OAD
Osservatorio
Attacchi Digitali
in Italia

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

RAPPORTO 2024 OAD

A CURA DI MARCO R. A. BOZZETTI

In collaborazione con:

AICA · Polizia Postale · FIDA INFORM · malabo ICT Advisory

Silver Sponsor

QINTESI

Prefazione di:
Ivano Gabrielli, Direttore Polizia Postale e delle Comunicazioni
Alessandro Musumeci, Capo della Segreteria Tecnica del Sottosegretario all'Innovazione Tecnologica

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 2024.
Uno speciale ringraziamento agli estensori delle due prefazioni al Rapporto:

- al dott. Ivano Gabrielli, Direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica
- all'ing. Alessandro Musumeci, Capo della Segreteria Tecnica del Sottosegretario all'Innovazione Tecnologica

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

- per AIPSI: Massimo Chirivì, dott.ssa Elena Bernucci
- per Malabo Srl: dott. Andrea Bozzetti, dott. Francesco Zambon
- per il Servizio Polizia Postale e per la Sicurezza Cibernetica, che ha fornito dati e testi del Capitolo 8: il Direttore dott. Ivano Gabrielli, l'Ispettore dott. Gaetano Martucci e dell'Assistente Luigi Ummaro.

Dichiarazione di non responsabilità

I grafici ed i testi del presente Rapporto OAD 2024 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 2024** 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 2024**.

OAD è un progetto scelto da Repubblica Digitale

Rapporto OAD 2024 pubblicato il 20 ottobre 2024.

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

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

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

INDICE Rapporto OAD 2024

Sommario

INDICE Rapporto OAD 2024 3

PREFAZIONI 7

PREFAZIONE del dott. Ivano Gabrielli 8

PREFAZIONE dell'ing. Alessandro Musumeci 9

1. Sintesi direzionale 10

1Bis Executive Summary 15

2. L'indagine OAD 19

2.1 L'indagine OAD 2024 19

3. Il quadro generale degli attacchi digitali intenzionali 22

3.1 Il quadro a livello europeo 24

3.2 I principali attacchi digitali a livello mondiale nel 2023 28

3.2.1 Esempi di significativi di attacchi a livello mondiale nel 2023 29

3.3 I principali attacchi digitali in Italia nel 2023 32

3.4 Le vulnerabilità causa degli attacchi 36

3.4.1 Le vulnerabilità tecniche 36

3.4.2 Le vulnerabilità delle persone 37

3.4.3 Le vulnerabilità organizzative 39

3.5 Gli attaccanti e le loro motivazioni 39

3.6 Le contromisure per la sicurezza digitale e la loro evoluzione 40

3.6.1 La terziarizzazione della sicurezza digitale 43

3.7 Il quadro di riferimento Italiano per la sicurezza digitale 43

3.7.1 Aziende e PA in Italia 43

3.7.2 La spesa in sicurezza digitale in Italia nel 2023 45

3.7.3 Il PNRR ed il suo impatto nella trasformazione digitale del Paese 46

3.7.4 Le Istituzioni per la sicurezza digitale 47

3.7.5 Le leggi italiane in vigore per la sicurezza informatica 49

4. Gli attacchi digitali in Italia dall'indagine OAD 2024 51

4.1 Tipologie e tecniche di attacco emerse 54

4.2 Gli attacchi digitali alle applicazioni ed agli ambienti web in Italia 57

4.3 Gli attacchi digitali ai sistemi OT in Italia 66

5. Tipologie attacchi digitali e tecniche di attacco più temute nel prossimo futuro 74

6. Il campione delle aziende/enti rispondenti e dei loro SI 77

6.1 L'Azienda/Ente rispondente 78

6.2 Tipologia, ruolo e principali caratteristiche dei sistemi informativi 81
6.3 Ruolo della persona rispondente 87
Cap. 7 Le misure di sicurezza digitale nei sistemi informativi (SI) 89
7.1 Le misure organizzative per la sicurezza digitale dei SI 92
7.1.1 La struttura organizzativa per la sicurezza digitale ed il ruolo di CISO 93
7.1.2 Policy e procedure organizzative per la sicurezza digitale 94
7.1.3 Analisi dei rischi digitali e dei possibili impatti 98
7.1.4 Auditing sulla sicurezza digitale 101
7.1.5 Certificazioni aziendali e individuali sulla sicurezza digitale 103
7.2 Le misure tecniche di sicurezza digitale 105
7.2.1 Architetture per la sicurezza digitale 105
7.2.2 Misure tecniche di sicurezza fisica e perimetrale 108
7.2.3 Identificazione, autenticazione e autorizzazione degli utenti 112
7.2.4 Misure tecniche di sicurezza delle reti dei sistemi informativi 115
7.2.5 Misure di sicurezza delle applicazioni nei SI 117
7.2.6 Misure tecniche di sicurezza digitale per la protezione dei dati 121
7.2.7 Misure e strumenti per la gestione ed il controllo della sicurezza digitale dei SI ... 125
7.3 Le misure di sicurezza per gli ambienti OT 137
Cap 8 Contributo della Polizia Postale e per la Sicurezza Cibernetica 142
PREMESSA 145
CENTRO NAZIONALE ANTICRIMINE INFORMATICO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE (C.N.A.I.P.I.C.) – COMPUTER CRIME 148
PREVENZIONE CYBERTERRORISMO 149
LE FRODI INFORMATICHE 150
LE TRUFFE ONLINE 150
REATI CONTRO LA PERSONA 150
ALLEGATI 151
Allegato A Aspetti metodologici dell'indagine OAD 2024 152
A.1 L'indagine OAD 2024 154
A.2 La tassonomia degli attacchi digitali per OAD 2024 155
A.2.1 Le classi di tecniche di attacco considerate (come si attacca) 156
A3 La macro valutazione qualitativa del livello di sicurezza digitale del sistema informatico oggetto delle risposte al questionario 159
ALLEGATO B Glossario 160
ALLEGATO C Profili SPONSOR SILVER 172

Gruppo Qintesi 173
Allegato D Profilo Patrocinatori 176
Allegato E Principali fonti e riferimenti 181
E.1 Dall'OCI all'OAI e a OAD: un po' di storia della sicurezza digitale in Italia 182
E.2 Le principali fonti sugli attacchi e sulle vulnerabilità 182
Allegato F AIPSI 184
Allegato G Malabo srl 186
Allegato H Il profilo dell'autore Marco R. A. Bozzetti 188

PREFAZIONI

PREFAZIONE del dott. Ivano Gabrielli

Come Direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica, sono lieto di presentare la mia recensione del Rapporto OAD 2024, un documento importante per comprendere l'evoluzione delle minacce digitali e le misure di sicurezza adottate dalle aziende e dagli enti pubblici in Italia.

Il Rapporto OAD 2024, giunto alla sua 17ª edizione, rappresenta un punto di riferimento imprescindibile per tutti gli operatori del settore della sicurezza informatica. L'indagine, condotta in modo rigoroso e anonimo, offre una panoramica dettagliata sugli attacchi digitali intenzionali subiti nel 2023, con un focus particolare sugli attacchi ai sistemi informativi e agli ambienti OT (Operational Technology) delle aziende rispondenti.

Uno degli aspetti più rilevanti del rapporto è l'analisi delle misure di sicurezza digitali in uso, sia tecniche che organizzative. Questa sezione fornisce una valutazione complessiva del livello di sicurezza digitale delle aziende, evidenziando le principali aree di miglioramento e le *best practice* adottate. È incoraggiante notare come molte aziende stiano investendo in tecnologie avanzate e in formazione per il personale, dimostrando una crescente consapevolezza dell'importanza della sicurezza informatica.

Se il 2022 è stato l'anno che potremmo definire del riscatto sociale dopo il biennio precedente contrassegnato dalla pandemia da COVID-19 con i suoi lunghi e forzosi lockdown, durante i quali tutti, privatamente e lavorativamente, abbiamo fatto ricorso alla tecnologia per continuare a vivere nonostante l'isolamento sociale, il 2023 è stato sicuramente l'anno della consapevolezza dell'importanza di investire in sicurezza informatica e in *awareness*.

Il rapporto sottolinea anche l'importanza della collaborazione tra settore pubblico e privato per affrontare le sfide poste dalle minacce digitali. La Polizia Postale, in questo contesto, gioca un ruolo cruciale nel prevenire e contrastare i crimini informatici, lavorando a stretto contatto con le aziende e le istituzioni per garantire la sicurezza delle infrastrutture critiche e dei dati sensibili.

Il Rapporto OAD 2024 è uno strumento informativo essenziale per chiunque operi nel campo della sicurezza informatica. Le informazioni dettagliate e le analisi approfondite contenute nel rapporto offrono una guida preziosa per migliorare le strategie di difesa e per rimanere aggiornati sulle ultime tendenze e minacce nel panorama digitale.

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

PREFAZIONE dell'ing. Alessandro Musumeci

Il rapporto OAD 2024, arrivato ormai alla diciassettesima edizione consecutiva, rappresenta un insostituibile strumento di analisi, di comprensione e di prevenzione delle minacce informatiche.

Continua una larghissima e grave diffusione di attacchi digitali con forti impatti sui sistemi informativi attaccati, anche a causa dell'incremento dello sviluppo dei sistemi di intelligenza artificiale di tipo generativo, che permettono di realizzare attacchi informatici sempre più sofisticati. E' fondamentale, pertanto, avere un osservatorio che non solo "fotografi" la situazione, ma dia anche indicazioni concrete agli operatori, pubblici e privati, su come prevenire attacchi e frodi che possono causare seri danni alle aziende, alle istituzioni finanziarie, alle infrastrutture di produzione e distribuzione dell'energia, ai sistemi di trasporto ed in definitiva alla popolazione e alle stesse istituzioni democratiche.

Per questo motivo ho aderito all'invito dell'amico e collega, Ing. Marco Bozzetti, con cui ho avuto il piacere di collaborare svariati anni fa, quando ero direttore specialistico dei sistemi informativi del Comune di Milano, ad introdurre questa sua ennesima fatica, che "fa il punto" sullo stato attuale della Cybersecurity nel nostro Paese, e al tempo stesso costituisce un prezioso strumento per far crescere la cultura della sicurezza nelle varie fasce della popolazione.

Il fattore umano, infatti, rappresenta l'anello più debole della catena di Cybersecurity che caratterizza qualunque sistema di protezione aziendale; tale elemento è messo sempre più in crisi dai sistemi di intelligenza artificiale di tipo generativo, che "apprendono" le possibili debolezze dei sistemi informatici e pianificano le strategie più opportune per attaccarli e realizzare crimini e frodi.

Pertanto, il rapporto OAD 2024, può essere anche un valido strumento didattico, non solo nelle scuole e nelle università ma anche nei punti di facilitazione digitale attivi nel nostro Paese, per diffondere a tutti i livelli la cultura informatica e la consapevolezza che solo un utilizzo responsabile dei sistemi informatici, a tutti i livelli (servizi Web, social media, ecc….) può prevenire disservizi e frodi causate da delinquenti che, con diverse motivazioni, attaccano i sistemi informativi aziendali.

Solo la crescita della cultura informatica nelle varie fasce della popolazione potrà tutelarci maggiormente dalle minacce informatiche prossime venture e dai rischi insiti nei sistemi di intelligenza artificiale di tipo generativo (che ovviamente aprono anche infinite opportunità di progresso scientifico e tecnologico). Il rapporto OAD 2024 rappresenta un notevole passo avanti in tale crescita e nell'acquisizione di una maggiore consapevolezza dei rischi e delle opportunità correlate all'innovazione tecnologica.

Alessandro Musumeci
Capo della Segreteria Tecnica del Sottosegretario all'Innovazione Tecnologica

1. Sintesi direzionale

L'Osservatorio Attacchi Digitali in Italia, OAD[1], con la presente edizione 2024 giunge al diciassettesimo 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 per la Sicurezza Cibernetica, che ha fornito dati e testo del Capitolo 8 del presente Rapporto.
L'indagine online **OAD 2024** fa riferimento agli attacchi intenzionali rilevati **nell'intero anno 2023,** ed evidenzia il **permanere di una larga e grave diffusione di attacchi digitali** con forti impatti sui sistemi informativi (SI) delle aziende ed enti rispondenti.

L'anno **2023** ha visto un **peggioramento della situazione geopolitica a livello mondiale**, con guerre digitali in pieno corso quali l'invasione della Federazione Russa in Ucraina a febbraio 2022 e la difesa di quest'ultima, e la "guerra" tra lo Stato di Israele e Hamas, chiamata anche la guerra di Gaza, causata dall'attacco terroristico del 7 ottobre 2023 ad Israele da parte di Hamas. A fianco di questi due eventi, che sono sola la punta del critico e pericoloso iceberg geopolitico, e che hanno portato innumerevoli attacchi digitali, è fortemente cresciuta la **disinformazione e la mala informazione**, inizialmente assai preoccupante in Europa soprattutto per le elezioni 2024 (ora passate), e le tecniche di Intelligenza Artificiale (IA) usate in vari strumenti di attacco. Insieme al "tradizionale" crimine informatico, tutto questo ha portato il 2023 ad avere ancora una **altissima diffusione di attacchi digitali intenzionali**, con gravi impatti sia sul budget del SI sia, in certi casi, sul conto economico dell'azienda/ente rispondente.

Il Rapporto OAD 2024 nel Capitolo 3 fa un quadro della situazione degli attacchi digitali a livello mondiale, con riferimento anche al World Economic Forum e a livello europeo con riferimento ai rapporti di ENISA, l'Agenzia Europea per la cybersicurezza (si veda §3.1). Il paragrafo §3.2 riporta esempi di alcuni dei più significativi attacchi perpetrati nel 2023. A livello nazionale il Rapporto considera, oltre ai risultati emersi dall'indagine online OAD 2024, che costituiscono il cuore del Rapporto stesso e sono dettagliati nel Capitolo 4, anche i principali dati dal rapporto annuale al Parlamento di ACN, l'Agenzia per la Cybersicurezza Nazionale (§3.3), e quelli forniti dalla Polizia Postale e per la Sicurezza Cibernetica (§8).

Il questionario online via web di OAD 2024 ha posto due sole domande sugli attacchi digitali subiti nel 2023 dai SI delle aziende/enti rispondenti, in modo da poter continuare l'analisi dei trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 ad oggi, ed ha approfondito gli attacchi digitali rilevati nel 2023 **alle applicazioni ed agli ambienti web** ed ai **sistemi OT, Operation Technology**.

OAD distingue chiaramente che cosa si attacca, la tipologia d'attacco classificata in 15 macro voci, ed il come si attacca, le tecniche usate per l'attacco e distinte in 7 macro voci (per il dettaglio metodologico si rimanda all'Allegato A, per quanto rilevato dall'indagine al Capitolo 4).

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

Nel corso dell'intero 2023, il **72,4%** delle aziende/enti rispondenti ha subito attacchi digitali ai propri SI. Per questi i **tipi di attacchi più diffusi** includono:

- le **modifiche malevoli/non autorizzate ai programmi e alle configurazioni dei sistemi ICT,** con il **31,7%** delle risposte; a questo primo posto sicuramente contribuisce la larghissima diffusione di malware e di ransomware in Italia;
- gli attacchi **DoS/DDoS**, per la saturazione dei sistemi ICT connessi ad Internet, con il **20,7%**; sono stati uno degli attacchi più usati nell'ambito delle cyber warfare, in particolare da parte delle organizzazioni hacker schierate pro Russia;
- l'**uso non autorizzato e malevolo di sistemi ICT del SI**, con il **18,3%**;
- **gli attacchi alla supply chain informatizzata,** con il **15%**: questa è la tipologia di attacco aggiunta alla precedente tassonomia di attacchi di OAD, e il dato conferma la diffusione e la criticità di questa tipologia d'attacco, considerata dal World Economic Forum uno dei principali rischi a livello mondiale;
- Il **furto di dispositivi mobili**, con il **13,4%**, prevalentemente per gli smartphone, i moderni cellulari, che da un lato contengono, talvolta senza protezione alcuna, preziose informazioni dell'identità digitale del proprietario, come le password e le modalità di accesso ai servizi informatici utilizzati, dall'altro hanno un alto valore sul mercato dell'usato. Entrambe motivazioni importanti per il loro furto.

Tutte le altre tipologia d'attacco considerate nella tassonomia OAD hanno percentuali al di sotto del 10% e per la prima volta con OAD 2024 i sistemi di controllo degli accessi (IAA, Identificazione-Autenticazione-Autorizzazione) e gli attacchi alle reti geografiche/locali non sono ai primi posti di questa classifica, come lo erano invece nelle precedenti edizioni di OAD.

Le **tecniche di attacco più diffuse** negli attacchi più gravi vedono ai primi posti:

- l'uso di **più tecniche per lo stesso attacco** con il **40,4%;**
- **raccolta illegale di informazioni**, ottenute tipicamente con il **social engineering**, con il **37,6%**;
- i **codici maligni**, alla base degli assai diffusi attacchi di ransomware, con il **25,3%.**

La correlazione dei dati sugli attacchi rilevati con le dimensioni ed il fatturato delle aziende/enti rispondenti mostra anche per il 2023 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.

L'indagine "verticale" sugli **attacchi ai siti, alle applicazioni e agli ambienti web** (descritto in §4.2) si è basata, dal punto di vista tecnico, sulla verifica delle cause degli attacchi più gravi subiti in riferimento alle principali vulnerabilità e rischi indicati a livello mondiale da OWASP[2]. La maggior parte delle applicazioni sono di tipo web, e molte di queste sono in cloud: i moderni SI, indipendentemente dalle loro dimensioni, sono quindi in parte in locale (on premise) e in parte su uno o più cloud di fornitori diversi, il multi cloud. Da qui la motivazione di approfondire le cause tecniche degli attacchi rilevati dalle aziende/enti rispondenti all'indagine. Da questo bacino emerge che il **58,4%** ha **rilevato attacchi** alle applicazioni ed agli ambienti web, e di questi il **60,6%** li ha subiti nei propri ambienti web **in cloud** (ambienti in cloud che dovrebbero essere più sicuri di quelli on premise). Le vulnerabilità associate a questi attacchi, in particolare quelli più gravi, sono state identificate per il **92,3%** come di **natura personale**, in parte influenzate dall'organizzazione, come ad esempio la mancanza di formazione degli utenti. **Inoltre, il 82,7% delle vulnerabilità è di tipo tecnico.**

[2] OWASP, Open Web Application Security Project, iniziativa che formula a livello mondiale linee guida, strumenti e metodologie per migliorare la sicurezza delle applicazioni in ambito web.

Con riferimento alle 10 principali vulnerabilità per l'ambiente web di OWASP, per gli attacchi **più gravi** rilevati dalle aziende/enti rispondenti, sono al primo posto i **componenti software obsoleti** e vulnerabili, con il **31,7%**. Segue, con il **20,4%**, **l'errata configurazione** degli strumenti di sicurezza.
Il questionario OAD 2024 ha esaminato quali dei 10 principali rischi delle **interfacce API**[3] **negli ambienti web** elencate da OWASP, ed il risultato evidenzia **l'API** Security Misconfiguration come la causa più diffusa e grave per gli attacchi agli ambienti web dei rispondenti.
L'**impatto** dell'attacco più grave agli ambienti web **a livello tecnico** è stato **pesante** per i SI delle aziende/enti rispondenti, con il **85,3%** dei casi che ha riscontrato un disservizio nel SI durato **da 2 giorni in su**. Anche **l'impatto economico** è stato **significativo,** per il **86,5%** con un **aumento dei costi** sul **budget** del SI, e per il **24%** il ripercuotersi dei costi anche **sul bilancio dell'azienda/ente**.
Le **probabili motivazioni** per l'attacco più grave sono, per **quasi i 2/3 dei rispondenti**, di **tipo economico** con **la frode ed il ricatto** . Per la prima volta rispetto alle precedenti edizioni OAD, la motivazione di **cyber warfare** è al terzo posto con un **20,2%**.

L'indagine "verticale" sugli **attacchi agli ambienti OT**[4] (descritto in §4.3) ha coinvolto solo aziende/enti che hanno dichiarato di utilizzare sistemi OT, il **37%** del totale dei rispondenti: di questi, il **48,2**% ha dichiarato di aver **subito attacchi ai propri sistemi OT**.
L'**impatto** dell'attacco più grave ad un sistema OT è stato molto alto, in termini di blocco del sistema: per **circa 1/3** dei rispondenti il **blocco è durato tra i 2 e 3 giorni**, ma **per quasi la metà è durato più di 3 giorni.**
Poiché la maggior parte dei sistemi OT interagisce oggi con le applicazioni del sistema informativo, il blocco si è esteso anche a queste ultime, causando significativi disservizi. In particolare, il **40,7%** degli intervistati ha riportato **interruzioni** delle applicazioni del sistema informativo della durata di **2-3 giorni** a causa di questo propagarsi.

Quanto emerge dall'indagine OAD 2024 è sostanzialmente allineato con quanto indicato dal World Economic Forum, da ENISA, da ACN e dal Servizio Polizia Postale e per la Sicurezza Cibernetica, che ha fornito ad OAD i dati sul crimine informatico rilevati nel 2023 e nel 1 semestre del 2024, riportati nel Capitolo 8 del presente Rapporto, cui si rimanda per i dettagli. La Tabella sottostante, elaborata coi dati forniti ad OAD negli anni, confronta alcuni dati rilevati dallo specifico gruppo della Polizia Postale C.N.A.I.P.I.C. per gli attacchi alle infrastrutture critiche italiane.

Protezione strutture critiche/essenziali	1 gen - 30 giugno 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Attacchi rilevati (*)	5.903 **	12.101 **	13.099	282	509	1181	459	1.032	844
Alert diramati	31.033	77.012	113.420	24.824	83.416	82.484	80.777	31.524	6.721
Indagini avviate (***)	36	96	110	34	103	155	74	72	70
Persone denunciate/indagate (*)	101 **	224 **	334	n.d.	105	117	14	1.316	1.226
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	23	79	77	17	69	79	108	83	85
Indagini avviate su attacchi rilevati	0,61%	0,79%	0,84%	12,06%	20,24%	13,12%	16,12%	6,98%	8,29%
Persone indagate su attacchi rilevati	1,71%	1,85%	2,55%	n.d.	20,63%	9,91%	3,05%	127,52%	145,26%

* Per il 2023-24: Target: Infrastrutture Critiche (I.C.), Operatori Servizi Essenziali (OSE), Pubbliche Amministrazioni Locali (PAL), Aziende, Privati
** Per il 2023-24: Dati aggregati C.N.A.I.P.I.C. e Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.).
*** Per il 2023-24 dal C.N.A.I.P.I.C.

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

Gli attacchi rilevati, gli allarmi diramati, le indagini avviate e le persone denunciate/indagate (prime quattro righe della tabella) sono diminuiti nel 2023 rispetto a quelle del 2022, pur rimanendo dello stesso ordine di grandezza, assai più alto degli anni prima del 2022.

[3] API, Application Programming Interface, è un insieme di regole e protocolli che consentono alle applicazioni software di comunicare tra loro per scambiare dati e funzionalità. Le API web vengono usate per consentire il trasferimento di dati e funzionalità via Internet con il protocollo HTTP/HTTPS.
[4] OT, Operational Technology, definisce un ampio insieme di sistemi ICT per controllare, monitorare ed automatizzare processi fisici ed i dispositivi e le infrastrutture che effettuano e/o supportano tali processi fisici. Tipici esempi di tali processi sono quelli manifatturieri, quelli chimici, quelli nucleari, quelli del controllo del territorio, delle reti di distribuzione dell'energia, e così via. Il concetto di OT è molto ampio ed include i sistemi ICS, Industrial Control System, i robot industriali e di ricerca, i sistemi di diagnostica medica, i sistemi IoT, Internet of Thinks e IIoT, Industrial IoT.

