
- **sconti** con alcuni fornitori per la partecipazione a corsi anche online;
- la possibilità di partecipare, per conto di AIPSI-ISSA, ad eventi e a tavoli istituzionali e pubblicare articoli, anche in collaborazione di altri Soci, su varie riviste, incluso il prestigioso ISSA Journal;
- i **Gruppi di Lavoro specialistici** (SIG italiani):
  - l'uso dell'Intelligenza Artificiale in ambito sicurezza digitale per strumenti di sicurezza, di gestione, di analisi vulnerabilità e rischi, etc.;
  - nuove logiche ed architetture per la sicurezza digitale, che includono ad esempio Zero Trust, SASE, SOAR, etc.;
  - crescita e percorsi professionali per la sicurezza digitale, con riferimento a CSCL, certificazioni individuali, corsi, **mentorship** tra Soci. In questo ambito iniziano ad essere importanti anche in Italia le **"**onorificenze ISSA**"** per i meriti acquisiti professionalmente e nella vita dell'associazione, meriti che devono essere tutti documentati e valutati da apposite commissioni AIPSI ed ISSA**;**
- **n**etwork **s**oci a livello nazionale

I principali servizi erogati da ISSA ed utilizzabili dai soci AIPSI includono:

- **la rivista mensile** ISSA Journal**;**
- **l'indagine** ESG ISSA "The Life and Times of Cyber Security Professionals"**;**
- **c**onvegni, workshop, webinar in inglese**;**
- **c**orsi online in inglese**;**
- **partecipazione a vari** SIG, Special Interest Group**, ISSA i cui argomenti cambiano nel tempo;**
- **a**ccordi **con fornitori vari per** sconti **su corsi e** certificazioni individuali**;**
- **n**etwork **s**oci a livello mondiale**.**