In termini di trend sugli attacchi digitali ad imprese/enti in Italia, l'andamento della Tabella in fig. 1-1 è simile a quello mostrato nel grafico di fig. 1-2, che mette a confronto gli attacchi rilevati dalle aziende/enti che hanno risposto negli anni all'indagine OAD. Dal 2016 gli attacchi rilevati dai rispondenti aumentano, e dal 2020 la percentuale delle aziende/enti attaccati supera quella dei non attaccati.

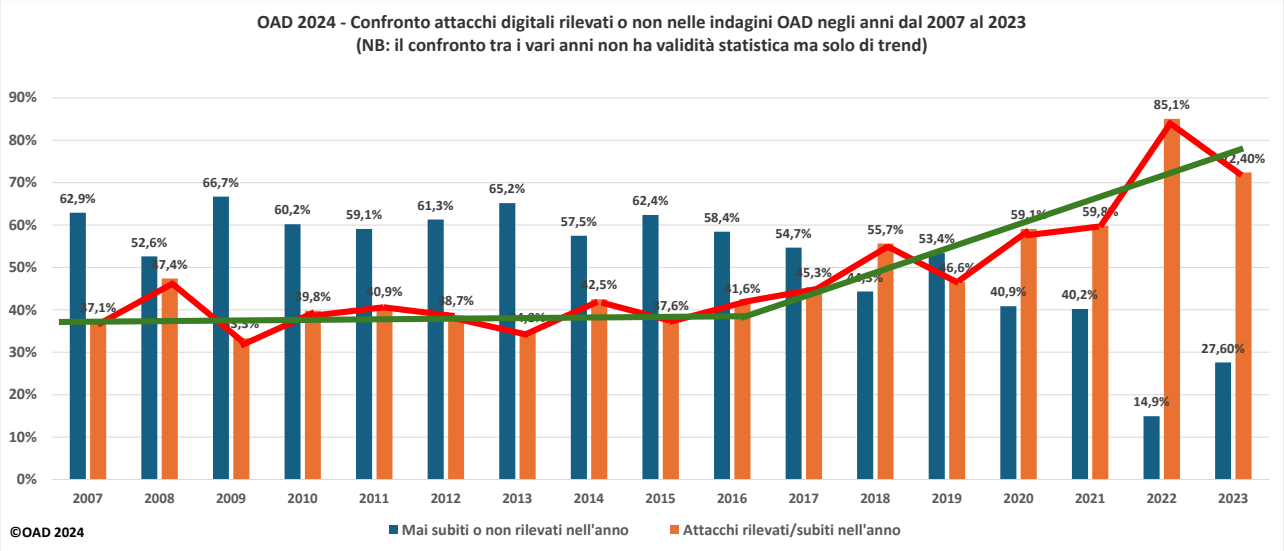


Fig. 1-2

Per comprendere e contestualizzare meglio i risultati sugli attacchi digitali, OAD esamina in generale il tipo di azienda o ente rispondente (§6.1), il tipo di sistema informativo utilizzato e la sua rilevanza per le attività e il business (§6.2), oltre alle misure di sicurezza digitali adottate.

Il bacino di aziende/enti rispondenti emerso dall'indagine copre tutti i settori merceologici, incluse le Pubbliche Amministrazioni, anche se i più numerosi risultano essere il settore **Istruzione** con il **23,6%**, il settore **Servizi Professionali e di supporto alle aziende** (avvocati, commercialisti, notai, etc.) con il **12,3%,** il settore **Industria manifatturiera e costruzioni** con l'**11%**.
In termini di dimensioni, come numero di dipendenti, hanno risposto il **69,8%** di piccole e medie organizzazioni, ossia quelle con meno di 250 dipendenti. Significativa, tra queste, il **22,9%** di organizzazioni con meno di 10 dipendenti, che in Italia costituiscono la stragrande maggioranza delle imprese.

Il **ruolo del SI** per supportare le attività ed i processi dell'impresa pubblica o privata è **essenziale** per il **70,1%** delle aziende/enti rispondenti e per questo motivo la sua sicurezza digitale deve essere di alto livello, efficace ed efficiente. Il **10,6 %** dei SI fornisce **servizi essenziali** per l'Italia, soggetti quindi al NIS e nel prossimo futuro alle nuove normative europee NIS2, DORA, etc.

Il SI è **gestito e controllato totalmente in Italia** per **l'85,4%** delle aziende/enti rispondenti, e per il **63,4%** è di piccole-medie dimensioni senza un Data Center. Il **92%** utilizza servizi ICT terziarizzati, soprattutto in cloud.
La **gestione operativa** del SI è effettuata totalmente **internamente** per **24,4%** dei rispondenti, tutti gli altri terziarizzano o in toto, il **38,6%**, o solo per alcune parti, il **37,1%**.
La **gestione operativa della sicurezza digitale** del SI è effettuata **internamente** dal **20%** dei rispondenti, **l'80% la terziarizza,** e di questi il **41,6% totalmente**. Il dato percentuale della "completa" terziarizzazione della gestione operativa della sicurezza digitale è alto e significativo: le piccole organizzazioni, salvo eccezioni, non

possono essere in grado di gestire autonomamente la sicurezza digitale, e devono fare pertanto ricorso a consulenti o a società specializzate.

Nel questionario OAD 2024, le domande sulle **misure tecniche, organizzative e di gestione della sicurezza digitale** presenti nei SI e nelle aziende/enti rispondenti **erano opzionali**: ad esse ha risposto il **35,4%** del totale di rispondenti. Nel capitolo 7 sono riportati i dati emersi dall'indagine OAD, cui si rimanda per i dettagli.
Nel complesso la **maggior parte dei rispondenti risulta avere buoni livelli di sicurezza sia fisica che organizzativa che gestionale**. Questo dato positivo è probabilmente dato anche dal fatto che aziende/enti con bassi livelli di sicurezza non hanno compilato la parte opzionale sulle misure di sicurezza,
Alcune carenze sono più diffuse, come è logico, nelle organizzazioni più piccole, soprattutto per gli aspetti organizzativi; anche le piccole organizzazioni utilizzano servizi terziarizzati per la gestione della sicurezza digitale.

I SI delle aziende/enti rispondenti si posizionano in gran parte **nella fascia alta** per le misure tecniche ed organizzative di sicurezza digitale implementate: ma nonostante questo hanno subito molti attacchi digitali, che hanno avuto forti impatti in termini di disservizi e di costi per il SI e per l'intera azienda/ente.

In estrema sintesi, **nel 2023 permane complessivamente l'ampia diffusione di gravi attacchi digitali e di un forte rischio cibernetico a livello mondiale, europeo e in Italia.**
Come ben si evidenzia dalla fig. 1-2 per l'Italia, dal 2020 si è entrati nell'**era della insicurezza digitale sistemica** (**systemic cyber insecurity**), una condizione che riguarda l'intero mondo.
Nonostante gli investimenti spesso onerosi in misure di sicurezza, queste non sono riuscite, né riescono tuttora, a prevenire completamente gli attacchi informatici. Di fronte a questa situazione, le soluzioni attuali, che richiedono un potenziamento anziché un abbandono, devono essere integrate con politiche di **resilienza** per l'intera organizzazione e il suo SI. Sul fronte aziendale, la resilienza può essere assicurata dalla **business continuity**, ossia la continuità operativa dei processi essenziali; mentre, sul versante ICT, da un piano di **Disaster Recovery** efficace, attuabile e testato.

1Bis Executive Summary

The **OAD** (Digital Attack Observatory) **2024** marks the **seventeenth consecutive year** of surveys on cyber attacks and cybersecurity measures in Italy. This edition benefits from the cooperation of the Italian Postal Police, which contributed data and authored Chapter 8 of this Report.
The OAD 2024 survey covers intentional cyber attacks detected throughout 2023, underscoring the ongoing and widespread impact of these attacks on the IT systems of the public and private companies participating this survey.

The year 2023 was marked by a worsening global geopolitical landscape, with cyber warfare associated with events such as the Russian Federation's invasion of Ukraine in February 2022 and the defense efforts that followed. Additionally, the conflict between Israel and Hamas, escalated following Hamas' terrorist attack on Israel on 7 October 2023.
These conflicts are part of a broader geopolitical crisis that has sparked numerous cyber attacks, alongside a significant increase in misinformation and disinformation. Furthermore, AI techniques have been increasingly utilized in cyber attack tools. Alongside traditional cybercrime, these factors have contributed to a persistently high number of intentional digital attacks in 2023, with significant impacts on the budgets for cyber security and, in some cases, the financial health of the attacked organizations.

In Chapter 3, the OAD 2024 Report offers a comprehensive overview of digital attacks on a global scale, with references to the World Economic Forum, and at a European level, citing reports from ENISA, the European Union Agency for Cybersecurity (see §3.1). It also highlights examples of some of the most significant attacks carried out in 2023 (see §3.2). On a national level, in addition to the findings from the OAD 2024 online survey—central to the report and detailed in Chapter 4—the Report examines key data from the annual report to Parliament by ACN, the National Cybersecurity Agency (see §3.3), as well as insights provided by the Italian Postal Police (see Chapter 8).

The OAD 2024 online questionnaire included only two questions about all the digital attacks suffered in 2023 by the IT systems of the responding companies. This approach aimed to continue analyzing general attack trends (what is targeted and the techniques used) from 2007 to the present.
It also delves into the specific digital attacks detected in 2023 on **web applications** and on **OT** (Operational Technology) systems.
OAD makes a clear distinction between what is targeted—the type of attack, categorized into 15 different macro-categories—and how it is attacked, referring to the techniques used, classified into 7 macro-categories (for methodological details refer to Annex A).
Throughout 2023, 72.4% of the responding companies reported experiencing digital attacks on their IT systems. The most widespread types of attacks include:

- Malicious/unauthorized modifications to ICT programs and configurations (31.7% of responses), largely driven by the widespread presence of malware and ransomware in Italy.
- DoS/DDoS attacks (20.7%), which overload ICT systems connected to the Internet. These attacks were frequently used in the context of cyber warfare, particularly by hacker groups aligned with Russia.
- Unauthorized and malicious use of ICT systems (18.3%).
- Attacks on the computerized supply chain (15%). This data highlights its prevalence and criticality, aligning with the World Economic Forum's classification of this as a major global risk.
- Theft of mobile devices (13.4%), mainly smartphones. These devices often store valuable digital identity information, such as passwords and access methods, without sufficient protection, making

them attractive targets. Additionally, smartphones have significant value on the second-hand market, providing further incentive for theft.

All other types of attacks listed in the OAD taxonomy recorded percentages below 10%. For the first time in OAD 2024, access control systems and network attacks are no longer at the top of the ranking for the most widespread types of attacks, as they were in previous editions.

The most widespread cyber attack's techniques in the most serious attacks see at the top:

- The use of multiple techniques in a single attack, reported by 40.4% of respondents.
- Illegal information gathering, often achieved through social engineering, at 37.6%.
- Malicious code, a core component of the widespread ransomware attacks, at 25.3%.

The correlation of data on detected attacks with the size of the company (as number of employees) confirms that in 2023, the largest and wealthiest organizations were the primary targets of the most frequent and sophisticated digital attacks. Small and very small organizations, whether private or public, are generally not of specific interest to cybercriminals in targeted attacks. However, they can still become victims of mass attacks, such as those based on phishing and ransomware.

The 2024 "vertical" survey on attacks targeting web applications (outlined in §4.2) was based on analyzing the causes of the most severe attacks, focusing on the main vulnerabilities and risks identified by OWASP. Given that most applications are web-based, and many are hosted in the cloud, modern IT system, regardless of their size, tend to be partially on-premise and partially on one or more clouds from different providers (multi-cloud). This prompted a deeper investigation into the technical causes of attacks experienced by the survey's responding companies. From this data, 58.4% of respondents reported detecting attacks on web applications and environments, and of these, 60.6% suffered attacks within their cloud environments—despite the expectation that cloud environments are generally more secure than on-premise systems. The vulnerabilities that caused the most severe attacks were attributed 92.3% of the time to human factors, which also partially reflect organizational shortcomings (such as inadequate user training), and 82.7% to technical issues.

When referencing OWASP's top 10 web vulnerabilities, the most serious attacks identified by respondents were primarily caused by outdated and vulnerable software components, ranking first at 31.7%. This was followed by misconfiguration of security tools at 20.4%.

The OAD 2024 questionnaire also addressed the 10 main risks related to API interfaces in web environments as identified by OWASP. Around 50% of the respondents stated that the most serious attack they experienced was not caused by any of the OWASP top ten web API risks. Among the remaining respondents, API security misconfiguration emerged as the leading cause, aligning with the findings on web vulnerabilities.

The impact of the most serious attack on web environments was severe for the IT systems of the respondents. In 85.3% of cases, the attack resulted in a disruption lasting two days or more. Economically, the impact was also significant, with 86.5% reporting increased costs to their IT system budget, and 24% noting that these costs extended to affect the broader budget of the company.

Regarding the motivations behind the most serious attacks, nearly two-thirds of respondents cited economic reasons, such as fraud and blackmail. Notably, for the first time in OAD's history, cyber warfare ranked third among attack motivations, reported by 20.2% of respondents.

The 2024 "vertical" survey on attacks targeting OT (Operational Technology) systems, detailed in §4.3, included only those respondents that reported using OT systems, accounting for 37% of the total. Among these, 48.2% confirmed experiencing attacks on their OT systems.

The impact of the most serious OT attack was significant, particularly in terms of system downtime. For approximately one-third of respondents, the system was blocked for 2 to 3 days, while for nearly half, the downtime exceeded 3 days. Given that most modern OT systems are interconnected with the centralized applications of the IT system, these disruptions extended to some IT systems as well. As a result, 40.7% of

respondents reported that centralized IT applications were also blocked for 2 to 3 days due to this cross-system impact.

The findings of the OAD 2024 survey are largely consistent with those reported by key organizations such as the World Economic Forum, ENISA (European Union Agency for Cybersecurity), ACN (National Cybersecurity Agency), and the Italian Postal Police. The latter contributed data on cybercrime detected during 2023 and the first half of 2024, which are detailed in Chapter 8 of this Report.

To provide a clearer understanding and context for the findings on digital attacks, OAD conducts an extensive analysis of the responding companies. This includes the type of company (§6.1), the nature and importance of their IT systems for their operations or business (§6.2), and the cybersecurity measures they have implemented. The pool of respondents encompasses a wide range of sectors, including Public Administrations. The most represented sectors are:

- Education, with 23.6% of respondents,
- Professional and business support services (including lawyers, accountants, notaries, etc.), accounting for 12.3%,
- Manufacturing and construction industry, which makes up 11% of the total respondents.

In terms of company size, based on the number of employees, 69.8% of the respondent companies are small and medium-sized organizations, defined as those with fewer than 250 employees. Notably, 22.9% of the respondents are organizations with fewer than 10 employees, reflecting the structure of the Italian economy, where such small businesses make up the vast majority of companies.

For 70.1% of the responding companies, the IT system plays a crucial role in supporting their activities and processes, underscoring the need for robust, effective, and efficient digital security. Additionally, 10.6% of the respondents provide essential services for Italy, making them subject to the NIS Directive and soon to new European regulations such as NIS2 and DORA.
Among the respondents, 85.4% manage and control their IT systems entirely within Italy, with 63.4% having small-to-medium-sized systems without a dedicated Data Center. A vast majority, 92%, rely on outsourced ICT services, particularly in the cloud.
Regarding operational management, 24.4% of respondents handle it entirely in-house, while 38.6% fully outsource it and 37.1% partially outsource certain aspects. When it comes to the management of digital security, 20% of respondents manage it internally, but 80% outsource it—41.6% completely. This high percentage of fully outsourced digital security management is significant, as smaller organizations typically lack the resources to manage security independently and must turn to consultants or specialized companies for support.

In the OAD 2024 questionnaire, the questions regarding the measures for cybersecurity were optional, and 35.4% of respondents provided answers. The data, detailed in Chapter 7, indicates that most respondents show good levels of both technical and organizational cybersecurity. This positive outcome likely reflects the higher participation of companies with more robust security systems, as those with weaker security measures may have been less inclined to respond.
However, some security deficiencies were more prevalent, particularly among smaller organizations, especially in organizational aspects. Many of these smaller entities also rely on outsourced services for managing their digital security.

While the majority of responding companies are positioned within the higher range for digital security measures, they still experienced numerous digital attacks. These attacks resulted in significant disruptions and incurred substantial costs for their IT systems and, in many cases, for the entire economic budget.

In summary, throughout 2023, serious digital attacks and significant cyber risks continued to spread globally, across Europe, and in Italy.

In Italy, we have been in the era of *systemic digital insecurity* since 2020, and this reality affects the entire world. Despite the implementation of security measures—often at substantial cost—these defenses have not been sufficient to stop digital attacks. With the current available measures, which must be strengthened rather than abandoned, **companies need to learn to manage this insecurity through resilience strategies**.

On the business side, resilience can be ensured through *business continuity*—the ability to maintain the operation of critical processes. On the IT side, resilience requires an effective, actionable, and thoroughly tested *Disaster Recovery* plan. These are essential tools to navigate the persistent insecurity and maintain functionality in the face of digital threats.

2. L'indagine OAD

OAD, Osservatorio Attacchi Digitali in Italia, è l'unica indagine on line via web in Italia sugli attacchi digitali intenzionali ai sistemi informativi di aziende ed enti operanti in Italia, e sulle misure di sicurezza tecniche ed organizzative in essi presenti. L'indagine è rivolta liberamente e in maniera anonima ad aziende/enti di ogni settore merceologico, incluse le Pubbliche Amministrazioni Centrali e Locali, e di ogni dimensione (come numero di dipendenti e fatturato/giro d'affari). Essendo totalmente libero l'accesso ai questionari online su Internet, il campione emerso non ha stretta valenza statistica ma, dato il numero di risposte e la buona distribuzione per dimensioni e per settore merceologico delle aziende/enti 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 §3.7.1) e che difficilmente sono considerate nelle altre indagini nazionali ed internazionali.

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

Un quadro contestualizzato nella realtà europea e mondiale, con riferimenti ai rapporti del World Economic Forum e delle Agenzie per la sicurezza digitale, quella europea ENISA e quella italiana ACN.
L'approccio adottato per tutte le indagini OAD consiste nel coinvolgere liberamente e in modo rigorosamente anonimo il maggior numero possibile di rispondenti al questionario online, comprendendo aziende ed enti di ogni settore e dimensione. La diffusione del questionario avviene tramite tutti i canali mediatici di AIPSI, con il supporto delle associazioni patrocinanti. Questo metodo non prevede la definizione di un campione fisso anno dopo anno, ma al termine della raccolta emerge un insieme eterogeneo di rispondenti, provenienti da diversi settori, incluse le Pubbliche Amministrazioni, e di varie dimensioni in termini di numero di dipendenti.

2.1 L'indagine OAD 2024

OAD 2024 arriva al **17° anno** consecutivo di indagini online via web, ed è focalizzato sugli **attacchi subiti nel 2023** per i **siti e gli ambienti web** e per gli **ambienti OT, Operational Technology**, dei sistemi informativi delle aziende/enti rispondenti. Erano presenti nel questionario online due domande sulle altre tipologie di attacco rilevate nel 2023, per poter continuare l'analisi dei trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 al 2023.

Per semplificare il questionario e ridurre il tempo di compilazione, mantenendo comunque rilevanti i contenuti per l'analisi degli attacchi informatici e garantendo continuità con le informazioni raccolte nelle

precedenti indagini, è stata resa opzionale la sezione relativa alle misure di sicurezza adottate. Tuttavia, la compilazione di questa parte è stata consigliata per permettere, al termine del questionario, di ottenere una **macro valutazione** automatica e anonima del **livello di sicurezza del SI** oggetto delle risposte.

Il questionario OAD 2024 è rimasto online da fine aprile 2024 a fine agosto 2024: le/i rispondenti sono stati complessivamente **345**, un numero leggermente maggiore ma dello stesso ordine di grandezza delle indagini OAD degli anni precedenti: questo nonostante la forte semplificazione del questionario ed il coinvolgimento di importanti associazioni patrocinanti, elencate nell'Allegato D di questo rapporto.

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

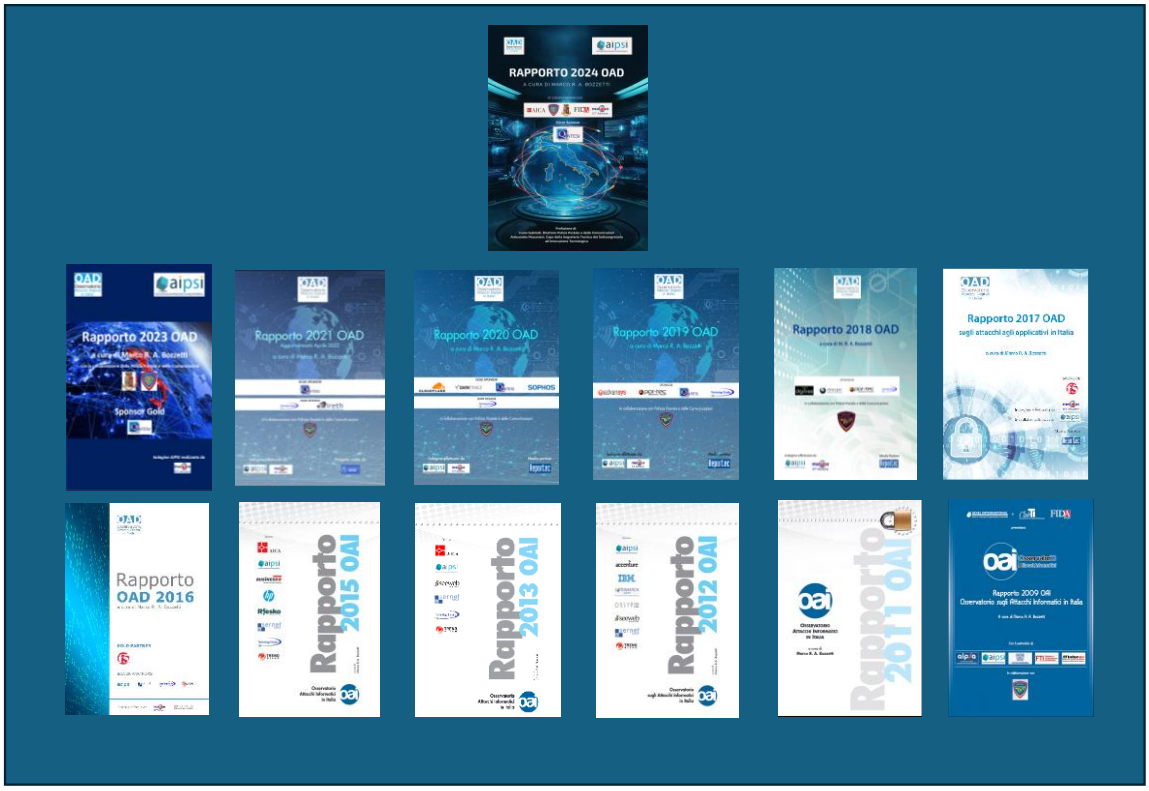


Fig. 2.1-1

OAD 2024 annovera il **patrocinio gratuito** di numerose associazioni, il cui elenco, con una breve descrizione delle loro attività, è nell'Allegato D. Per OAD il ruolo attivo dei Patrocinatori è significativo per poter allargare e stimolare il potenziale bacino dei compilatori del questionario via web, tipicamente tramite i loro soci e simpatizzanti. Inoltre, il loro supporto è prezioso per promuovere e diffondere il rapporto finale.

Il presente Rapporto OAD 2024, 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 si propone né potrebbe essere un manuale 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 è richiesta una conoscenza di base di informatica e di sicurezza digitale, e per facilitarne la lettura, è disponibile nell'Allegato B un glossario degli acronimi e dei termini tecnici specialistici usati.

3. Il quadro generale degli attacchi digitali intenzionali

L'indagine OAD fa riferimento al solo contesto italiano, ma per comprendere appieno il fenomeno degli attacchi digitali è bene inserirlo in un quadro più ampio, considerando le dinamiche a livello europeo e mondiale.
L'arco temporale di riferimento di OAD 2024 è **l'intero anno 2023** durante il quale vari elementi hanno dominato e caratterizzato gli aspetti di sicurezza digitale:

- le **crescenti tensioni geopolitiche** tra l'occidente democratico e liberale ed altri stati che non lo sono, con due principali guerre in corso e che aggravano tali tensioni:
  - la guerra in Ucraina causata dall'invasione dell'Ucraina da parte della Federazione Russa a febbraio 2022, ma con un conflitto tra le due nazioni già iniziato nel 2014 con l'invasione della Crimea;
  - la guerra di Gaza, causata dall'attacco terroristico del 7 ottobre 2023 ad Israele da parte di Hamas, organizzazione palestinese islamista fondamentalista, dalla reazione israeliana e dell'estensione del conflitto con l'altro gruppo terroristico Hezbollah;
- i **rischi digitali per le elezioni europee del 2024**, con forti timori di **disinformazione e fake news**, capaci di influenzare l'orientamento politico ed il voto nell'intera area dell'Unione Europea (UE);
- la **diffusione di tecnologie emergenti**, in primis quelle relative all'**intelligenza artificiale**, che pur offrendo significative innovazioni, da un lato introducono nuove vulnerabilità e rischi a chi le utilizza, dall'altro sono alla base di nuove tecniche di attacco.

A questi specifici fattori si devono aggiungere quelli "tradizionali", ossia attacchi digitali per ottenere illegali ricavi economici, dalle frodi finanziarie ai furti sui conti corretti bancarie, dai ricatti con ransomware, alla saturazione delle risorse dei sistemi informativi (DoS/DDoS), dai furti di informazioni e di identità digitali al furto "fisico" di dispositivi ICT, quali ad esempio i più avanzati smartphone che hanno un significativo mercato dell'usato.
Gli **attori** più critici degli attacchi digitali includono strutture a livello di stato ed organizzazioni criminali ben organizzate, dotate di elevate capacità tecniche ed economiche, che operano sia per le strutture statali, di fatto in logica di guerra informatica (cyber warfare)[5], sia autonomamente per i loro obiettivi criminali, che sono quasi sempre di tipo economico.

Come approfondito nel Capitolo 4, dal 2020 si è entrati di fatto nell'**era della insicurezza digitale sistemica** (**systemic cyber insecurity**), ed anche il 2023 ha confermato questo epocale cambiamento, nel corso del quale le contromisure adottate, pur numerose e costose, non si sono rilevate efficaci. Un importante fattore di questo cambiamento è dato dalla **crescente gravità degli attacchi**, soprattutto in termini di impatti sul business e sulle attività dell'attaccato.

A livello mondiale Il Global Risk Report[6] 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**: a breve termine è al quarto posto (era all'ottava nell'edizione precedente) ed a lungo termine, rimane all'ottavo posto, come nella precedente edizione (si veda fig. 3-1).

[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*".
[6] https://www.weforum.org/reports/global-risks-report-2023/

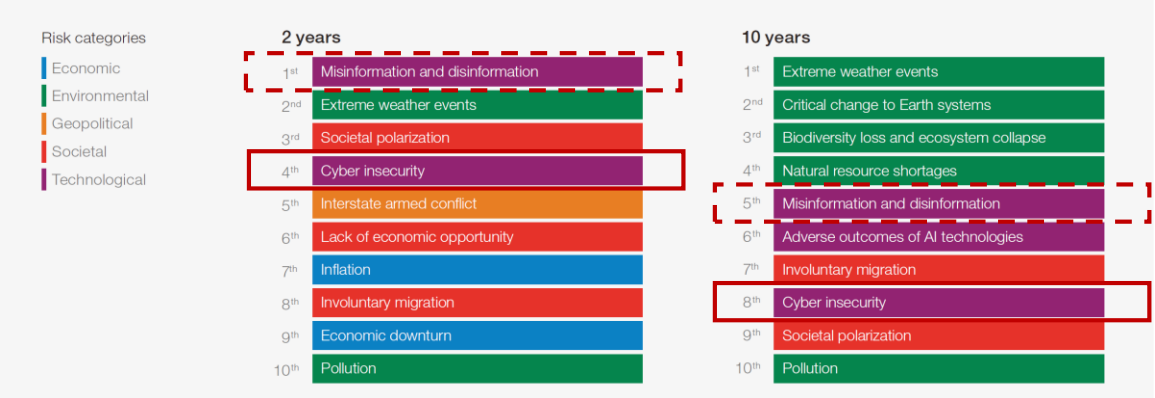


Fig. 3-1 (Fonte: World Economic Forum Global Risks Perception Survey 2023-2024)

Questa figura evidenzia che al primo posto, nel breve termine, si colloca la "**misinformation and disinformation**", due termini che sono spesso considerati sinonimi, ma che hanno significati diversi:

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

Misinformation e disinformation nel lungo termine scendono al quinto posto in ordine di criticità. Ma rimangono un grave pericolo, soprattutto nell'ambito delle guerre sempre più ibride[7], delle tensioni geopolitiche, delle votazioni. E come mostrato nella fig. 3-2, essi hanno legami con la sicurezza digitale e con gli altri rischi individuati da WEF; e sono il rischio digitale a più alta influenza (le dimensione del cerchio nella figura).

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

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

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

Si noti come nel lungo termine, al sesto posto nel rapporto WEF, si collocano i rischi di **un cattivo ed improprio uso e gestione** dell'**Intelligenza artificiale**.

[7] 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).

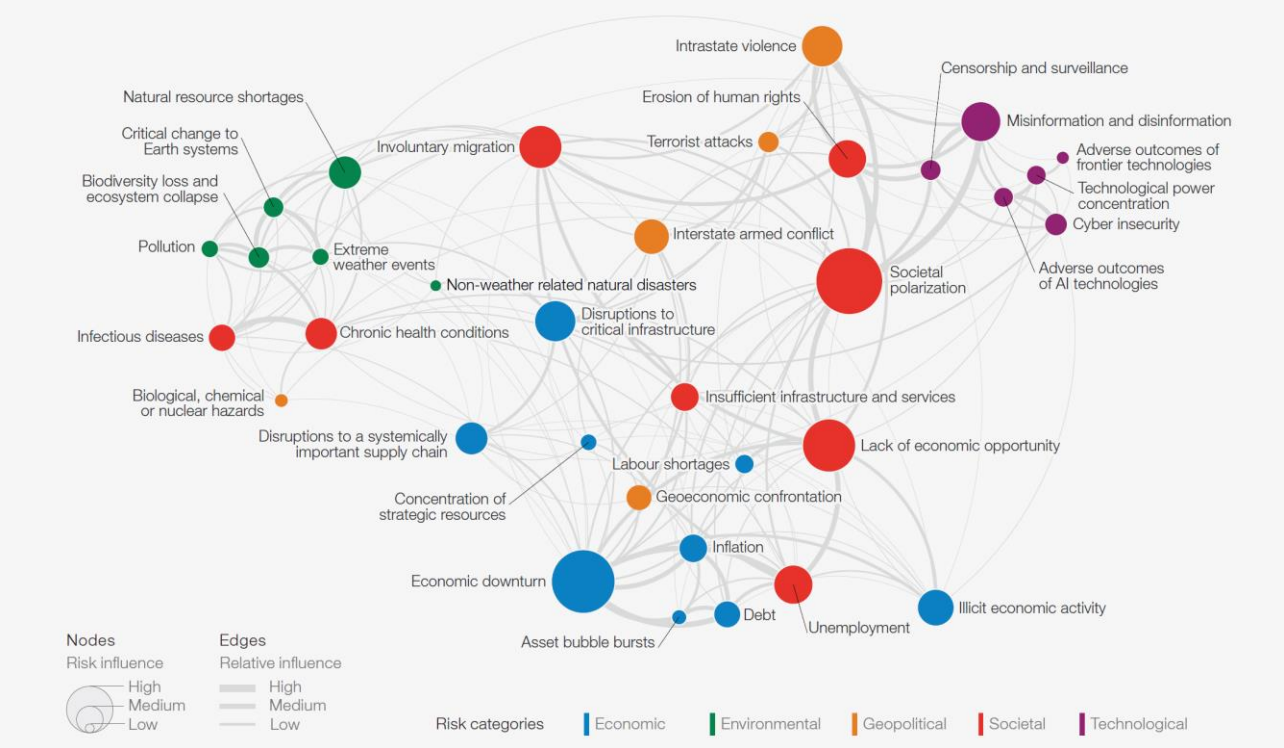


Fig. 3-2 (Fonte: World Economic Forum Global Risks Perception Survey 2023-2024)

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

3.1 Il quadro a livello europeo

A livello europeo, per gli attacchi e la sicurezza digitale, 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) 2023*", l'"*ENISA Threat Landscape (ETL) 2024*" ed il "*Foresight Cybersecurity Threats for 2030 – UPDATE*", aggiornato e pubblicato a marzo 2024.

Quest'ultimo rapporto ripropone i 21 principali rischi elencati nella tabella di fig. 3.1-1, già identificati nelle edizioni precedenti. Tuttavia, per molti di essi è cambiato il posizionamento, in termini di gravità e possibile diffusione. Si lascia al lettore l'approfondimento dal rapporto, ma è bene evidenziare come:

- al primo posto, come rischio più grave entro il 2030, rimane **l'attacco ai sistemi informativi nella supply chain con clienti e fornitori**;
- il problema della **mancanza di competenze ICT** è al secondo posto, molto critico non solo per l'Italia;

- l'impatto dei **forti cambiamenti atmosferici** che possono **impattare sull'erogazione dell'energia elettrica**, bloccando anche per tempi significativi la connettività ad Internet ed in certi casi distruggendo gli stessi Data Center che erogano servizi ICT, ad esempio con inondazioni e frane.

Il rapporto dettaglia i 21 rischi indicando i probabili attaccanti, le probabili tecniche di attacco, i probabili impatti, e gli scenari più rilevanti per attuarli.
E opportuno considerare che quasi tutte queste 21 minacce sono già attuali, e utilizzate in molti attacchi.
Le minacce di oggi continueranno a essere rilevanti anche in futuro, ma evolveranno grazie a nuove tecnologie, in particolare l'intelligenza artificiale, diventando più interconnesse e dipendenti tra loro.

Fig. 3.1-1 (Fonte: Enisa)

Nei Rapporti ETL 2023 e 2024, ENISA, con riferimento ai 21 più gravi rischi di cui sopra, riporta quanto rilevato da lei e dalle varie agenzie per la cybersicurezza dei paesi UE.
OAD 2024 considera entrambi i rapporti ETL in quanto il primo fa riferimento al periodo luglio 2022 – giugno 2023, il secondo a luglio 2023 – giugno 2024: l'intero anno 2023 è a cavallo tra i due rapporti.

I **principali trend sugli attacchi digitali** del rapporto ETL 2024 sono riassunti nei seguenti punti.

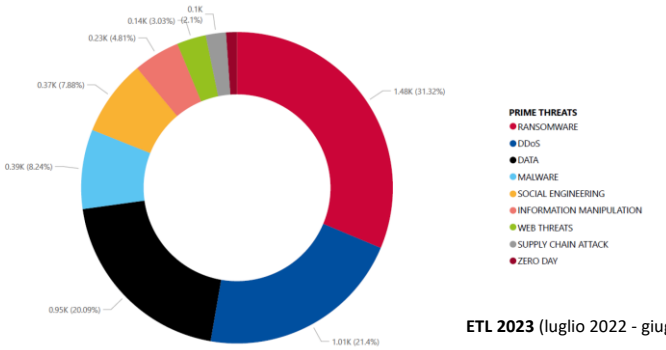
- Le minacce alla disponibilità dei sistemi ICT (DoS/DDoS) e il **ransomware** si sono classificate al primo posto come diffusione nell'UE anche per il 2023-2024.
  - Le interruzioni di Internet sono ai massimi storici, a causa della crescente dipendenza delle attività umane e della società da Internet, soprattutto nell'era post-Covid.
  - Gli attacchi DDoS stanno diventando più grandi e complessi, si stanno spostando verso reti mobili e IoT e vengono sovente utilizzati nelle guerre digitali e nei conflitti ibridi.
- Anche per ENISA il riferimento per le vulnerabilità è il data base CVE della Mitre e l'NVD gestito da NIST e FIRST (si veda §3.4.1).
- Gli attaccanti più capaci utilizzano strumenti legittimi per eludere il rilevamento dell'attacco il più a lungo possibile e per oscurare le loro attività utilizzando software ampiamente disponibili nella maggior parte dei sistemi, così da rendere più difficile la loro identificazione. In particolare:
  - Living Off Trusted Sites (LOTS): gli autori delle minacce hanno esteso le loro tecniche furtive nel cloud, utilizzando siti attendibili e servizi legittimi per evitare il rilevamento e mascherare

le comunicazioni di comando e controllo come traffico ordinario o messaggi innocui su piattaforme come Slack[8] e Telegram[9].
    - Progressi nelle tecniche di evasione difensiva: i gruppi di criminalità informatica, in particolare gli operatori di ransomware, hanno eluso il rilevamento utilizzando tecniche Living Off The Land (LOTL) per mimetizzarsi negli ambienti e mascherare le loro attività dannose.
- Si è registrato un forte aumento negli incidenti di compromissione della posta elettronica aziendale (BEC). Il phishing è il vettore più comune per l'accesso iniziale. Ma sta emergendo anche un nuovo modello di ingegneria sociale, un approccio che consiste nell'ingannare le vittime nel mondo fisico.
- Gli infostealer[10] continuano a essere ampiamente utilizzati dagli autori delle minacce, soprattutto grazie ai downloader, e sono ora componenti essenziali nelle catene di attacco digitale.
- Le offerte Malware-as-a-Service (MaaS) hanno continuato a essere una minaccia significativa e in rapida evoluzione, in particolare da metà del 2023.
- Le piattaforme di virtualizzazione sono diventate fondamentali e diffuse per i SI sia on premise che su cloud, ma possono soffrire di configurazioni errate e di specifiche vulnerabilità. I sistemi virtualizzati terziarizzati sono obiettivi primari per i criminali informatici, in particolare per le bande di ransomware. Il tipico attacco si articola nelle seguenti fasi: si ottiene l'accesso iniziale tramite ingegneria sociale, tipicamente con spear phishing, o sfruttando delle vulnerabilità individuate; una volta all'interno, eliminano o crittografano i sistemi di backup, esfiltrano i dati, lanciano il ransomware e sovente lo diffondono oltre l'ambiente virtuale.
- Cresce la diffusione di strumenti di intelligenza artificiale (IA) per i criminali informatici: gli autori dgli attacchi hanno utilizzato strumenti come FraudGPT e modelli di linguaggio di grandi dimensioni per co-creare e-mail di phishing e generare script PowerShell dannosi, aumentando la sofisticazione degli attacchi.
- La minaccia della manipolazione delle informazioni abilitata dall'IA è stata osservata, ma ancora su una scala limitata, seppur in evoluzione. Ad esempio, alcuni attori della minaccia stanno sperimentando l'IA per la manipolazione delle informazioni apparentemente per valutare come l'IA può essere sfruttata in questo contesto.
- È stata osservata una recente ondata di trojan bancari mobili, con un concomitante aumento della complessità dei loro vettori di attacco.
- Stanno emergendo compromissioni della supply chain attraverso tecniche di ingegneria sociale, che sfruttano vulnerabilità umane per infiltrarsi nei sistemi aziendali. Ad esempio, a marzo 2024 è stato introdotto un codice backdoor in un progetto open source XZ Utils, un set di strumenti e librerie utilizzati per la compressione dei dati[11].
- La compromissione dei dati è aumentata nel 2023-2024.
- DDoS-for-Hire consente il lancio di attacchi DDoS su larga scala da parte di utenti non qualificati.
- Le organizzazioni criminali hanno progressivamente combinato diverse tecniche di estorsione, che ormai quasi sempre includono una qualche forma di furto di dati. La doppia estorsione ha registrato un aumento significativo, con alcuni gruppi che si concentrano esclusivamente sul furto di informazioni per ricattare le vittime.
- La geopolitica continua a giocare un ruolo significativo nella sicurezza digitale (come già sottolineato, attacchi digitali anticipano, supportano e seguono scontri militari, in una logica di guerre ibride) e continua ad essere un forte motore pergli attacchi digitali.

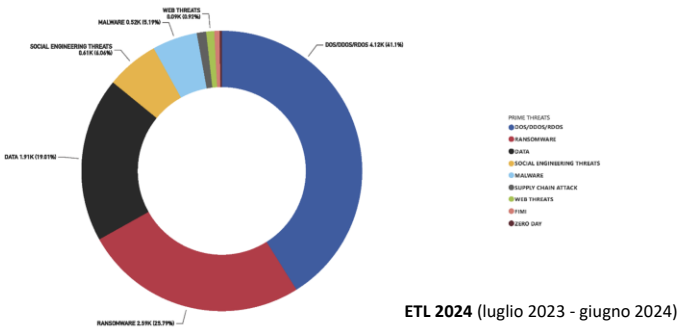
[8] Servizio di messaggistica per le aziende che collega le persone alle informazioni di cui hanno bisogno, creando e gestendo gruppi di lavoro.
[9] Servizio di messaggistica istantanea e di broadcasting criptato e gratuito.
[10] Sono dei malware progettati per carpire informazioni, tipicamente quelle di un utente mentre effettua un login.
[11] https://www.csirt.gov.it/contenuti/rilevata-backdoor-in-xz-utils-al01-240330-csirt-ita

- Gli hacktivist sovrappongono le loro attività con gli attori "State-nexus", ossia collegati e/o dipendenti da uno Stato, per il quale effettuano attacchi e crimini informatici.
- La manipolazione delle informazioni continua a essere un elemento chiave della guerra di aggressione della Russia contro l'Ucraina. La manipolazione delle informazioni è un elemento chiave della guerra di aggressione della Russia contro l'Ucraina, ed è una componente essenziale e consolidata delle strategie di sicurezza della Russia.
- Si sono avute significative operazioni congiunte a livello europeo delle forze di Polizia, come Operation Chronos[12] e Operation Endgame[13], e lo smantellamento dell'infrastruttura ICT del gruppo ransomware ucraino che ha diffuso Hive[14], Trickbot[15] ed altri malware[16].

La fig. 3.1-2 confronta le tecniche di attacco usate nel periodo 2023, considerando sia il rapporto ETL 2023 che quello 2024. Si evidenzia il crescendo degli attacchi tipo DoS/DDoS ed il ridursi degli attacchi ransomware; gli attacchi ai dati, sostanzialmente per il loro furto, si mantengono in terza posizione con circa il 20%.



ETL 2023 (luglio 2022 - giugno 2023)



ETL 2024 (luglio 2023 - giugno 2024)

Fig. 3.1-2 (fonte: ENISA ETL 2023 e 2024)

Sono circa 100 principali gruppi di attaccanti individuati a livello mondiale, responsabili di circa 2/3 degli attacchi ransomware, e tra i principali sono quelli pro Russia che effettuano soprattutto attacchi DDoS e

[12] L'Operazione Chronos è stata condotta da FBI, Europol e da agenzie di altre 10 nazioni, ed ha bloccato le piattaforme di supporto e le operazioni di LockBit, il famigerato e ben noto gruppo russo di RaaS, Ransomware as a Service.
[13] Altra importante operazione contro le botnet a livello mondiale condotta tra Europa e Statu Uniti, coordinata da Europol con le forze di polizia di vari paesi. Sono stati sequestrati più di 2000 domini e 100 server, arresto delle persone, e l'operazione non è ancora conclusa. Si veda https://www.operation-endgame.com/
[14] https://en.wikipedia.org/wiki/Hive_(ransomware)
[15] https://www.csirt.gov.it/contenuti/nuova-funzionalita-del-malware-trickbot-al01-200603-csirt-ita
[16] Europol ha messo a disposizione gratuitamente gli strumenti di decriptazione per molti ransomware: https://www.nomoreransom.org/it/decryption-tools.html

malware/ransomware. Tra i principali NoName57, LockBit 3.0, Alphv/Blackcat, Play, 8Base, BlackBasta, Malas, Akira, BianLian, Medusa, Royal.

ENISA in ETL 2024 ha creato una classifica dei principali gruppi di cybercriminali per "attivismo" nel 2023, mostrata nella fig. 3.1-3, dalla quali si evidenzia che:

- più di 1/3 degli attacchi è stato portato da attori non indentificati;
- al secondo posto si trova NoName57, un gruppo filo Russo che opera prevalentemente con DDoS ed ha attaccato, ed attacca, siti ucraini, europei e statunitensi;
- al terzo posto, ma con una percentuale molto inferiore, C10p, chiamato anche Clop, un gruppo criminale filo e di lingua russa, noto per gli attacchi basati su malware e su "multilevel extortion" con i ransomware (ricatta più volte l'attaccato, prima per eliminare il ransomware e far funzionare il sistema infetto, poi per non vendere i dati estratti illegalmente, e così via);
- al quarto posto rimane ancora LockBit, non totalmente eliminato dalla operazione Chronos e che in qualche moto sta "risorgendo dalle ceneri".

Tutti gli altri gruppi di attaccanti hanno percentuali sotto il 3%, ma non per questo sono da considerarsi meno pericolosi.

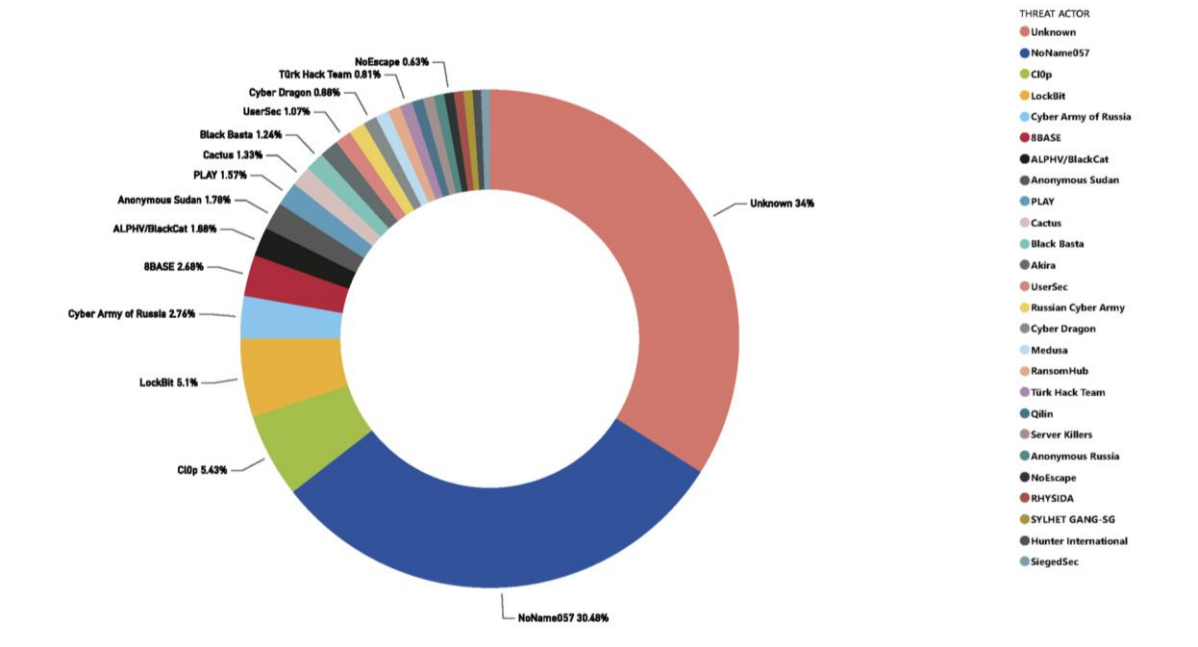


Fig. 3.1-3 (fonte: ENISA ETL 2024)

3.2 I principali attacchi digitali a livello mondiale nel 2023

Attacchi digitali per frodi e "tradizionale" criminalità informatica, e in parallelo gli attacchi di hactivist e quelli di cyber warfare 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 individuare gli attacchi digitali a livello mondiale elencati nel prossimo paragrafo §3.2.1, l'autore ha fatto soprattutto riferimento al FIRST[17], ai rapporti di ENISA, alla statunitense CISA[18], al CSIS[19], allo CSIRT Italia, oltre che ad alcuni dei più autorevoli rapporti di enti ed industrie ICT e del settore della sicurezza digitale.