ALLEGATO G - Profilo dell'autore Marco R. A. Bozzetti

Marco Rodolfo Alessandro Bozzetti, ingegnere elettronico laureato al Politecnico di Milano, è fondatore e amministratore di Malabo S.r.l (www.malaboadvisoring.it), società di consulenza direzionale sull'ICT (Information and Communication Technology) attiva da febbraio 2001.
Attraverso Malabo, Marco ha condotto e conduce**,** insieme ai suoi collaboratori**,** interventi presso Aziende ed Enti lato sia offerta sia domanda ICT.
Marco ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti ed Italtel, e di consulenza, quali Arthur Andersen Management Consultant e GEA/GEALAB, oltre ad essere stato il primo responsabile dei sistemi informativi dell'intero Gruppo ENI (1995-2000). In tale posizione ha realizzato la terziarizzazione delle infrastrutture ICT dell'intero Gruppo**,** a quella data una delle più grandi terziarizzazioni in Italia e in Europa. Agli inizi della sua carriera, in ambito Olivetti e del CREI del Politecnico di Milano, è stato uno dei primi ricercatori a livello mondiale ad occuparsi di internetworking, a partire dalla sua tesi di laurea dal titolo "Rounting and Internetworking". Nel corso della sua carriera Marco ha fondato e ha diretto o è stato partner di alcune aziende dell'offerta ICT, tra le quali CA.SI, Abiemme, Ibimaint System Engineering, ClickICT**,** System Engineering**.** Negli anni '90 e fino al 2003 ha ideato e coordinato per SMAU EITO, European Information Technology Observatory, l'indagine annuale europea sul mercato ICT e sui suoi trend. Dal 2009 ha ideato e realizzato ogni anno l'indagine OAD, Osservatorio Attacchi Digitali in Italia (https://www.oadweb.it/).
A livello consulenziale innumerevoli gli interventi tecnici-organizzativi sui sistemi informati**v**i di medie e grandi **a**ziende private, oltre che di alcuni **e**nti pubblici. aventi il principale obiettivo di allineare l'ICT al business, di innovarlo e di generare valore effettivamente misurabile. I principali campi di intervento includono il governo e la gestione di un sistema informativo, la sicurezza digitale, l'analisi e gestione dei rischi ICT e dei loro impatti (BIA), il disegno di architetture ICT, la razionalizzazione, la definizione ed il supporto di strategie ICT, l'assessment delle tecnologie, delle competenze e dei ruoli ICT, l'analisi del valore per l'ICT, l'innovazione tramite l'ICT, la riorganizzazione di strutture e processi, il supporto per la compliance alle varie normative, in particolare alla privacy secondo il GDPR.
Fin dall'inizio della sua carriera al CREI, ha realizzato e tenuto corsi di formazione in aula, e più recentemente anche online, su vari argomenti tecnici e manageriali, sia presso clienti finali sia presso enti di formazione, anche per master. Gli argomenti prevalentemente trattati: agli inizi il modello OSI ed suoi protocolli, la sua evoluzione nello stack TCP/IP di Internet, l'office automation, e successivamente le architetture ICT, la SOA (Service Oriented Architecture) e la sua evoluzione negli attuali microservizi in cloud, la sicurezza digitale, l'analisi dei rischi e delle vulnerabilità, ITIL e COBIT, la business continuity ed il Disaster Recovery, la gestione operativa di un sistema informativo, la governance strategica dell'ICT, la trasformazione digitale di un'impresa. In tutti i suoi corsi ha inserito la sua diretta esperienza con casi reali di intervento presso aziende/enti nei quali ha svolto consulenza e/o realizzato interventi progettuali ed implementativi.
Marco è stato Presidente e VicePresidente di FidaInform, di SicurForum in FTI e del ClubTI di Milano, oltre che componente del Consiglio del Terziario Innovativo di Assolombarda.
È attualmente Presidente di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica e Capitolo Italiana della mondiale ISSA, nel Consiglio Direttivo **e Tesoriere** di FIDAInform, socio e revisore dei conti del ClubTI di Milano, socio AICA **.** Dal 2023 partecipa come esperto all'iniziativa europea ESSA (https://www.softwareskills.eu/) sulle competenze per lo sviluppo di software.
È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser". È Commissario d'Esame in AICA per le certificazioni eCFPlus (EN 16234-UNI 11506).
Ha pubblicato numerosi articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, le normative, gli scenari e gli impatti dell'ICT.
I curricula di maggior dettaglio, in italiano e in inglese, e l'elenco delle sue pubblicazioni, sono scaricabili da: https://www.malaboadvisoring.it/it/chi-siamo/marco-rodolfo-alessandro-bozzetti/curricula-e-pubblicazioni-di-marco-r-a-bozzetti.html
Su LinkedIn: https://www.linkedin.com/in/marco-rodolfo-bozzetti-8a71ba/?originalSubdomain=it

ALLEGATO H - MALABO Srl

Malabo Srl, https://www.malaboadvisoring.it/, opera dal 2001 nell'ambito della consulenza direzionale sull'ICT (Information and Communication Technology) e sul digitale, basandosi su una rete consolidata di esperti "senior" e di società ultra-specializzate, per clienti lato sia offerta sia domanda ICT,.
Malabo dispone di un piccolo laboratorio ICT, in parte in cloud e in parte on premise, con il quale può installare e testare sistemi e piattaforme ICT che potrebbero essere utilizzate in un suo progetto per un Cliente.

Malabo è in grado di fornire, ai Clienti sia della domanda che dell'offerta ICT:

- interventi **consulenziali e di mentorship/coaching**
  - presso il responsabile del sistema informatico (CIO) e del suo staff: riorganizzazione della sua struttura, rapporti con l'alta direzione e con le altre direzioni, miglioramento della gestione operativa e della "governance" del Sistema Informatico, ruolo di supervisore o di capo progetto in progetti critici, 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 Sistema Informatico, per migliorare ed accelerare la trasformazione digitale, per migliorare la governance del Sistema Informatico, Piano di Business Continuity e suo periodico test, analisi del valore dell'ICT, etc.**;**
  - 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 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 concretamente il cliente nell'uso efficace ed efficiente dell'ICT in modo da incrementare l'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, il governo strategico e la gestione operativa di un sistema informativo, la conformità a normative e standard (compliance), le competenze, i profili ed i ruoli ICT nell'organizzazione.

I principali vantaggi competitivi di Malabo, così come percepiti dai suoi 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, il fornire servizi on line e formazione per gli utenti finali e privilegiati.

OAD
Osservatorio
Attacchi Digitali
in Italia

Associazioni Patrocinanti OAD2023

malabo
ICT Advisory

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

ISSA
Information Systems Security Association