Le minacce non intenzionali (in inglese i "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 sostituiti da personale non sufficientemente preparato, dalla difficoltà di cooperare efficacemente da remoto, e così via. Questi incidenti **non sono considerati nell'indagine OAD**, ma **ENISA ha rilevato la loro cresciuta diffusione**, che costituisce una **ulteriore significativa minaccia ai SI**.

Gran parte degli **attacchi intenzionali**, soprattutto quelli effettuati dall'esterno dell'azienda/ente, **utilizzano il phishing e lo spear phishing** come **vettore iniziale dell'attacco**, e sfruttano le **vulnerabilità personali** degli utenti, in particolare di quelli privilegiati: queste email malevole contengono come allegati malware, e sovente ransomware, con file di tipo ISO[20] e .LNK[21]; 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 dell'identità digitale** e di **snoofing**. Molti degli attacchi, non solo di malware, sfruttano le **backdoor lasciate aperte** nei programmi in produzione, ossia in funzione nel SI.
La maggior parte delle tecniche di attacco usate nel 2023 non sono nuove, così come negli ultimi due-tre anni, ma 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 SI hanno dismesso gli strumenti di contrasto (o tali "obsoleti" strumenti non sono più in grado di contrastarli). La maggior parte degli attacchi digitali di una certa complessità, 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 alle varie risorse ICT presenti per comprometterle, fino ad **arrivare al sistema obiettivo** (target), o per individuare risorse ICT più interessanti e vulnerabili da attaccare.

Mentre si stanno scrivendo queste note, un bug nell'aggiornamento di un programma di sicurezza CrowdStrike usato da Microsoft ha bloccato milioni di server e PC con sistema operativo Windows nel mondo, ed anche in Italia, incluse la maggior parte delle infrastrutture critiche soggette in Europa alla normativa NIS (ed a breve alla NIS2). E' un dato molto preoccupante che un aggiornamento software, se errato, comunque blocchi dei sistemi ICT che sono dotati, o dovrebbero esserlo, di elevate misure di sicurezza tecniche ed organizzative, e di ripristino dopo un incidente.

3.2.1 Esempi di significativi di attacchi a livello mondiale nel 2023

L'elenco non ha alcuna pretesa di essere esaustivo: il criterio di scelta è stato quello di mostrare diversi tipi di attacchi digitali portati ad aziende/enti di diversi settori merceologici, PA incluse.

[17] FIRST, Forum of Incident Response and Security Teams (https://www.first.org/)
[18] CISA, Cybersecurity Infrastructure Security Agency (https://www.cisa.gov/), è l'Agenzia statunitense per la sicurezza informatica e delle infrastrutture.
[19] CSIS , Center for Strategic and International Studies, è un'autorevole 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.
[20] File ISO: 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.
[21] 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.

- **Gennaio 2023**
  - T-Mobile annuncia un "data breach", che ha interessato 37 milioni di clienti a dati personali quali il nome completo, informazioni di contatto inclusi i numeri di telefono, PIN dell'account T-Mobile, numero di previdenza sociale, documento d'identità governativo, data di nascita, codici interni che T-Mobile utilizza per gestire gli account dei clienti.
  - Attacco ransomware al Royal Mail, il servizio postale del Regno Unito, dal gruppo LockBit, che ha causato un'interruzione temporanea delle consegne internazionali. Royal Mail ha rifiutato di pagare la richiesta di 65,7 milioni di sterline per la restituzione dei dati rubati, ma ha subito ingenti costi a seguito dell'attacco, tra cui ingenti perdite di fatturato, e forse 10 milioni di sterline per la rimozione del ransomware.
- **Febbraio 2023**
  - Il fornitore di televisione satellitare Dish Network ha subito un'esfiltrazione di dati e per questo ha chiuso le sue comunicazioni interne, i suoi siti Internet ed i call center dei clienti e i conseguenza. Dish non ha fornito dettagli sull'attacco
  - La città di Oakland, California, ha dichiarato lo stato di emergenza a seguito di un attacco ransomware, con il furto di dati sensibili, comprese informazioni sui dipendenti in ruoli sensibili come la polizia. L'incidente ha bloccato molti servizi non di emergenza, mentre gli edifici governativi sono stati costretti a chiudere temporaneamente.
- **Marzo 2023**
  - Cybercriminali hanno compromesso l'applicazione desktop di 3CX e l'hanno poi utilizzata per lanciare attacchi alla supply chain. 3CX fornisce software per Voice over IPil furto di 14 milioni di record, (VoIP) utilizzato da oltre 600.000 aziende in tutto il mondo. Tra i clienti dell'azienda ci sono American Express, BMW e Coca-Cola.
  - Latitude Financial, società di Melbourne, che fornisce prestiti personali e carte di credito a persone in Australia e Nuova Zelanda, ha subito un furto di 16 milioni di record, che includono contratti finanziari, patenti di guida e passaporti.
- **Aprile 2023**
  - T-Mobile ha subito un secondo data breach, dopo quello di gennaio, che ha convolto i dati di 836 clienti.
  - Shields Health Care Group, un provider di servizi medici del Massachusetts, ha subito un furto di dati personali e sensibili di 2,3 milioni di persone.
- **Maggio 2023**
  - Attacco di hacker filo russi al sistema di telecomunicazioni ucraine Kyivstar.
  - Hacker cinesi hanno intercettato gli account di posta elettronica di oltre due dozzine di organizzazioni statunitensi, tra cui i Dipartimenti di Stato e Commercio.
  - Diverse agenzie governative statunitensi sono state colpite dallo stesso gruppo ransomware russo Cl0p che ha sfruttato il sistema di trasferimento di file MoveIT. Il Dipartimento dell'Energia degli Stati Uniti ha confermato di essere tra quelli colpiti. L'attacco è avvenuto sulla scia di attacchi che Cl0p ha avviato contro le reti informatiche degli stati dell'Illinois e del Minnesota, la British Broadcasting Company (BBC), British Airways, la provincia canadese della Nuova Scozia, Shell Oil, una catena di vendita al dettaglio nel Regno Unito e la farmacia Walgreen's,
  - Microsoft ha subito un attacco di cyber-spionaggio che ha consentito al gruppo Storm-0558 di ottenere l'accesso agli account di posta elettronica dei clienti dal 15 maggio 2023. Tra questi c'erano dipendenti dei Dipartimenti di Stato e Commercio degli Stati Uniti e di altre agenzie governative statunitensi. Per lanciare la campagna, gli aggressori hanno compromesso l'account aziendale di un ingegnere Microsoft.
- **Agosto 2023**

- Cloudflare ha trovato la vulnerabilità "HTTP/2 Rapid Reset" nell'agosto 2023, sviluppata al momento da ignoti e che sfrutta il protocollo HTTP/2 standard, essenziale per il funzionamento di Internet e della maggior parte dei siti Web. Quando Cloudflare ha subito un attacco Rapid Reset, l'azienda ha adottato una mentalità "assume-breach", collaborando con i partner del settore per trovare il modo migliore per mitigare l'attacco. Al culmine della campagna DDoS Rapid Reset, Cloudflare ha registrato e gestito oltre 201 milioni di richieste al secondo e la mitigazione di migliaia di attacchi aggiuntivi che sono seguiti. Questo attacco è probabilmente il più ampio mai portato ad Internet.
- Attacco alla supply chain informatica di Dollar Tree che gestisce circa 16.000 punti vendita omonimi e Family Dollar in Nord America. L'attacco ha compromesso le informazioni personali di circa 2 milioni di persone, ed è iniziato da un attacco al fornitore di servizi di terze parti Zeroed-In Technologies.
- La Commissione elettorale del Regno Unito ha rivelato di essere stata vittima di un "complesso attacco informatico" che ha esposto i dati personali di chiunque nel Regno Unito si fosse registrato per votare.

- **Settembre 2023**
  - Johnson Controls, un fornitore di tecnologia specializzato in edifici e spazi "smart", ha subito un attacco ransomware dal gruppo di hacker Dark Angles, che hanno rubato circa 27 terabyte di dati e crittografato i server ESXi. Gli haxker hanno richiesto 51 milioni di dollari per fornire un decryptor e cancellare i dati rubati, che probabilmente includevano dati sensibili del Department of Homeland Security (DHS) ed informazioni di sicurezza su contratti di terze parti insieme a planimetrie fisiche di alcune strutture di DHS.
  - Attacco a MGM Resorts con il furto di dati personali di circa 10,6 milioni di clienti.
- **Ottobre 2023**
  - Comcast, un provider statunitense di televisione via cavo e Internet, ha subito un attacco che ha sfruttato una vulnerabilità nel software Citrix e che ha causato la violazione di quasi 36 milioni di account Xfinity.
  - La British Library, una delle biblioteche più grandi e rinomate al mondo, è stata colpita da un attacco ransomware da parte del gruppo Rhysida che ha bloccato i servizi online e in loco e che ha messo in vendita i dati rubati degli utenti sul dark web. La biblioteca ha confermato che i dati interni delle risorse umane sono stati rubati e che sono stati hackerati e messi in vendita
- **Novembre 2023**
  - Attacco ransomware a 5 ospedali canadesi in Ontario da parte di Daixin Team, un gruppo di hacker cinesi specializzato nell'attaccare ambiti sanitari.
  - Attacco con il ransomware LockBit a Shimano, ben noto costruttore di componenti per biciclette. Presumibilmente violati 4,5 TB di dati sensibili, tra cui dati dei passaporti dei dipendenti, documenti finanziari e diagrammi riservati.
  - Attacco ransomware (probabilmente LockBit) al ramo statunitense della ICBC, The Industrial and Commercial Bank of China's, con blocco delle contrattazioni sul mercato dei titoli del Tesoro statunitense.
  - Attacco al DP World Australia, operatore portuale, che ha causato la chiusura dei terminal principali nei porti di Sydney, Melbourne, Brisbane e Fremantle ed il conseguente blocco di circa 30.000 container.

- **Dicembre 2023**

- Furto di più 1,5 miliardi di record dalla banca dati di 1,6 TB della Real Estate Wealth Network di New York, contenente informazioni sulle case acquisite o vendute di milioni di persone (tra cui celebrità e politici), con i loro dati personali.
- Furto di più di 1,5 milioni di record di clienti dalla banca dati di TuneFab, nota azienda di software per convertitori di musica digitale.
- Attacco a Kyivstar, provider ucraino di comunicazioni mobili, con blocco delle sue attività per uun certo periodo.
- Attacco ai sistemi informatici del Parlamento e ad un provider TLC dell'Albania da parte di un gruppo iraniano di hacker.

3.3 I principali attacchi digitali in Italia nel 2023

Attraverso il CSIRT Italia, ACN ha potuto monitorare l'evoluzione della minaccia, caratterizzata sempre più da eventi di tipo ransomware e DDoS , ma anche dalla diffusione di malware via e-mail e phishing, indirizzati a diverse realtà pubbliche oltre che ad aziende attive nei settori più disparati (primi fra tutti telecomunicazioni, trasporti e servizi finanziari). CSIRT opera prevalentemente con e per le "infrastrutture critiche", come definite dal NIS, ora aggiornato a NIS2.
La fig. 3.3-1, dal Rapporto ACN 2023, sintetizza i numeri delle principali attività svolte dal CSIRT Italia nel 2023.

Fig. 3.3-1 (Fonte: Rapporto ACN 2023)

Per comprendere i dati della fig. 3.3-1 e della successiva fig. 3.3-2, che confronta tali dati con quelli del precedente Rapporto ACN 2022, occorre far riferimento alle definizioni usate da ACN, e qui di seguito riportate:

- ***Asset a rischio**: sistemi o servizi esposti su Internet da soggetti italiani, rilevati dalle attività di monitoraggio proattivo e per i quali vengono inviate specifiche comunicazioni.*

- ***Case**: un avvenimento d'interesse per il CSIRT Italia, opportunamente approfondito al fine di identificare il possibile impatto e valutare la necessità di azioni di resilienza. I case possono diventare eventi cyber.*
- *Comunicazione inviata: alert, anche massivi, inviati a Pubbliche Amministrazioni e soggetti privati potenzialmente interessati da eventi cyber.*
- *Comunicazione ricevuta: e-mail ricevute dal CSIRT Italia relative a informazioni contenenti profili di natura cyber anche generiche, sottoposte a valutazione preliminare (triage) per determinare l'apertura o meno di un case.*
- *Constituency: insieme dei soggetti nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli incidenti di sicurezza informatica.*
- ***Evento cyber**: case con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, il CSIRT Italia dirama alert e/o supporta, eventualmente anche in loco, i soggetti colpiti.*
- ***Incidente**: un evento cyber con impatto su confidenzialità, integrità o disponibilità delle informazioni confermato dalla vittima.*
- *Portale di collaboration: portale riservato ai membri della constituency del CSIRT Italia; costituisce lo strumento privilegiato per favorire lo scambio di informazioni tecniche specifiche con i soggetti accreditati.*
- *Portale pubblico: sito web del CSIRT Italia accessibile all'intera comunità.*
- *Richiesta di informazioni: richiesta effettuata dal CSIRT Italia al soggetto potenzialmente impattato da un evento cyber per acquisire ulteriori elementi, ad esempio la conferma di una possibile compromissione (e la conseguente classificazione dell'evento cyber quale incidente).*
- *Segnalazione: comunicazione prevista per legge per i soggetti appartenenti al Perimetro di sicurezza nazionale cibernetica (PSNC), per gli operatori di servizi essenziali e fornitori di servizi digitali (Direttiva NIS), e per gli operatori del settore comunicazione (Decreto Telco). Le segnalazioni vengono trattate direttamente come eventi cyber.*
- *Triage: fase in cui gli operatori analizzano le segnalazioni, le comunicazioni ricevute e ogni possibile evento cyber di cui il CSIRT Italia venga a conoscenza, anche a seguito di attività di monitoraggio proattivo, al fine di identificare i potenziali impatti e classificare quindi l'informazione come evento cyber, proseguendo o meno con le ulteriori fasi di trattazione.*

In pratica sono gli "incidenti" gli attacchi digitali andati a buon fine (per gli attaccanti) rilevati da ACN, con un aumento del **140,5%** rispetto al 2022, come mostrato in fig. 3.3-2. Un numero assai significativo, dato che riguarda infrastrutture critiche a livello nazionale, che dovrebbero avere e gestire le più elevate misure di sicurezza digitale. Tale aumento differisce da quanto riportato nello stesso anno dalla Polizia Postale (si veda §8), che registra una diminuzione degli attacchi (così come l'indagine OAD 2024, si veda §4). A giudizio dell'autore, questa differenza è dovuta ai bacini numericamente diversi di chi segnala gli attacchi digitali allo CSIRT di ACN rispetto al C.N.A.I.P.I.C. della Polizia Postale e per la Sicurezza Cibernetica: il bacino di aziende/enti cui fa riferimento CSIRT è al momento più piccolo rispetto a quello del C.N.A.I.P.I.C.

		2022	2023	variazione percentuale
Gestione eventi	Segnalazioni	81	349	+330,9%
	Comunicazioni ricevute	5.974	5.444	-8,9%
	Case	2.643	2.684	+1,6%
	Eventi *cyber*	1.094	1.411	+29,0%
	Incidenti	126	303	+140,5%
	Interventi *in loco*	10	13	+30,0%
	Soggetti *target*	1.150	3.302	+187,1%
Allertamento	*Alert* e bollettini portale pubblico	410	447	+9,0%
	Alert e bollettini portale di *collaboration*	38	72	+89,5%
	Richieste di informazioni	185	205	+10,8%
Monitoraggio	*Asset* a rischio	764	3.624	+374,3%

Fig. 3.3-2 (Fonte: Rapporto ACN 2023)

Nel corso del 2023 il CSIRT Italia ha trattato 1.411 eventi *cyber* con impatto a livello nazionale, per una media di circa 117 al mese, con un picco di 169 a ottobre. Di questi, 303 sono stati classificati come incidenti, per una media di circa 25 al mese.

I vari eventi cyber trattati sono stati categorizzati da ACN come mostrato nella fig. 3.3-3.

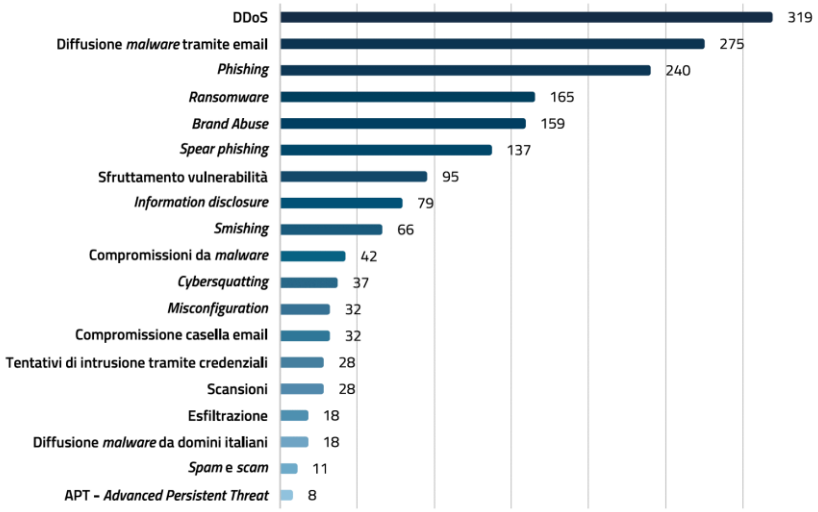


Fig. 3.3-3 (Fonte: Rapporto ACN 2023)

Si noti che:

- Smishing è il phishing effettuato tramite l'SMS, Short Message Service, degli smartphone; è una delle tecniche di ingegneria sociale per carpire l'identità digitale di persone, e/o di indurle, tramite

messaggini SMS, a scaricare involontariamente malware, condividere informazioni riservate, inviare denaro;

- Cybersquatting è l'azione di acquisto e/o registrazione di un nome di dominio web identico o simile a un dominio esistente, con l'intento illegale e truffaldino di trarre profitto illegalmente da un marchio, da un nome di azienda o da un nome di persona famosa cui il dominio fa di fatto riferimento.

Dalle indagini ACN-CSIRT, le prevalenti tecniche di attacco usate in Italia sono il ransomware ed il DoS/DDoS, e questo conferma quanto emerso dall'indagine OAD 2024 e descritto nel prossimo Capitolo 4.

La fig. 3.3-4 mostra i Gruppi hacker di ransomware individuati da ACN negli eventi cyber trattati nel 2023; la dimensione del cerchio indica l'ampiezza di diffusione in Italia negli eventi cyber considerati.

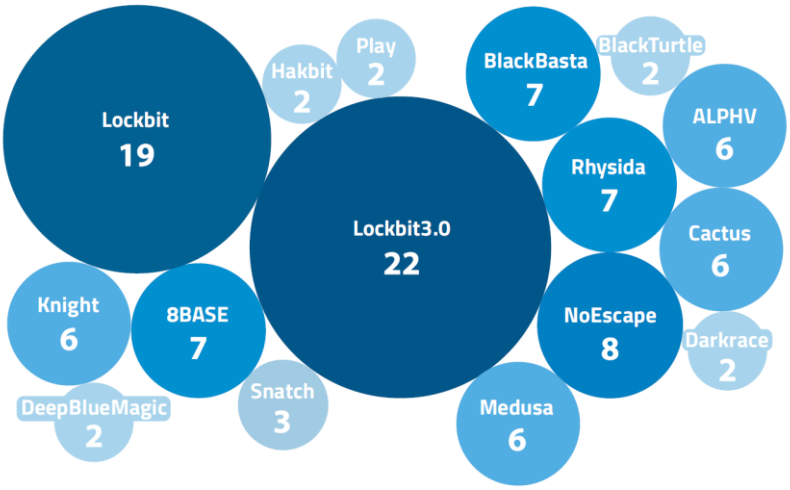


Fig. 3.3-3 (Fonte: Rapporto ACN 2023)

Nel 2023 l'Italia è risultata il terzo Paese dell'Unione europea più colpito da ransomware, mentre a livello globale è stato il sesto Paese più colpito.
Per la saturazione delle risorse ICT, tipicamente ambienti web, attaccati prevalentemente con il DDoS, Distributed Denail of Service, ACN evidenzia che essa ha avuto un significativo aumento tra gli event cyber trattati, a causa dei conflitti in corso. Come mostrato nella fig. 3.3-4, nel 2023 ACN ha rilevato 319 eventi DDoS nel 2023, con un incremento rispetto al 2022 del 625%.
Al di là dei dati sull'insieme e sulle tipologie degli attacchi digitali in Italia nel 2023, nei rapporti pochi sono i riferimenti a specifici attacchi in questo periodo, probabilmente proteggere la reputazione dell'azienda/ente attaccata/o.

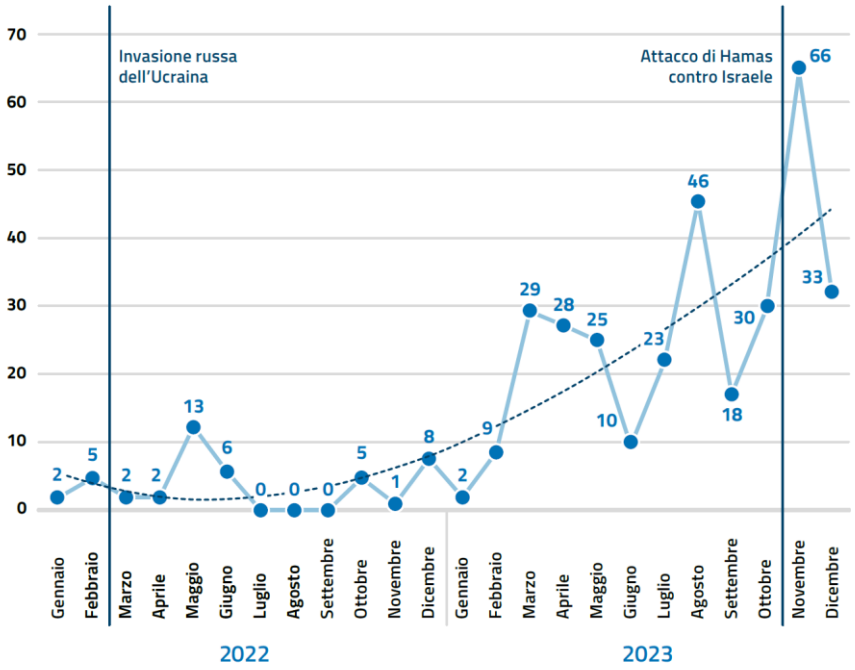


Fig. 3.3-4 (Fonte: Rapporto ACN 2023)

3.4 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 in ambito ICT è spesso involontaria e deriva da fattori come inconsapevolezza, imprudenza, imperizia o ignoranza, spesso aggravati dalla mancanza di formazione e addestramento. Queste ultime sono tipiche vulnerabilità organizzative, alle quali si aggiungono frequentemente altre carenze ed inefficienze, come l'assenza di procedure scritte e divulgate o la mancanza di controlli efficaci.

3.4.1 Le vulnerabilità tecniche

A livello tecnico esistono autorevoli ed aggiornati siti che elencano, classificandole, le vulnerabilità tecniche individuate su tutti i prodotti/sistemi/servizi ICT a livello mondiale: in particolare i più noti ed usati sono il CVE/MITRE[22] (https://cve.mitre.org/) e lo statunitense NVD, National Vulnerability Database, (https://nvd.nist.gov/) che a sua volta fa riferimento ai dati e alla numerazione CVE. Per ciascuna vulnerabilità questi siti riportano le modalità per eliminarle o ridurle, se esistono e sono state provate.

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

Alla data della scrittura del presente rapporto OAD, settembre 2024, il totale delle vulnerabilità tecniche individuate e registrate nella banca dati CVE è di **240.830**, rispetto al 212.202 di settembre 2023. L'incremento

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

delle vulnerabilità tecniche scoperte nel periodo è di 28.628, mentre tra il 2022 ed il 2023 risultava di più di 25.000.

In termini 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.

Ogni vulnerabilità tecnica di un codice software ha un diverso **livello di severità**, ossia la gravità degli impatti nel caso fosse sfruttata da attaccanti, che è stabilito da una metrica associata alle vulnerabilità registrate nella banca dati CVE, il **CVSS**, Common Vulnerability Scoring System. CVSS fornisce una metrica ed una logica per stabilire un punteggio indicatore del livello di **gravità** della vulnerabilità, basandosi sulle sue principali caratteristiche di base, su quelle che potrebbero cambiare nel tempo, sul contesto nel quale potrebbe essere sfruttata. La valutazione della severità di una vulnerabilità è importante nell'ambito dell'analisi dei rischi e per poter dare priorità ai processi di gestione delle vulnerabilità ICT. Attualmente il CVSS è alla versione 4.0 ed **è composto da tre gruppi di metriche (base, temporale e ambientale) e dalle loro possibili combinazioni.**
Per ogni vulnerabilità individuata in CVE, nella banca dati NVD del NIST è pubblicato il livello di severità di base, l'unico che non cambia nel tempo ed è comune a tutti gli ambienti d'utilizzo. Questo punteggio della severità di base, da 0 a 10, con 10 la massima gravità, fa riferimento alle caratteristiche intrinseche di una vulnerabilità nel caso fosse sfruttata, ed è fornito dal produttore della risorsa ICT per la quale è stata individuata la vulnerabilità.
Le vulnerabilità individuate e classificate in NVD con le più alte severità di base sono numerose ed arrivano al 18% circa delle vulnerabilità totali.
Per approfondimenti si veda https://nvd.nist.gov/vuln-metrics/cvss **e** https://www.first.org/cvss/ (First è l'ente che attualmente gestisce CVSS e la sua evoluzione).

3.4.2 Le vulnerabilità delle persone

Le vulnerabilità delle persone rappresentano per il mondo digitale rischi ancora più diffusi e gravi rispetto a quelle tecniche: e sono amplificate dalle vulnerabilità organizzative di cui in §3.4.3
Per le vulnerabilità personali lo strumento di contrasto più importante è la formazione continua e la consapevolezza che, nell'uso dei sistemi informatici, occorre comportarsi sempre in maniera attenta ed etica, seguendo le indicazioni che dovrebbero essere state divulgate dall'azienda/ente in termini di policy, linee guida e procedure organizzative. In Italia tale consapevolezza è ancora carente, così come lo sono le competenze specialistiche informatiche, cui si aggiunge, a livello generale, un ancor forte gender gap.
Il primo significativo indicatore sulle competenze ICT è dato dall'**indice DESI**[23] sul livello di digitalizzazione dell'economia e della società, grazie alla voce **competenze digitali** tra i 36 indicatori considerati e raggruppati nelle quattro dimensioni illustrate nella fig. 3.4.2-1.

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

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

Fig. 3.4.2-1 (Fonte: Commissione Europea)

L'ultima analisi DESI disponibile, di agosto 2024, indica che in termini di "**specialisti ICT**" l'Italia risulta quart'ultima rispetto ai 28 paesi dell'Unione Europea, e ben sotto la media europea, come evidenziato nella fig. 3.4.2-2 .
Il problema delle competenze ICT in Italia, anche solo di base, costituisce un grave "minus" per la competitività del paese, non solo in ambito europeo ma mondiale.
Le specifiche competenze per la sicurezza digitale sono ancor più ridotte, essendo un di cui delle più generali competenze avanzate nel digitale, ed **incidono profondamente sul livello di sicurezza digitale delle singoli organizzazioni e dell'intero sistema paese**.
Considerando l'enorme numero di piccole e piccolissime aziende e amministrazioni pubbliche (si veda §3.7.1), 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 (anche il singolo consulente) idoneo a fornire una soluzione adeguata alla propria realtà.

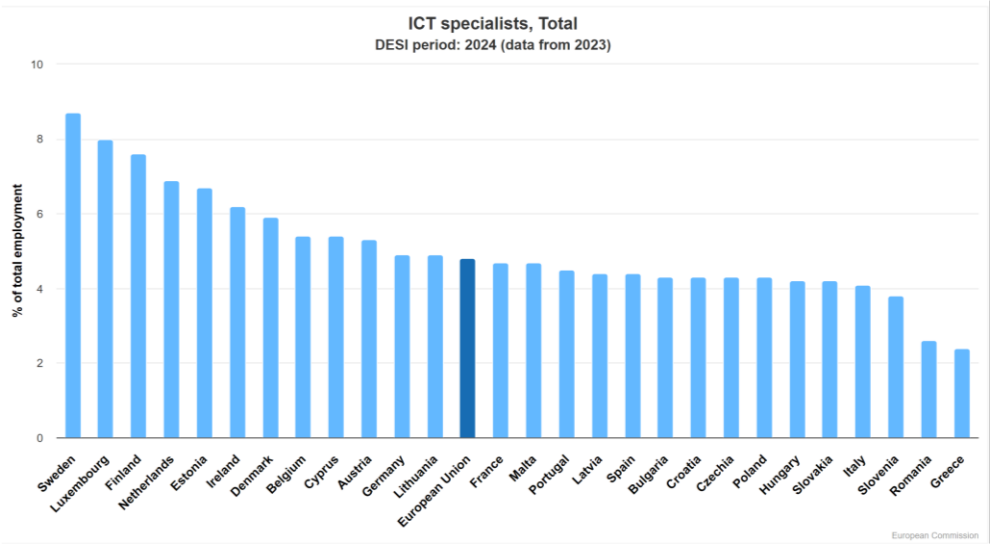


Fig. 3.4.2-2 (Fonte: Commissione Europea)

3.4.3 Le vulnerabilità organizzative

Gli aspetti organizzativi sono determinanti per l'attuazione di una reale ed effettiva sicurezza digitale, ed impattano sul personale utente del sistema informativo.
Le piccole e medie organizzazioni, ma talvolta anche quelle piuttosto grandi, difficilmente possono disporre al proprio interno delle competenze tecniche ed organizzative aggiornate per la sicurezza digitale: sarebbe opportuno che le terziarizzassero ma, al contempo, devono saperle controllare ed indirizzare rispetto al loro specifico contesto. In caso contrario dipenderanno sempre più dagli outsourcer e dagli altri fornitori esterni, in primis i consulenti, che a loro volta potrebbero avere non adeguate competenze nella sicurezza digitale: in tal senso, il cerchio delle incompetenze si chiude con possibili conseguenze molto negative per l'azienda/ente cliente.
In termini di figure e ruoli preposti alla sicurezza digitale, il responsabile è indicato con l'acronimo **CISO**, Chief Information Security Officer: questa figura negli anni passati operava prevalentemente nell'ambito della struttura dei sistemi informativi, indicata nei rapporti OAD con l'acronimo **UOSI** , Unità Organizzativa Sistemi Informativi, alle dipendenze del suo responsabile, il **CIO**, Chief Information Officer.
La tendenza è ora di porre il CISO nell'ambito di altre strutture, non in UOSI, per garantire una effettiva separazione delle responsabilità tra CIO e CISO.
Lato domanda ICT, almeno a livello di vertice, occorrerebbe possedere le competenze necessarie per "governare" a livello strategico l'evoluzione del sistema informativo in funzione delle necessità e del business dell'azienda/ente. In tale "governo" il vertice deve saper scegliere fornitori competenti e affidabili, e saperli supervisionare nella loro gestione della sicurezza digitale; essa non rappresenta solo un problema tecnico, ma soprattutto di business, dato che ormai è determinante per la continuità operativa dell'intera azienda/ente.

3.5 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 digitali. **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 ed europeo. 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 già citato rapporto "Threat Landscape 2023", considera le seguenti categorie di attori che minacciano la sicurezza digitale:

- attori vicini e sponsorizzati da stati (State-nexus threat groups)
- 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. Ma negli ultimi anni è andato crescendo il numero ed il ruolo , come singolo attaccante, di **attivisti** che per il loro "credo" e per le loro idee intendono attaccare i "nemici", veri o presunti. Gli attivisti sconfinano sovente nel fanatismo, da lupi solitari si aggregano e gli attacchi digitali possono sconfinare in terrorismo digitale e/o essere parte di guerre digitali.

L'indagine, e quindi il questionario, OAD 2024 ha approfondito gli attacchi rilevati in ambito web e in ambito OT, Operational Technology, descrivendo quanto rilevato nel Capitolo 4, cui rimanda. Per quanto riguarda i probabili attaccanti e le loro motivazioni, la maggior parte è dall'**esterno** dell'azienda/ente oggetto dell'attacco, talvolta con l'involontaria complicità di utenti interni. La principale motivazione è di tipo **economico**, ossia di un illecito guadagno.
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)** [24], e da gruppi da questi ultimi pilotati come il ben noto Gruppo Conti, creatore e diffusore di ransomware, ed il Gruppo Sandworm pilotato da Gru.

ACN ha individuato i principali gruppi di attaccanti che più hanno operato in Italia nel 2023, mostrati nella precedente fig. 3.3-3.

In generale è difficile poter individuare i vari gruppi di cyber criminali, dato che i più bravi si camuffano e si nascondono, ma altri si palesano e addirittura si fanno pubblicità suo 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 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 anch'esso coinvolto nella creazione di Stuxnet. Per un più ampio elenco, comunque 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.

3.6 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[25], solo in parte proattive e preventive[26], e pochissime predittive[27].

[24] Per approfondimenti si veda l'articolo dell'autore: https://www.agendadigitale.eu/sicurezza/ucraina-come-agisce-la-guerra-cyber-e-quali-impatti-sulleuropa/

[25] 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.

[26] 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.

[27] 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.

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[28], che dovrebbe portare alla realizzazione di sistemi ICT intrinsecamente sicuri, indipendentemente dal buono o cattivo uso da parte dell'utente: sistemi senza vulnerabilità tecniche intrinseche e così facili da usare da ridurre, se non eliminare, le possibili vulnerabilità personali ed organizzative.
Le logiche evolutive e le tecniche più innovative per la sicurezza digitale, spesso indicate con il generico termine di "**Next Generation Security**", includono:

- Il passaggio dalla tradizionale logica "statica" di misure e strumenti di difesa in funzione delle vulnerabilità e rischi individuati, ad una logica "dinamica", basata sull'analisi predittiva e comportamentale dei sistemi ICT e dei loro utenti, effettuata anche tramite sistemi di machine learning (ML);
- una crescente e forte automazione dei processi e delle attività della gestione operativa della sicurezza digitale, con l'uso di tecniche di Machine Laerning (ML) e di altre tecniche di intelligenza artificiale (IA)[29];
- l'adozione di logiche, approcci ed architetture "Zero Trust" e di un mix, con questa, di altre logiche ed architetture quali SASE, SIEM, SOAR, EDM, etc., con una loro crescente interoperabilità, integrazione ed automazione;
- l'adozione di tecniche di IA e di ML sia nella gestione operativa, ad esempio nella correlazione dei log e delle segnalazioni di sistema, sia nella threat intelligence e nell'analisi dei rischi;
- l'adozione di tecniche di autenticazione forte "passwordless" degli utenti basate su riconoscimenti biometrici, seppur ancora embrionale data anche la necessità di autorizzazione da parte del Garante della privacy;
- l'introduzione di soluzioni EDR, Endpoint[30] Detection & Response[31], che si affiancano o integrano con soluzione SIEM, SASE, etc. sulla base di logiche ed architetture "zero trust";
- il rafforzamento della sicurezza digitale nella "supply chain", dato che alcuni gravi attacchi sono partiti da vulnerabilità di fornitori e/o di clienti interoperanti con il sistema informativo target;
- inizio utilizzo soluzioni di "Threat Intelligence"[32];
- la crescente adozione di misure di sicurezza digitale "as a service", la **Cybersecurity as a Service** , e più in generale la crescente terziarizzazione della sicurezza digitale, soprattutto a livello di gestione operativa;
- l'uso di SOC, Security Operation Centre, per una proattiva ed efficace gestione della sicurezza digitale, in particolare per la gestione delle infrastrutture (soprattutto quelle critiche), la rilevazione di incidenti e le relative azioni di contrasto e contenimento. Il SOC è una struttura iper specializzata, che alcune grandi organizzazioni, ad esempio di fornitori ICT e TLC, hanno al proprio interno, ma che è anche fornito "as a service" dai MSSP, Managed Security Service Provider;

[28] 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/

[29] 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.

[30] 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.

[31] 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.

[32] Threat Intelligence è la raccolta e la selezione di informazioni dettagliate ed utilizzabili sulle minacce digitali, in moda consentire una prevenzione proattiva e predittiva dei reali rischi alla sicurezza del sistema informativo

- l'adozione, oggi ancora embrionale, di soluzioni XR, Extended Reality, e del metaverso[33], per attività di formazione, simulazione ed analisi nella sicurezza digitale, oltre che di assistenza, gestione e manutenzione, il tutto anche (e soprattutto) da remoto, e quindi fornibili "as a service";
- la tendenza alla realizzazione di soluzioni di sicurezza digitale intrinseche (embedded) nei vari sistemi digitali, in modo che tale sicurezza sia di default ed impostata fin dal progetto del sistema stesso (by design).

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

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

In ambito europeo, un driver fondamentale per l'innalzamento del livello ed il miglioramento "continuo" della sicurezza digitale sono le "nuove" normative della UE in merito sulla sicurezza digitale, che dovranno essere attuate quasi tutte entro il 2024-25: le principali sono elencate nella tabella in fig. 3.6-1.
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.

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	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. 3.6-1

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 nell'Unione Europa (UE). 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[34] e alle normative sull'intelligenza artificiale, sull'identità digitale, sui dati e sul loro governo, sui chip.

[33] 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).
[34] Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (2022/0272(COD)).

I paragrafi del successivo Capitolo 7 forniscono una fotografia delle misure di sicurezza, tecniche ed organizzative, in essere nei SI delle aziende/enti che hanno risposto alle domande "opzionali" sull'argomento del questionario online OAD 2024.

3.6.1 La terziarizzazione della sicurezza digitale

Nella maggior parte dei casi, in particolare per le piccole e medie organizzazioni, non si può disporre al proprio interno di qualificate ed aggiornate competenze sulla sicurezza digitale: in questi casi è opportuno terziarizzarla, dal progetto alla gestione operativa: ma questo non significa rinunciare totalmente alle competenze in merito, occorre sempre controllare ciò che la/le terza/e parte/i fa/fanno e come, altrimenti si diverrà preda e si sarà in balia dei fornitori e dei consulenti.
Moderne piattaforme e soluzioni quali SIEM, SOAR, SESA, e le stesse tecniche di blockchain, costituiscono sistemi molto complessi e difficili da gestire anche per grandi organizzazioni con elevate competenze al proprio interno.
Vulnerabilità e rischi digitali esistono, e della stessa complessità e sofisticazione, sia per grandi che per piccole organizzazioni. La citata necessità di terziarizzare la sicurezza digitale, soprattutto per le piccole organizzazioni italiane sta creando un crescente mercato di fornitori di servizi di sicurezza gestiti, indicati con MSSP, Managed Security Service Provider, ed incominciano ad essere utilizzati simili servizi erogati dai grandi player digitali, da Google a AWS, da Microsoft ad IBM.

3.7 Il quadro di riferimento Italiano per la sicurezza digitale

3.7.1 Aziende e PA in Italia

ISTAT recentemente ha istituito "il censimento permanente" per imprese e Pubbliche Amministrazioni (PA), si veda http://dati-censimentipermanenti.istat.it/, ma i dati fanno riferimento per ora solo ad un campione parziale di imprese e PA rispetto al totale. OAD deve quindi fare ancora riferimento ai dati ISTAT del 2022, che a loro volta considerano le imprese attive al 2020, per poter avere la ripartizione per le classi di addetti considerate.
La fig. 3.7.1-1 mostra l'ultima rilevazione ISTAT disponibile, che indica un totale di 4.665.423 imprese attive cui corrispondono un totale di 18.217.608 addetti, ripartiti per classi di addetti. Tale ripartizione è ripresa dalla fig. 3.7.1-2 che mostra la ripartizione % per classe di addetti.
Anche se il numero complessivo di imprese è diminuito nel 2023, nella logica di trend di OAD si considera, e va bene, l'ultimo dato ufficiale ISTAT.

Dalle figure emerge che tra **le PMI, che costituiscono complessivamente il 99,9% del totale**, quelle più piccole, fino a 9 dipendenti, sono la stragrande maggioranza con un **94,9%** del totale.

La fig. 3.7.1-3 evidenzia come il numero medio per impresa sia di poco inferiore ai 4 dipendenti, e che questo media è rimasta stabile negli anni.

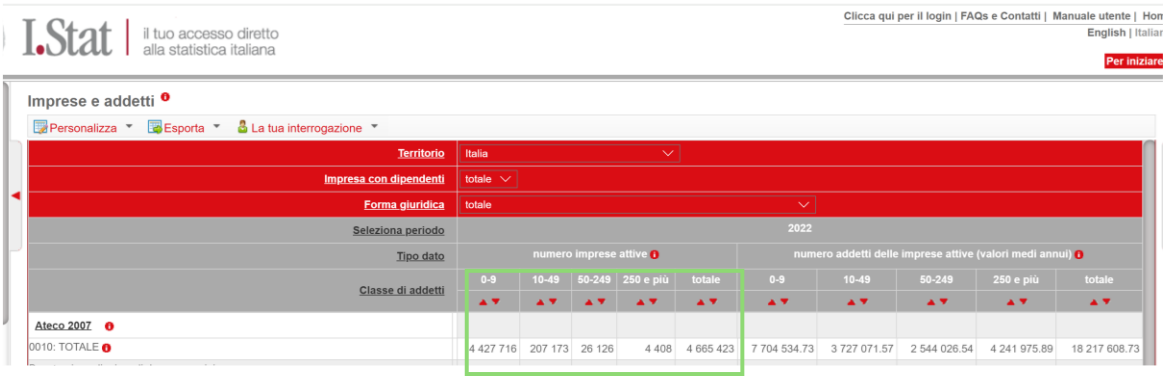


Fig. 3.7.1-1 (Fonte: ISTAT)

Numero addetti	Numero imprese	% aziende/classe addetti
0-9	**4.427.716**	**94,9%**
10-49	**207.173**	**4,4%**
50-249	**26.126**	**0,6%**
da 250 in su	**4.408**	**0,1%**
Totale	**4.665.423**	
Totale PMI	**4.661.015**	**99,9%**

Fig. 3.7.1-2 (Fonte: elaborazione OAD su dati ISTAT)

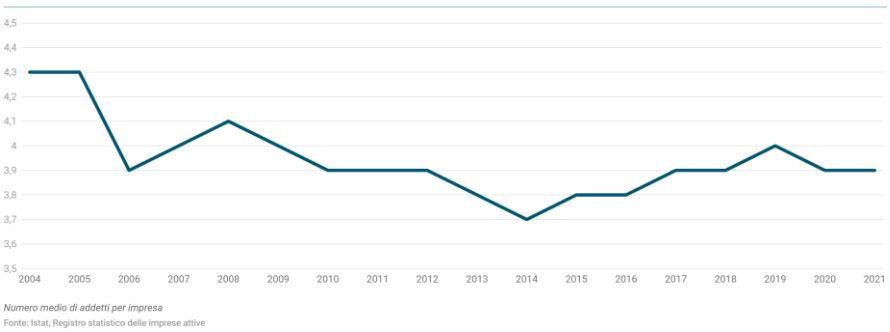


Fig. 3.7.1-3 (Fonte: ISTAT)

In estrema sintesi la stragrande maggioranza di imprese italiane sono “nano” imprese, quindi con sistemi informativi piccoli e con al proprio interno ben poche competenze sull’ICT, a parte le aziende, pur nane, che operano nell’ICT.

Per le Pubbliche Amministrazioni (PA), articolate in PA Centrali (PAC) e Locali (PAL), i dati più recenti sul numero di dipendenti complessivo, **3.266.180** a fine 2022, è fornito dalla Ricerca “Lavoro Pubblico 2023”

del ForumPA (https://www.forumpa.it/). Da questo documento OAD 2024 ha ripreso la fig. 3.7.1-4 che ripartisce i dipendenti a fine 2022 per i principali settori del complesso ed articolato mondo delle PA.

	Conto annuale Personale al 31.12.2021	Conto annuale Personale al 31.12.2022	Variazione assoluta 2022/ 2021	Variazione % 2022/ 2021
	(v.a. migliaia)			
FUNZIONI CENTRALI	203,8	205,1	1,3	0,7
FUNZIONI LOCALI	492,1	491,3	-0,8	-0,1
ISTRUZIONE E RICERCA	1.264,1	1.278,4	14,4	1,2
SANITA'	670,6	679,3	8,7	1,3
COMPARTO AUTONOMO O FUORI COMPARTO	40,3	42,4	2,1	5,3
PERSONALE IN REGIME DI DIRITTO PUBBLICO	568,1	569,6	1,5	0,3
TOTALE	**3.239,0**	**3.266,2**	**27,2**	**0,8**

Fig. 3.7.1-4 (Fonte: ForumPA)

Per il 2023 il numero di dipendenti della PA è ulteriormente aumentato.

Dal punto di vista informatico, l'intera PA è in fase di profonda trasformazione digitale, secondo le direttive dei Piani Triennali, prima da quello 2021-23, ora da quello 2024-206 (per i dettagli: https://pianotriennale-ict.italia.it/), e con la partecipazione a vari progetti, e fondi, del PNRR, il Piano Nazionale di Ripresa e Resilienza (si veda §3.7.3).

3.7.2 La spesa in sicurezza digitale in Italia nel 2023

I dati presi a riferimento sul tema sono derivati dall'ultimo ed autorevole rapporto **Anitec-Assinform,** patrocinatore di OAD 2024, "Il Digitale in Italia 2024" (https://www.anitec-assinform.it/media/news/pubblicato-il-rapporto-il-digitale-in-italia-2024.kl):

- l'intero mercato digitale in Italia nel 2023 è stimato in **78,7 miliardi di euro**, che rappresenta il 4% del PIL nazionale;
    - rispetto ai 77, 085 miliardi del 2022, si ha una crescita del 2,1%, maggiore del 1,5% del PIL nazionale;
- Il mercato della cybersicurezza nel 2023, ha un valore stimato di **1.787,9 milioni di euro**, con un **incremento del 12,4% rispetto al 2022**. La fig. 3.7.2-1 mostra la segmentazione di tale mercato e le percentuali di crescita rispetto agli anni precedenti. Si sottolinea come il segmento "Servizi MSS e Cloud" risulti quello con il più alto tasso di crescita.

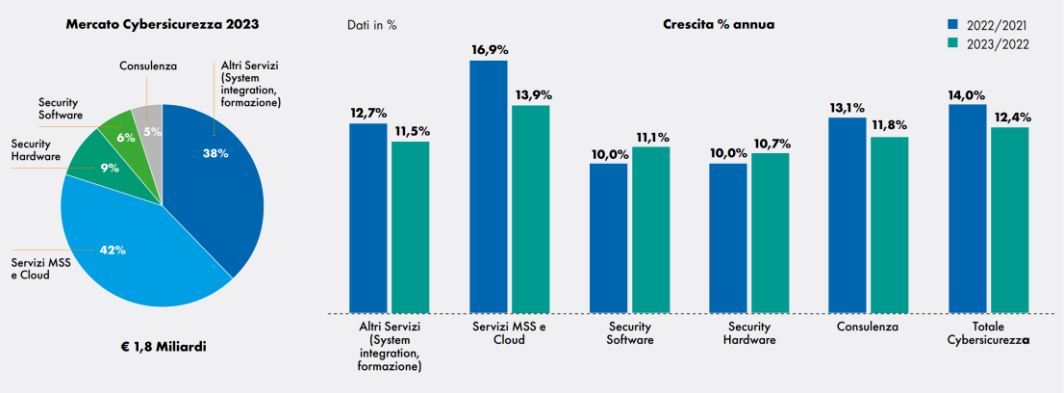


Fig. 3.7.2-1 (Fonte: Rapporto 2024 Anitec-Assinform)

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

Il PNRR[35], 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)[36] 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;
- conseguire una maggiore equità di genere, territoriale e generazionale.

Come già descritto nel precedente Rapporto OAD 2023 (liberamente scaricabile da https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-2023.html), 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.

L'intero PNRR si articola in sedici Componenti, raggruppate in sei Missioni e sintetizzate nella tabella di fig. 3.7.3-1 (per i dettagli si rimanda a https://italiadomani.gov.it/it/home.html).

Tra i progetti più importanti 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 milioni;
  - per l'ammodernamento del parco tecnologico ospedaliero, Regioni e Provincie Autonome stanno acquistandole da Consip.

[35] https://www.governo.it/sites/governo.it/files/PNRR.pdf
[36] https://ec.europa.eu/info/strategy/recovery-plan-europe_it

Per lo stato di avanzamento dei vari progetti si rimanda a https://www.italiadomani.gov.it/content/sogei-ng/it/it/strumenti/andamento-sull-attuazione-del-piano.html?orderby=%40jcr%3Acontent%2FyearAndSemesterLabel&sort=desc

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. 3.7.3-1 Composizione del PNRR per Missioni e Componenti con valori in miliardi di €

3.7.4 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. 3.7.4-1 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.

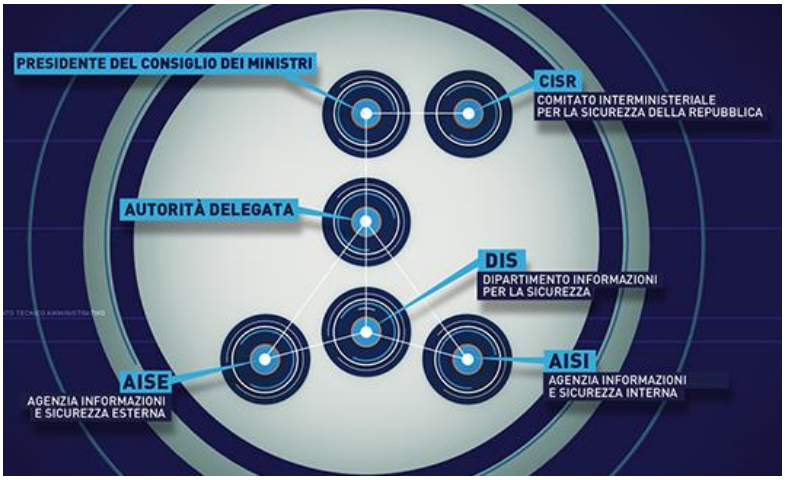


Fig. 3.7.4-1

La figura evidenzia le due Agenzie operative, l'**AISI** per l'intelligence in ambito interno al paese, e l'**AISE** per l'intelligence in ambito esterno, quindi all'estero negli altri paesi europei e non. A quest'ultima fanno riferimento, quando operano all'estero, anche gli organismi militari italiani di intelligence.
Questa logica di centralizzazione decisionale è stata 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 dello Stato Maggiore della Difesa (SMD), coordina le attività di sicurezza e difesa cibernetica delle Forze Armate e del Ministero della Difesa (https://www.difesa.it/smd/cor/la-missione-e-i-compiti/32647.html).

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

- **Polizia Postale e per la Sicurezza Cibernetica**: preposta al contrasto delle frodi postali e del crimine informatico (https://www.commissariatodips.it/)
    - **C.N.A.I.P.I.C**, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (https://www.commissariatodips.it/profilo/cnaipic/index.html)
- **NSTPFT,** Nucleo Speciale Tutela Privacy e Frodi Tecnologiche: Reparto Speciale della Guardia di Finanza che si occupa di contrastare le frodi telematiche ed informatiche, nonché tutelare la privacy (https://www.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/: il Comitato intergovernativo delle Nazioni Unite di esperti l'8 agosto 2024 ha approvato all'unanimità la Convenzione contro la Criminalità Informatica. Il trattato attende ora l'approvazione dell'Assemblea Generale.

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

3.7.5 Le leggi italiane in vigore per la sicurezza informatica

Per concludere l'inquadramento della sicurezza digitale in Italia è opportuno fornire qualche indicazione sulla normativa vigente, che è complessa e assai articolata.
La legislazione sulla sicurezza e sul crimine informatico in Italia ha iniziato ad apparire nei primi anni 90 del secolo scorso, con l'introduzione della Legge 547/1993 sul crimine informatico.
Sono poi seguite varie leggi, decreti legislativi e DPCM[37], alcuni dei quali sono aggiornamenti di precedenti normative, o normative nazionali per le Direttive UE (si veda $3.6 e fig. 3.6-1).
Norme di riferimento per la sicurezza digitale sono poi incluse in diverse altre normative, sia per specifici settori merceologici, quali ad esempio le telecomunicazioni, le banche, le assicurazioni, e le Pubbliche Amministrazioni, sia per specifiche tematiche quali ad esempio la privacy, il documento informatico, la firma elettronica e digitale, il diritto d'autore e la tutela del software.
La maggior parte delle normative italiana sulla sicurezza digitale rientrano nel codice civile, ma alcuni **reati informatici sono sanzionati anche a livello di codice penale**: si vedano ad esempio gli art. 392, 420, 491bis, 615, 616, 617, 621, 623bis, 635, 640 del Codice Penale.
La recentissima Legge del 28/06/2024 n. 90 - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, modifica il Codice Penale, introducendo il reato di "estorsione mediante attacco informatico": il riferimento all'ampiezza del fenomeno dei ransomware in Italia è evidente.

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

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

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

4. Gli attacchi digitali in Italia dall'indagine OAD 2024

Il questionario OAD 2024 ha posto due sole domande sugli attacchi digitali subiti nel 2023 dai Sistemi Informativi (SI) delle aziende/enti rispondenti, in modo da poter continuare l'analisi dei trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 ad oggi, ed ha approfondito gli attacchi digitali rilevati nel 2023 **alle applicazioni ed agli ambienti web** ed ai **sistemi OT, Operation Technology**.

La fig. 4-1 mostra, percentualmente, il numero di attacchi digitali intenzionali rilevati dalle/dai rispondenti nel 2023 e conferma il gran numero di attacchi digitali portati nel 2023 ai Sistemi Informativi (SI) delle aziende/enti rispondenti.

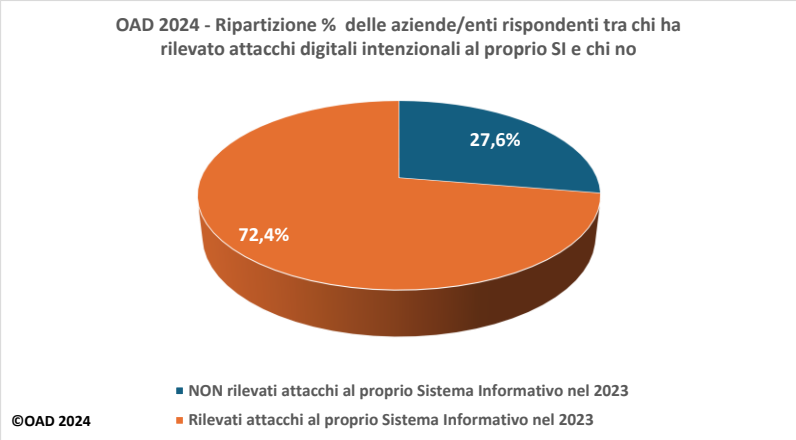


Fig. 4-1

La fig. 4-2 mostra il numero di attacchi rilevati nei diversi Rapporti OAI 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. 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 con il primo picco di 55,7%, porta la percentuale di attacchi rilevati a superare, e per più di 10 punti, la percentuale di quelli non occorsi/rilevati. Nel 2019 il trend di crescita dei precedenti tre anni si arresta, con una diminuzione al 46,6%, confermando ancora il trend di rafforzamento delle misure di sicurezza dopo una fase di maggiori e più sofisticati attacchi.

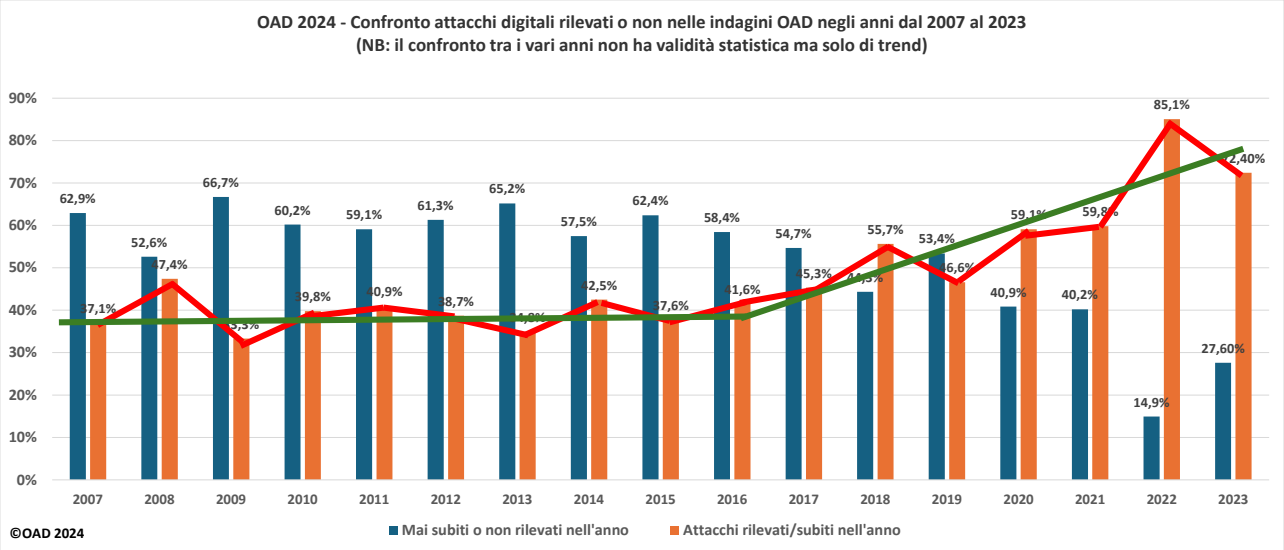


Fig. 4-2

Nel 2020 e nel 2021, nel campione dei rispondenti, la percentuale di chi ha rilevato attacchi cresce ancora avvicinandosi al 60%. Nel 2022 si rileva un vero e proprio balzo all'**85,1%** dei SI dei rispondenti che hanno rilevato attacchi, con un delta tendenziale di poco più del 25%.
Nel 2023 si ha una riduzione di tale percentuale al **72,4%**, percentuale sempre molto alta. Le motivazioni di tale riduzione sono, per l'autore, principalmente due:

- Un diverso mix di aziende/enti rispondenti al questionario OAD 2024 rispetto a quello dell'edizione OAD 2023, e con una più alta percentuale di piccole e piccolissime organizzazioni, che non sono di norma nel mirino di specifici attacchi, quelli targeted, e di grandi gruppi di attaccanti;
- Il tradizionale ciclo prima descritto, si attua novamente: dopo un 2022 di picco degli attacchi, che continua la crescita dal 2020, ed in presenza di attacchi a forte impatto sul SI e sul business degli attaccati, si impone alle imprese di rafforzare le misure di difesa dei propri SI; e nel 2023 la percentuale di attacchi subiti, nel campione emerso dall'indagine, diminuisce.

Anche i dati forniti dalla Polizia Postale per il 2023 evidenziano una riduzione degli attacchi alle infrastrutture critiche, si veda il Capitolo 8 ed in particolare la fig. 8-1. Tali indicazioni sembrano essere in contrasto con il dato dell'ACN, che nel Rapporto ACN 2023 dichiara un aumento degli attacchi nel 2023 rispetto al 2022 del 140%. A giudizio dell'autore, questa differenza è dovuta ai bacini numericamente diversi di chi segnala gli attacchi digitali allo CSIRT di ACN rispetto al C.N.A.I.P.I.C. della Polizia Postale: il bacino di aziende/enti cui fa riferimento CSIRT è al momento più piccolo rispetto a quello del C.N.A.I.P.I.C.

Nella fig. 4-2 la riga verde evidenzia nei 17 anni di indagine OAD il mega trend degli attacchi subiti. Dal 2020 la percentuale di attacchi rilevati supera sempre, e nettamente quella di attacchi non subiti, e conferma che **dal 2020** anche in Italia si è entrati nell'**era della insicurezza digitale sistemica** (**systemic cyber insecurity**).
Da un lato gli attacchi intenzionali sono sempre più sofisticati e difficili da individuare e contrastare, dall'altro le misure di sicurezza di contrasto in essere non risultano essere ancora adeguate e sufficienti, neppure per i SI più critici e quindi più protetti.
Le piccole e piccolissime organizzazioni nella maggior parte dei casi non hanno, e non possono avere, competenze e capacità economiche per acquisire e gestire gli strumenti di sicurezza digitale, tecnici ed organizzativi, necessari; ma esse non rappresentano un obiettivo di interesse specifico per i cyber criminali, soprattutto per gli attacchi mirati (targeted attack), mentre esse possono essere coinvolte in attacchi di massa,

come quelli basati sul phishing e sul ransomware, così come avviene tipicamente o per cogliere qualcuno nella massa, o per azioni di attivismo o di terrorismo informatico.
Questo è confermato analizzando la fig. 4-3 e la fig. 4-4 che mostrano la distribuzione percentuale degli **attacchi NON subiti** nel 2023 per dimensione (numero di dipendenti) e per fatturato/entrate (questo per le PA) dell'ultimo bilancio disponibile delle aziende/enti rispondenti (si veda §6.1 e in particolare fig. 6.1-3 e fig. 6.1-4).
Entrambe le fig. 4-3 e 4-4 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 questa tendenza, confermando quanto rilevato anche nelle precedenti indagini OAD: gli attacchi digitali, soprattutto quelli mirati ad una specifica impresa, o a un gruppo similare di imprese (attacchi "targeted"), sono effettuati prevalentemente a organizzazioni di grandi dimensioni, ben note come brand, e con un grande giro d'affari.
Alcune grandi organizzazioni rispondenti hanno dichiarato di non aver subito/rilevato attacchi: la maggior parte di esse ha sistemi informativi con elevatissimi livelli di sicurezza, che plausibilmente hanno proattivamente respinto e/o scoraggiato gli attacchi digitali. Per le misure di sicurezza dei sistemi informativi dei rispondenti si rimanda al Capitolo 7.
Come già indicato in precedenza, per una corretta interpretazione delle correlazioni elaborate per produrre queste due figure che correlano dati relative a diverse domande, si deve tener conto che le percentuali emerse dipendono anche dal numero di risposte ricevute: quello che interessa all'indagine OAD è evidenziare un determinato fenomeno, i numeri delle percentuali che emergono fanno solo riferimento al bacino di rispondenti.

La fig. 4-4 evidenzia un insieme percentualmente significativo di aziende/enti che non hanno voluto o potuto dichiarare il loro fatturato, e che dichiarano di non aver subito o rilevato nel 2023 attacchi digitali: non potendo distinguere tra loro in termini di fatturato, questa percentuale non fornisce indicazioni utili nella ripartizione per fatturato, e per questo è circondata da una cornice rossa.

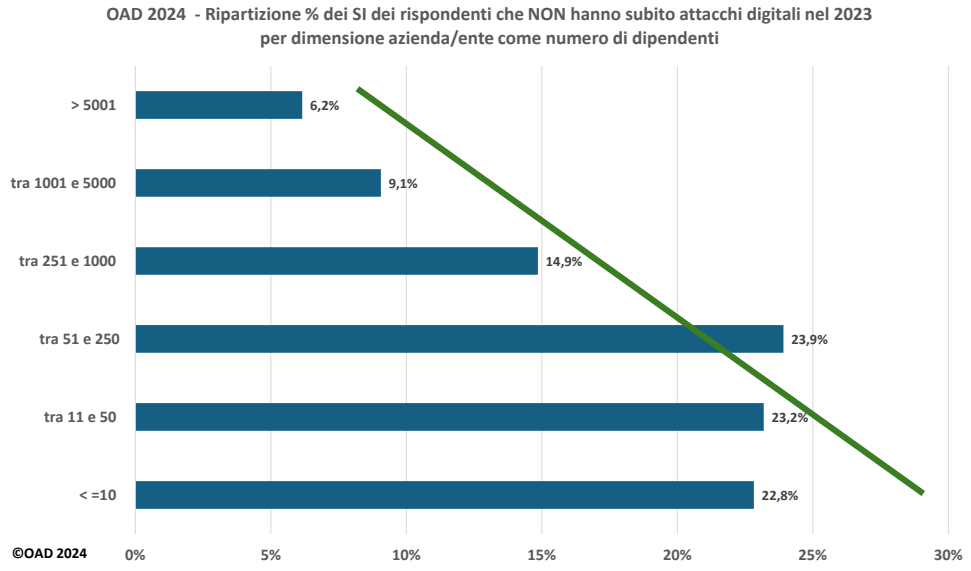


Fig. 4-3

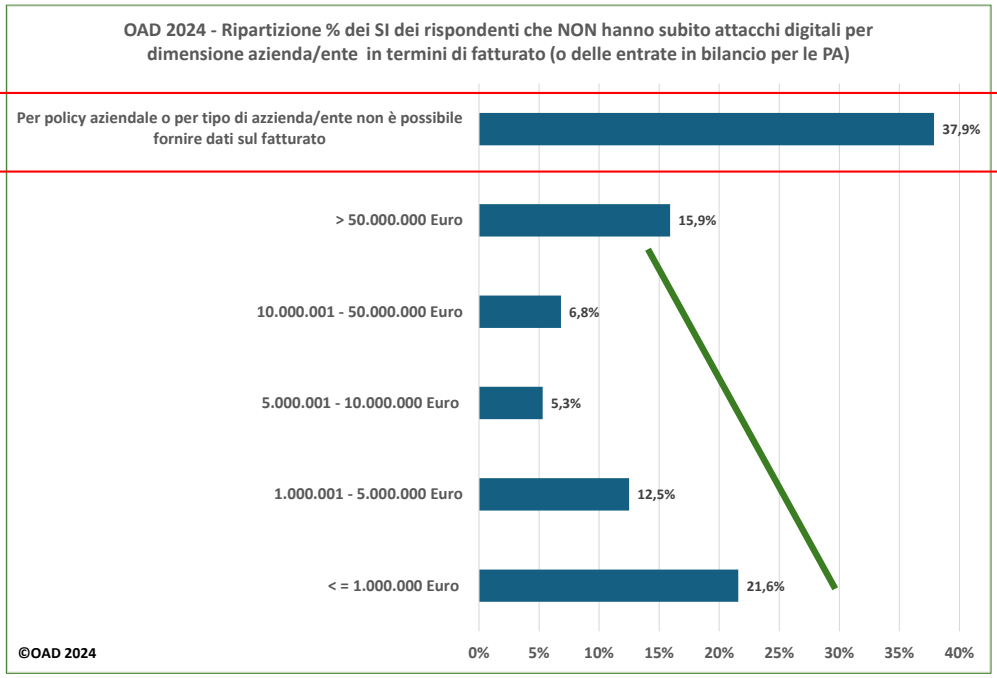


Fig. 4-4

4.1 Tipologie e tecniche di attacco emerse

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 2024 ha incluso nel questionario 15 diverse "famiglie di tipologie" di attacchi. Questi gruppi, che raggruppano attacchi simili, permettono di evitare richieste di dettagli eccessivi, semplificando la compilazione del questionario per i partecipanti.
OAD 2024 ha introdotto una nuova tipologia di attacco, rispetto a quelle considerate negli anni precedenti, relativa agli **attacchi alla supply chain informatizzata**, ossia quelli causati da attacchi ai SI di fornitori e/o clienti collegati ed interagenti con il SI target del rispondente. Se il SI di un fornitore o di un cliente ha lacune in termini di sicurezza, queste lacune vengono usate per portare un attacco al SI target tramite le applicazioni di logistica interoperanti tra i vari SI.

La fig. 4.1-1 mostra che il **27,6%** dei SI delle aziende/enti rispondenti non ha riportato/rilevato attacchi digitali, come già analizzato in §4, e in dettaglio evidenzia al primo posto, analogamente all'edizione precedente, con un **31,7%**, 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 20,7%, gli attacchi **DoS/DDoS**, che come si è visto in §3, sono stati uno dei mezzi più usati nell'ambito delle cyber warfare, in particolare da parte delle organizzazioni hacker schierate pro Russia.
Significativo al quarto posto, con un **15%, gli attacchi alla supply chain informatizzata**. Questo dato conferma la diffusione e criticità di questa tipologia d'attacco, considerata uno dei principali rischi a livello mondiale (si vedano le previsioni del World Economic Forum in §3).

Il **furto di dispositivi mobili**, in particolare gli **smartphone**, rimane un fenomeno significativo, con un **13,4%**: in essi non solo sono normalmente contenute tutte le password e le modalità di accesso ai servizi informatici utilizzati, come gli account di posta elettronica ed i conti in banca (e talvolta tali dati non sono protetti nel dispositivo, tutti i dati basilari per furti, frodi e furti di identità digitali, ma lo stesso dispositivo ha sovente un alto valore sul mercato dell'usato.
Tutte le altre tipologie di attacchi hanno percentuali al di sotto del 10% tra le/i rispondenti, e per la prima volta con OAD 2024 i sistemi di controllo degli accessi (IAA, Identificazione-Autenticazione-Autorizzazione) e gli attacchi alle reti geografiche/locali non sono ai primi posti di questa classifica di diffusione delle varie tipologie di attacco, come lo erano invece nelle precedenti edizioni di OAD.

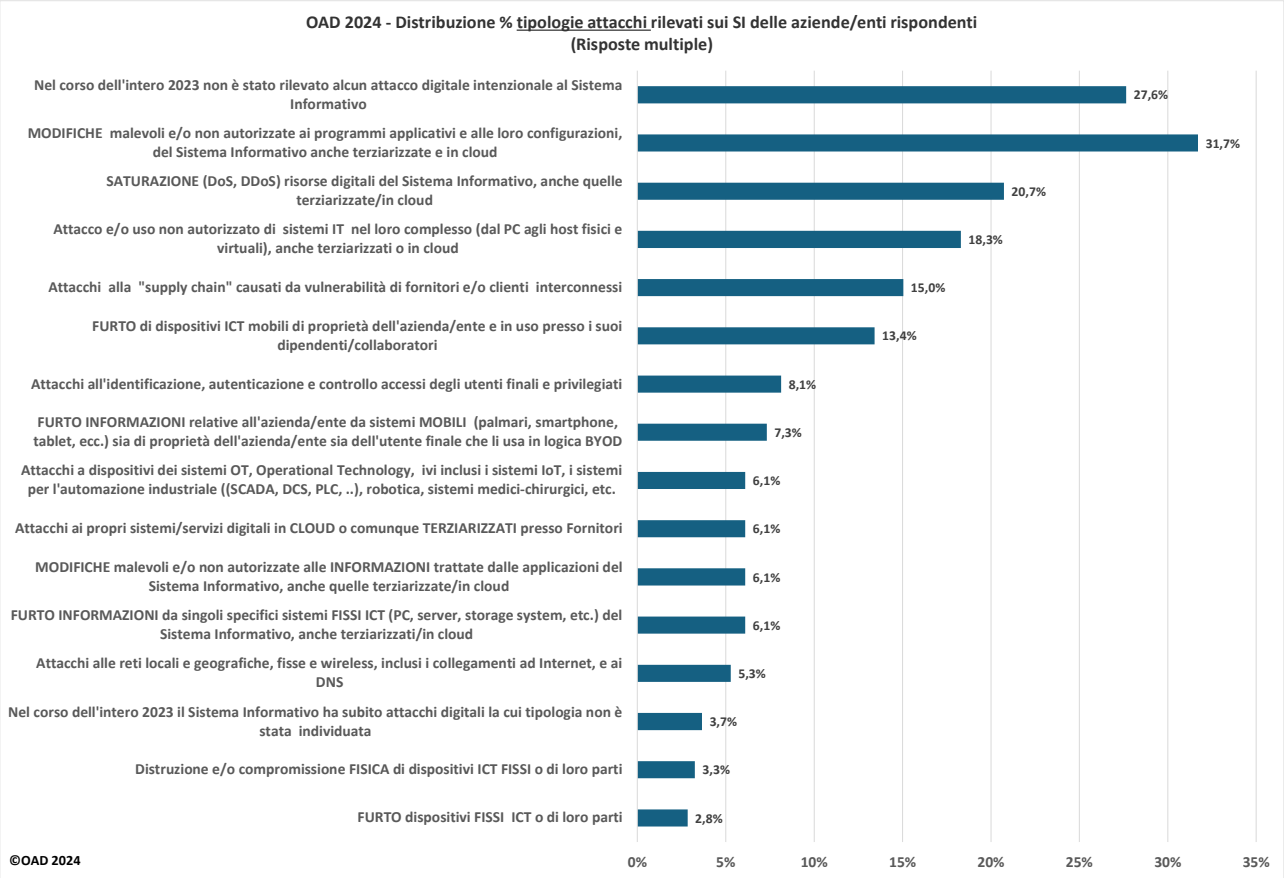


Fig. 4.1-1

La fig. 4.1-2 mostra la **diffusione**, in percentuale, delle **tecniche di attacco** riscontrate nei più gravi attacchi subiti nel corso del 2023.

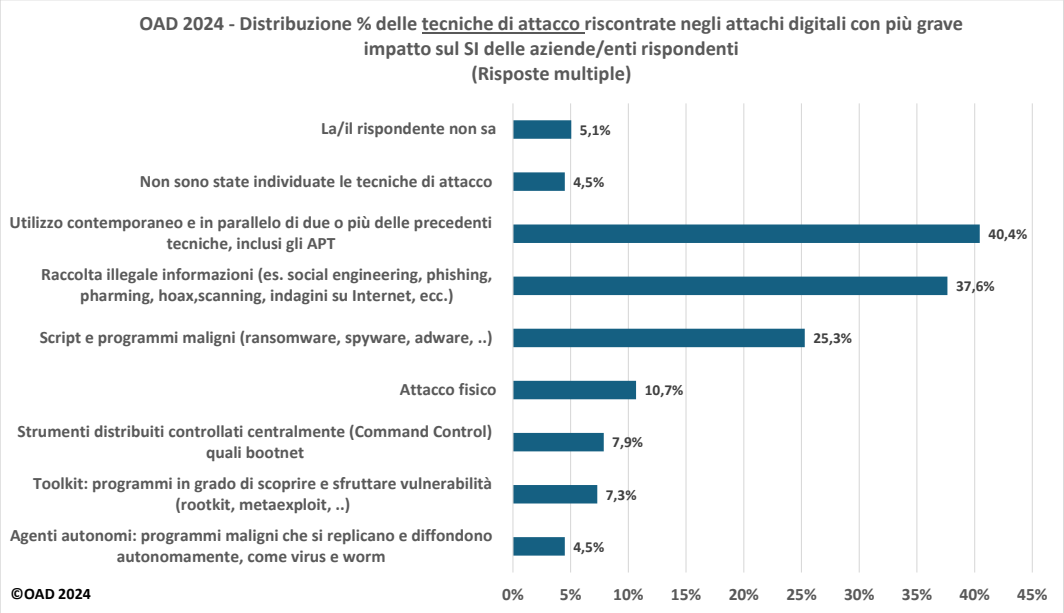


Fig. 4.1-2

Data la differenza e la molteplicità delle tecniche usate per i diversi attacchi, e la numerosità di questi ultimi, per avere risposte credibili si è richiesto nel questionario OAD 2024 di fare riferimento al più grave attacco subito; e tale logica è applicata a numerose altre domande di approfondimento sugli attacchi trattati nel seguito per gli ambienti web ed OT.

Nella fig. 4.1-2 emerge che risultano percentualmente pochi i rispondenti che non sanno fornire una risposta o perché non hanno specifiche informazioni o perché non sono state individuate le tecniche usate per l'attacco più grave subito. L'uso di **più tecniche per lo stesso attacco** risulta il metodo percentualmente più diffuso, con un **40,4%**. L'uso nello stesso attacco di più tecniche, sia in parallelo che sequenzialmente, è ormai una prassi consolidata, e non solo per gli attacchi più complessi e sofisticati. Si parte da un "entry point", costituito normalmente da vulnerabilità personali di un utente, che fornisce involontariamente dati tramite tecniche di social engineering: ad esempio dal furto del cellulare con informazioni sui suoi account non protetti, o dall'apertura di email di phishing con attivazione di un malware, e così via. L'entry point può essere fornito anche da vulnerabilità tecniche del sistema, che consentono l'inserimento e l'attivazione di un malware o di prendere il controllo del sistema "di ingresso". Con queste tecniche l'attaccante riesce ad entrare in una risorsa ICT del SI oggetto dell'attacco, e da qui analizzare le risorse e le loro vulnerabilità, individuando gli asset per lui più interessanti in funzione dei suoi scopi e da attaccare con le tecniche più idonee. Dopo questa analisi viene sferrato uno o più attacchi finali, talora in periodi diversi, qualora i gestori del SI non si fossero ancora accorti di essere sotto attacco.
Come tecniche più diffuse al secondo posto si colloca, con un **37,6%**, la **raccolta illegale di informazioni**, ottenute tipicamente con il **social engineering**, sfruttando la poca attenzione del soggetto interlocutore. Al terzo posto, con il **25,3%**, i **codici maligni**, alla base degli assai diffusi attacchi di ransomware.
Stupisce in questa classifica che tecniche tipo bootnet, che sono alla base di attacchi di saturazione di risorse ICT, i **DDoS/DoS**, abbiano solo un **7,9%** di diffusione quando i relativi attacchi hanno nel 2023 una diffusione percentuale del 20,7% tra i rispondenti. Per l'autore questa differenza è probabilmente dovuta alla non conoscenza, da parte di chi compila il questionario, che la saturazione delle risorse usa questa tecniche, o all'aver considerato le tecniche multiple anche per questo tipo di attacchi DDoS/DoS.

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

Come già sottolineato nei precedenti capitoli, l'indagine OAD 2024 ha effettuato, come nelle due precedenti edizioni, un'indagine "verticale" sugli **attacchi digitali in ambiti web**, che costituiscono ormai nei sistemi informativi la maggior parte degli ambiti applicativi, e per questo motivo, essendo esposte in Internet, attirano gran parte degli attacchi, sia di tipo target sia di tipo massivo.
Già con OAD 2017 era stata effettuata un'indagine "verticalizzata" sugli attacchi agli applicativi, ripresa e citata da AGID[38], e le indagini sul tema di OAD del 2024 e dei precedenti anni possono essere considerate un suo aggiornamento.

Per l' ambito web il questionario OAD 2024 ha posto domande di dettaglio, così come per gli attacchi ai sistemi OT trattati in §4.3, mentre per tutte le altre tipologie di attacco sono state poste solo due domande, sulla tipologia e sulle tecniche di attacco, con i risultati descritti nel precedente §4.1.

Rispetto al **72,4%** dei rispondenti che hanno rilevato attacchi ai propri SI, il **58,4%** ha rilevato attacchi alle applicazioni ed agli ambienti web, si veda fig. 4.2-1, e di questi il **60,6%** li ha subiti nei propri ambienti web **in cloud** (che dovrebbero essere, mediamente, più sicuri di quelli on premise), come evidenziato nella fig. 4.2-2 con risposte multiple.

La fig. 4.2-3, con risposte multiple, mostra la diffusione in percentuale di quali siano state le **vulnerabilità probabilmente sfruttate per l'attacco più critico rilevato**. Come già indicato in §3 e in §4.1, gli attacchi digitali odierni sfruttano più vulnerabilità, sia quelle tecniche che quelle personali e dell'organizzazione, e sono in grado, nel corso dell'attacco stesso, di cambiare l'obiettivo sulle risorse del sistema informativo bersaglio di maggior valore, per l'attaccante, e con minori difese. Dalla figura emerge che le **vulnerabilità tecniche assommano al 82,7%**, ma **quelle personali**, che in parte dipendono anche dall'organizzazione (ad esempio dalla non formazione degli utenti sia finali sia privilegiati), **al 92,3%**.

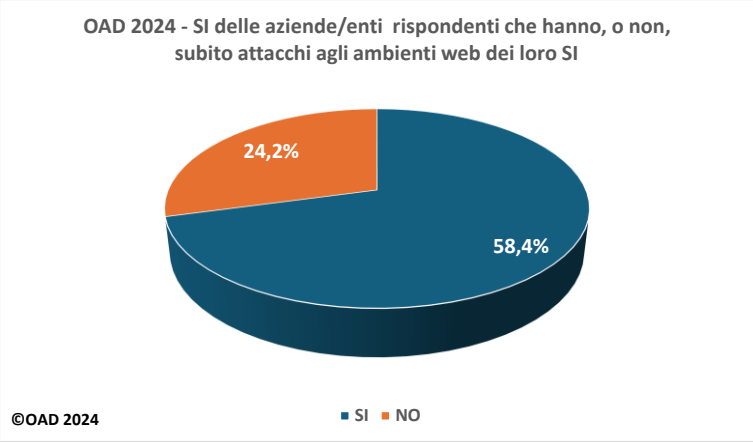


Fig. 4.2-1

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

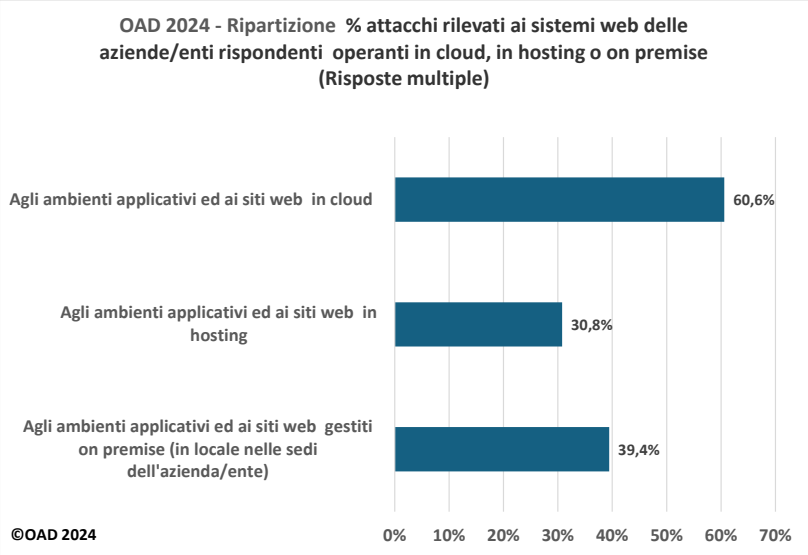


Fig. 4.2-2

Tra le vulnerabilità personali, quella **dell'utente privilegiato** si posiziona al primo posto, con il **55,8%**, mentre quelle dell'**utente finale**, con il **36,5%**, si posiziona al terzo posto. Tra le vulnerabilità tecniche, al secondo posto si posizionano quelle delle **piattaforme web di supporto**, con il **39,4%**: le vulnerabilità nel funzionamento di una applicazione web dipendono sovente da quelle della piattaforma su cui si basa. Le **vulnerabilità specifiche ed intrinseche** di una applicazione web si collocano al quarto posto, con un **30,8%**. Le altre vulnerabilità considerate, in particolare quelle dei dispositivi d'utente che si interfacciano ed interagiscono con gli ambienti web, hanno % basse. Nella voce "Altro" di fig. 4.2-3 non sono state indicate corrette vulnerabilità.

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

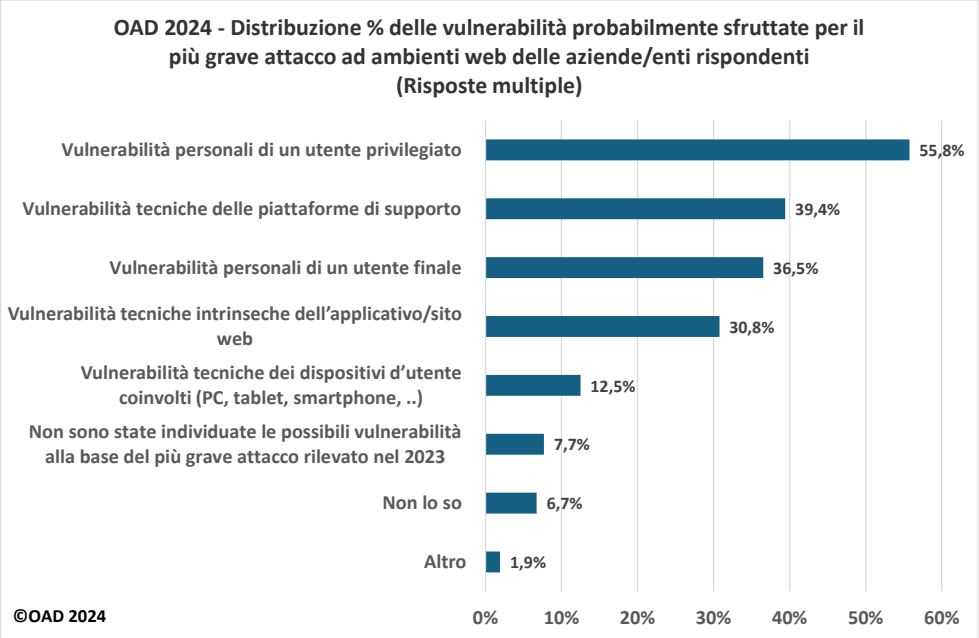


Fig. 4.2-3

Sulle vulnerabilità tecniche degli ambienti web, il questionario OAD 2024 ha posto due domande tecniche basate sulle analisi **OWASP**[39] a livello mondiale, sempre in riferimento all'attacco più grave e critico rilevato nel 2023 agli ambienti web del SI delle aziende/enti rispondenti:

- **OWASP Top Ten: le 10 principali vulnerabilità tecniche** per attacchi digitali al mondo web, nell'ultimo aggiornamento disponibile del 2021 (si veda https://owasp.org/Top10/it/). La fig. 4.2-4 elenca tali vulnerabilità nell'ordine di diffusione "mondiale" alla data dell'aggiornamento;
- **OWASP Top 10 API Security Risks – 2023**: i **10 principali rischi sulle interfacce API web**[40]**,** aggiornati nel 2023, che sono sfruttati per attacchi digitali agli ambienti web (si veda https://owasp.org/API-Security/editions/2023/en/0x11-t10/). La fig. 4.2-5 elenca tali API, Application Program Interface.

OAD 2024 ha voluto considerare anche questo secondo elenco di OWASP in quanto più aggiornato rispetto al primo.

[39] OWASP, Open Web Application Security Project, iniziativa che formula a livello mondiale linee guida, strumenti e metodologie per migliorare la sicurezza delle applicazioni in ambito web. (https://owasp.org/),
[40] API, Application Programming Interface, è un insieme di regole e protocolli che consentono alle applicazioni software di comunicare tra loro per scambiare dati e funzionalità. Le API web vengono usate per consentire il trasferimento di dati e funzionalità via Internet con il protocollo HTTP/HTTPS.

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

Fig. 4.2-4 (fonte: OWASP)

Interfaccia	Funzionalità	Dettagli OWASP
API1:2023	Broken Object Level Authorization	https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
API2:2023	Broken Authentication	https://owasp.org/API-Security/editions/2023/en/0xa2-broken-authentication/
API3:2023	Broken Object Property Level Authorization	https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-authorization/
API4:2023	Unrestricted Resource Consumption	https://owasp.org/API-Security/editions/2023/en/0xa4-unrestricted-resource-consumption/
API5:2023	Broken Function Level Authorization	https://owasp.org/API-Security/editions/2023/en/0xa5-broken-function-level-authorization/
API6:2023	Unrestricted Access to Sensitive Business Flows	https://owasp.org/API-Security/editions/2023/en/0xa6-unrestricted-access-to-sensitive-business-flows/
API7:2023	Server Side Request Forgery	https://owasp.org/API-Security/editions/2023/en/0xa7-server-side-request-forgery/
API8:2023	Security Misconfiguration	https://owasp.org/API-Security/editions/2023/en/0xa8-security-misconfiguration/
API9:2023	Improper Inventory Management	https://owasp.org/API-Security/editions/2023/en/0xa9-improper-inventory-management/
API10:2023	Unsafe Consumption of APIs	https://owasp.org/API-Security/editions/2023/en/0xaa-unsafe-consumption-of-apis/

Fig. 4.2-5 (fonte: OWASP)

La fig. 4.2-6 , con risposte multiple, riporta la **diffusione** percentuale tra i rispondenti a OAD 2024 dello sfruttamento (probabile) delle **Top Ten vulnerabilità elencate da OWASP** nell'attacco più grave agli ambienti web dei loro SI.

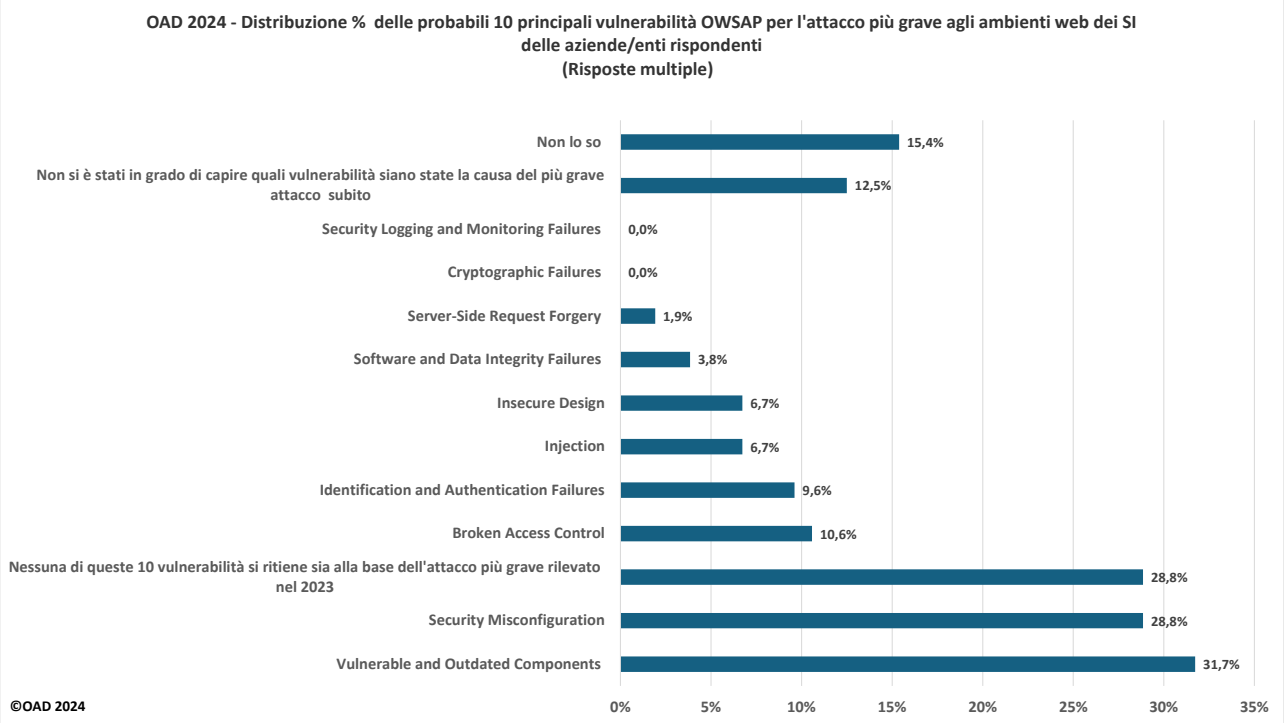


Fig. 4.2-6

La vulnerabilità in testa a questa classifica è, con il **31,7%**, quella dei **componenti software non aggiornati o obsoleti**. Segue, con **il 20,4%**, **l'errata configurazione** degli strumenti di sicurezza e **con uguale percentuale**, la/il rispondente che non ritiene nessuna di queste vulnerabilità la causa dell'attacco più grave. Infatti alcuni diffusi attacchi, quali ad esempio il DDoS/DoS, non hanno bisogno di alcuna vulnerabilità nel software del web e della sua piattaforma, ma solo la mancanza di strumenti atti a bloccare e/o dirottare l'enorme flusso di dati di attacco che satura le linee.
A scalare, ma con percentuali molto minori, le altre vulnerabilità "top" indicate da OWSAP. Significativo che il 15,4% di chi ha compilato il questionario ammetta di non saper rispondere, e che l'12,5% specifichi che non si è stati in grado di individuare le vulnerabilità tecniche causa dell'attacco più grave agli ambienti web del SI. In effetti questa domanda, così come la successiva, è tecnica e solo degli esperti del settore sono in grado di individuare correttamente quali di queste vulnerabilità è stata la causa di un attacco.
Nel complesso quanto emerge dalle risposte avute a questa domanda è ragionevole, per l'autore, considerando la realtà dei siti web di aziende/enti di ogni dimensione in Italia (ma non solo). Molti siti/applicazioni web utilizzano piattaforme e sistemi opensource non correttamente configurati soprattutto in termini di sicurezza digitale, in taluni casi con l'uso di moduli e componenti obsoleti e non aggiornati. Gli aspetti di sicurezza di un software, se esistenti, sono normalmente da settare a livello di configurazione del software, e spesso sono lasciati di default per la fretta e/o per la loro non conoscenza; ed il default il più delle volte coincide con il settaggio non attivo dei parametri/misure di sicurezza.

La fig. 4.2-7, con risposte multiple, riporta la diffusione percentuale tra i rispondenti a OAD 2024 dello sfruttamento (probabile) dei **10 rischi** sulle **interfacce (API) usate negli ambiti web** più diffusi a livello mondiale ed elencate da OWASP nell'attacco più grave agli ambienti web dei loro SI. Il **46,2%,** quasi la metà,

dei rispondenti dichiara che **l'attacco più grave non è stato causato dai rischi API della top ten di OWSAP**, il 20,2% ammette di non essere in grado di rispondere a questa domanda, a conferma della difficoltà a rispondere a questa domanda, e il 16,3% che non sono state individuate le vulnerabilità/rischi delle API usate. Congruentemente con quanto emerso sulle vulnerabilità web in fig. 4.2-6, **l'API Security Misconfiguration** ha la percentuale più alta con l'**8,7%.**

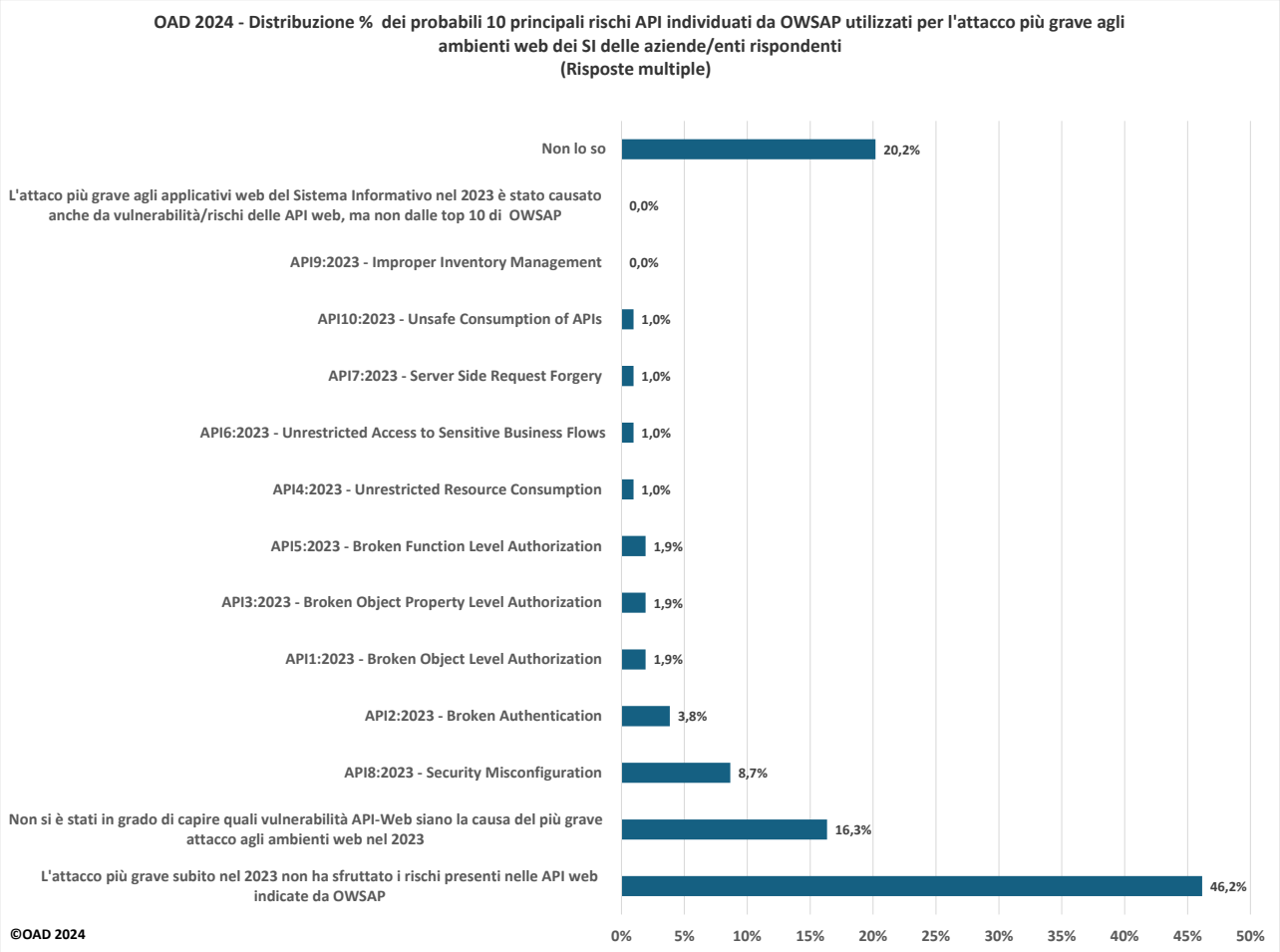


Fig. 4.2-7

Le fig. 4.2-8 e 4.2-9 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 a livello tecnico** dell'attacco più grave è stato **pesante** per i SI delle aziende/enti rispondenti, con il **85,3%** dei casi con un disservizio durato **da 2 giorni in su**.

Anche **l'impatto economico** è stato **significativo,** per il **86,5%** con un **aumento dei costi** sul **budget del sistema informativo**, ed il **24%** che ha visto questo costi ripercuotersi **sul bilancio dell'azienda/ente**.

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

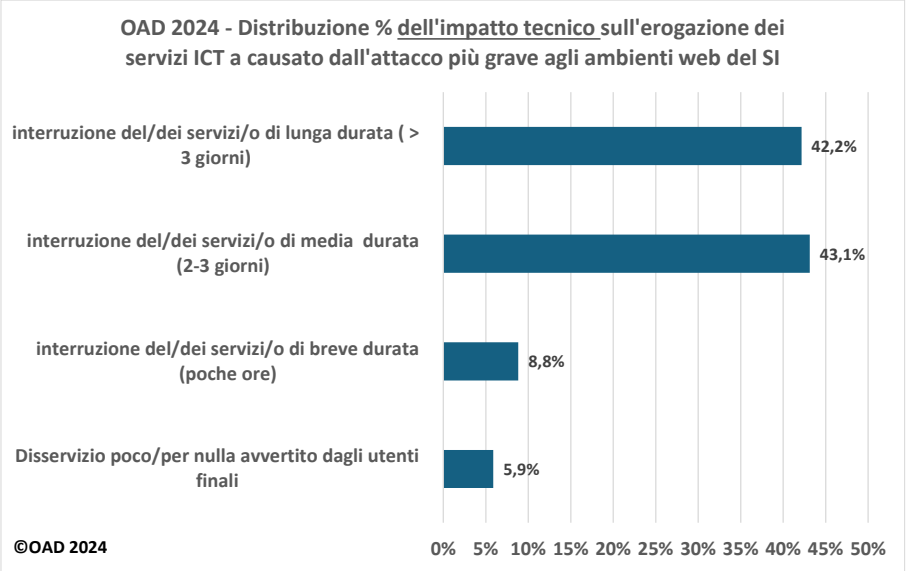


Fig. 4.2-8

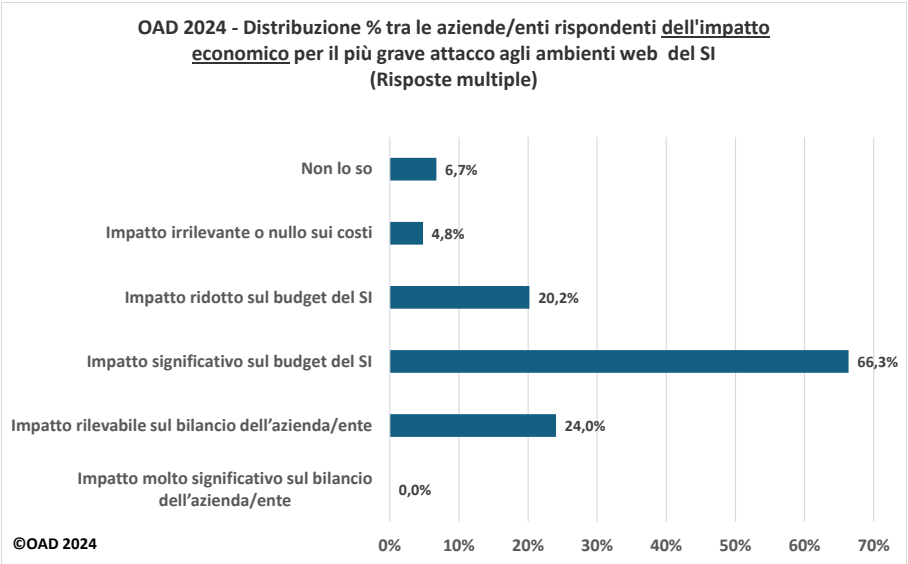


Fig. 4.2-9

La fig. 4.2-10 mostra, con risposte multiple, la distribuzione percentuale delle **possibili motivazioni** per l'attacco più grave sui siti e sulle applicazioni web del sistema informativo delle aziende/enti rispondenti. Al primo posto, con percentuali quasi uguali, sono **la frode** ed **il ricatto**, quest'ultima anche per la diffusione di ransomware, come evidenziato nelle precedenti fig. 4.1-1 (si veda: modifiche malevoli/non autorizzate ai programmi e alle configurazioni dei sistemi ICT, tipicamente causati da ransomware) e fig. 4.1-2 (si veda: codici maligni, che includono ransomware). Al terzo posto, non inaspettatamente, si posizione la **guerra informatica**, in inglese la cyber warfare. Al quarto posto il **sabotaggio**, considerato come probabile causa di attacchi soprattutto da piccole imprese e dagli studi professionali.

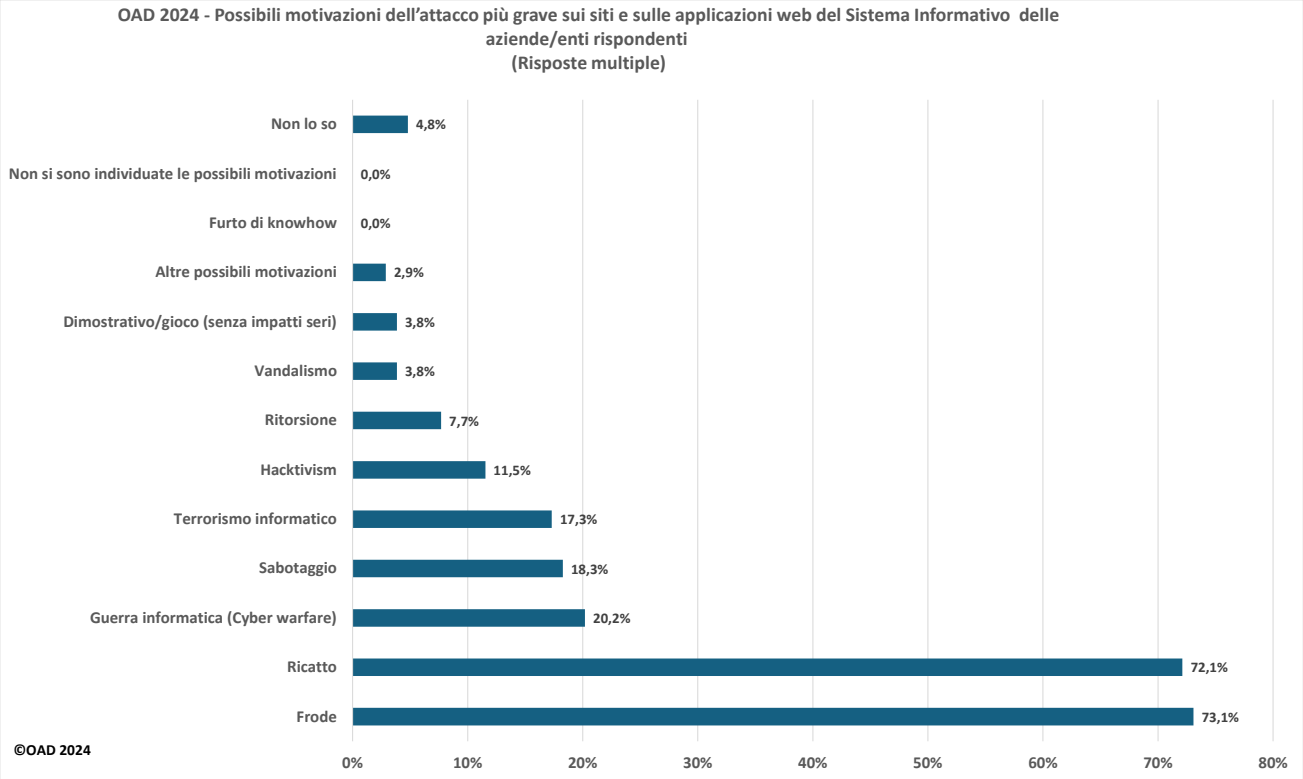


Fig. 4.2-10

I **probabili attaccanti per l'attacco più grave agli ambienti web** del SI delle aziende/enti rispondenti sono mostrati in fig. 4.2-11, con risposte multiple. La stragrande maggioranza delle risposte, con un **86,5%**, fa riferimento ad un **attacco dall'esterno**, ossia via Internet e da attaccanti il più delle volte sconosciuti. Tutti gli altri probabili attaccanti hanno percentuali molto inferiori. Al secondo ed al terzo posto si collocano i Clienti ed i Fornitori, secondo l'autore perché sono la causa degli attacchi (crescenti) alla **supply chain.**

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 un 3,8% delle/dei rispondenti non è stato in grado di determinare la provenienza dell'attacco.

La fig. 4.2-12, con risposte multiple, mostra la distribuzione percentuale, nel bacino dei rispondenti, degli **interlocutori esterni ai quali si comunica l'attacco subito**, in taluni casi anche per obblighi di legge, ad esempio all'Autorità Garante per la privacy in caso di un data breach su informazioni personali.
La stragrande maggioranza, con il **86,5%,** comunica l'accaduto **ai propri fornitori e consulenti** per farsi aiutare nel ripristinare la situazione ex ante l'attacco subito. La comunicazione alle autorità preposte, come ACN, Polizia Postale, Garante, ed altri ha percentuali assai inferiori. Quasi un 1/4, il **24%,** comunica l'attacco subito **alla Polizia Postale**, ed il **16,3% all'ACN**, soprattutto da parte delle infrastrutture critiche. Solo il **5,8%** lo comunica al **Garante della privacy**, probabilmente perché sono stati pochi i data breach e le estrazioni di dati personali. **L'8,7%** non comunica nulla a nessuno, e le motivazioni includono: per quasi il 60% perché anche il più grave attacco rilevato non è così significativo e non rientra tra quelli che per legge devono essere comunicati; per il 16,7% per motivi di immagine. Subire un attacco digitale, nella percezione comune, è riprovevole, fa presupporre (come spesso è vero) che non fossero presenti le idonee misure di sicurezza,

quindi perdita di affidabilità, autorevolezza, immagine: meglio quindi non comunicare alcuna informazione, non si sa mai che possa arrivare ai media. Qualche rispondente, di piccole e piccolissime organizzazioni, ammette di non sapere a chi e come comunicare l'attacco digitale subito. Anche se la percentuale non è elevata, ma comunque non trascurabile, questo è un chiaro indicatore della scarsa conoscenza che alcuni manager e/o addetti alla sicurezza informatica hanno di cosa occorre fare, al di là di interventi tecnici, quando si subisce un attacco digitale.

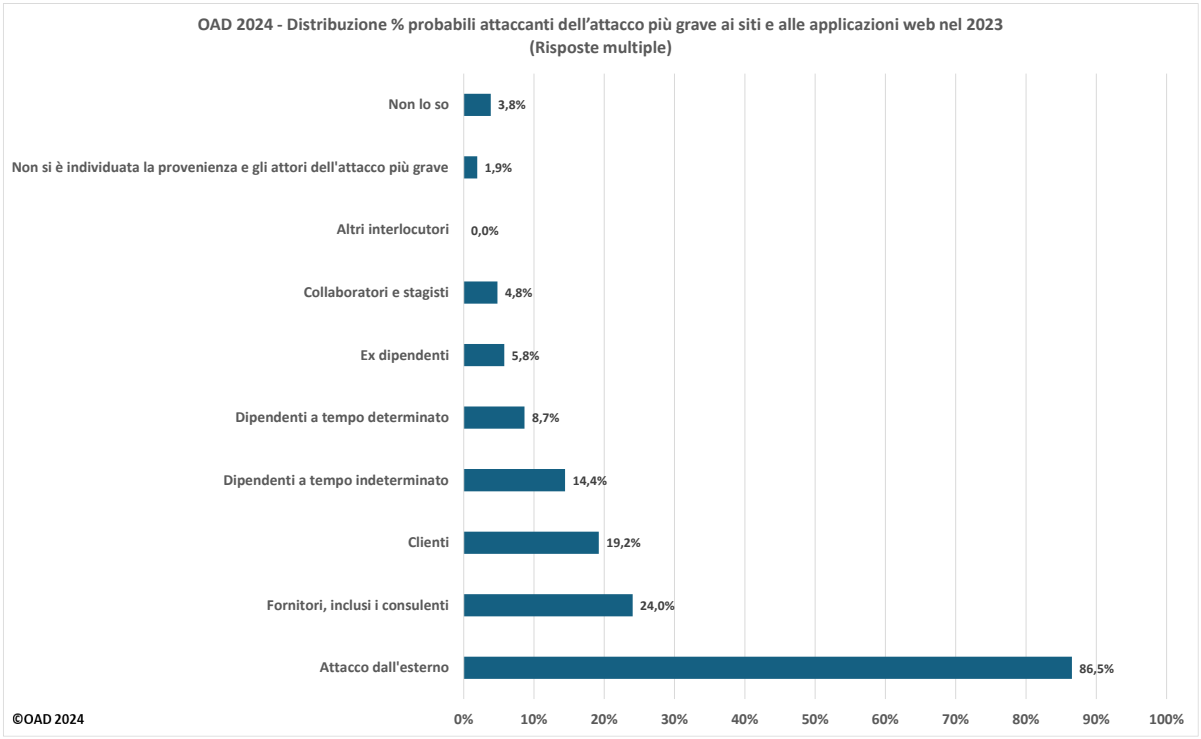


Fig. 4.2-11

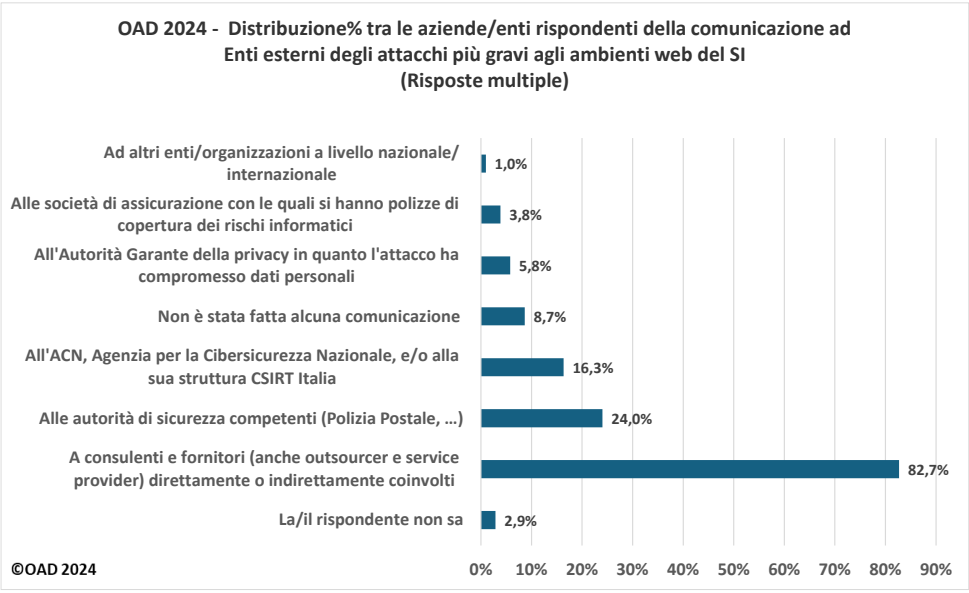


Fig. 4.2-12

La fig. 4.2-13, con risposte multiple, indica, in percentuale, la diffusione delle **principali attività intraprese dopo aver subito il più grave attacco ad ambienti web**. Al primo posto, con il **45,2%**, l'implementazione di **nuovi strumenti di sicurezza digitali**, che causano l'aumento dei costi sul budget informatico di cui in fig. 4.2-9.

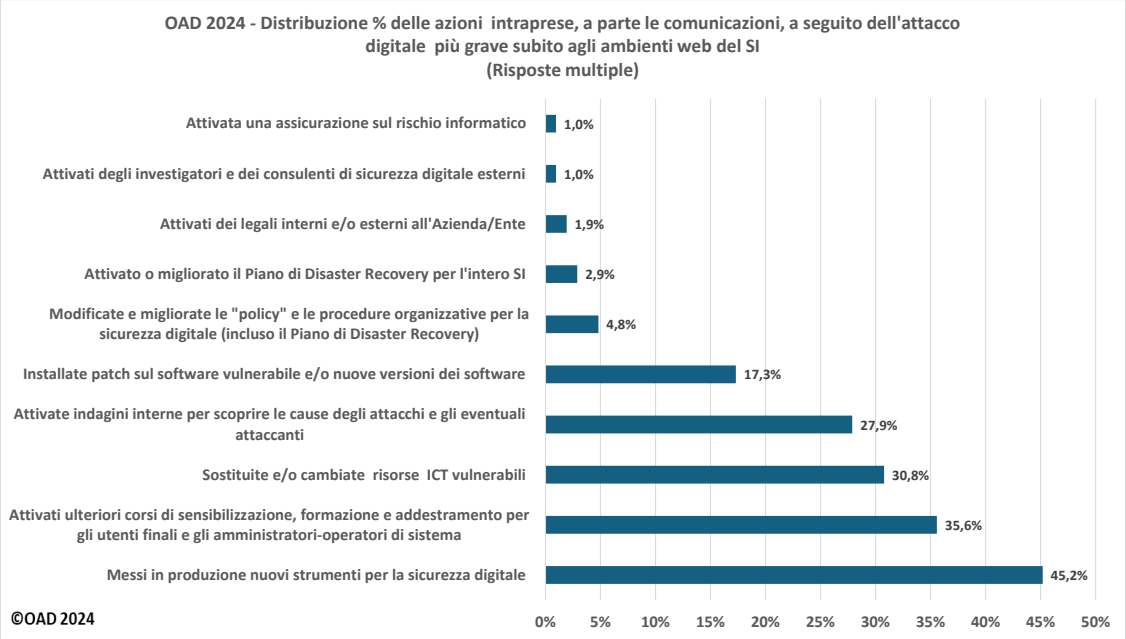


Fig. 4.2-13

Seguono a decrescere ma con percentuali significative, altri interventi sul sistema informativo, quali la sostituzione delle risorse ICT vulnerabili, gli aggiornamenti, etc. **Più di 1/3** delle aziende/enti rispondenti ha attivato ulteriori **corsi di sensibilizzazione e di formazione** sulla sicurezza digitale, che almeno in parte tende a ridurre il grave problema delle competenze digitali degli utenti, sia finali che privilegiati. Rimane sempre bassa, come nelle edizioni precedenti, la percentuale di chi ha attivato una **assicurazione sui rischi informatici**: polizze assicurative ce ne sono, ma difficili da "configurare" ed ancora con costi alti per le medie e piccole organizzazioni.

4.3 Gli attacchi digitali ai sistemi OT in Italia

Come già anticipato in §2, l'indagine OAD 2024 ha voluto effettuare anche un'indagine "verticale" sugli **attacchi digitali agli ambienti OT,** eventualmente presenti nei ed interoperanti con SI dei rispondenti.
In tutte le precedenti indagini OAD, ad eccezione di OAD 2023, gli ambiti OT erano sempre stati considerati, di volta in volta con leggere differenze di approfondimento, e prevalentemente sui sistemi di automazione della produzione. Nell'edizione OAD 2023 non sono state più poste domande sui sistemi OT, avendo verificato che nelle edizioni precedenti poche delle aziende/enti rispondenti dichiaravano di utilizzare questi sistemi; e così cercando di semplificare il questionario. Dato che ultimamente, a livello mondiale, si è riscontrato un aumento di tali attacchi, OAD 2024 ha voluto riprendere tale analisi in maniera "verticale".

Il termine **OT, Operation Tecchnology**, indica un ampio insieme di sistemi ICT per controllare, monitorare ed automatizzare processi fisici ed i dispositivi e le infrastrutture che effettuano e/o supportano tali processi

fisici. Tipici esempi di tali processi sono quelli manifatturieri, quelli chimici, quelli nucleari, quelli del controllo del territorio, delle reti di distribuzione dell'energia, del gas, dell'acqua, e così via.
I sistemi OT includono i sistemi **ICS**, Industrial Control System, i **robot** industriali e di ricerca, i sistemi **IoT**, Internet of Things e gli **IIoT**, gli Industrial IoT. I sistemi ICS includono sistemi **SCADA**, Supervisory Control And Data Acquisition, e i sistemi **DCS**, Distributed Control Systems. A livello di attuatori-controllori (dispositivi distribuiti che attuano e controllano localmente il funzionamento di un dispositivo ed inviano dati ad un sistema centrale di raccolta e di elaborazione), si usano i termini di **PLC**, Programmable Logic Controller, **PAC**, Programmable Automation Controller, **RPU**, Remote Processor Unit.

I sistemi OT non rientravano, e sovente ancora non rientrano, nell'ambito della gestione e del governo del SI, considerati come strumenti per la produzione, il più delle volte sotto il controllo della Direzione Produzione e non del CIO.
I problemi, gli incidenti e gli attacchi digitali agli ambienti OT possono riguardare non solo la sicurezza dei sistemi ICT (**security**) e del loro funzionamento, ma anche la sicurezza delle persone (**safety**) che interagiscono o che possono essere coinvolte nei processi controllati/attuati dai sistemi OT.
Data l'ampiezza e la complessità del mondo OT, per comprendere i relativi problemi di sicurezza digitale ed i possibili attacchi è opportuno introdurre, almeno a livello architetturale, come operano i sistemi OT. Le fig. 4.3-1 e 4.3-2 schematizzano esempi di funzionamento per tipici sistemi di automazione industriale. La prima mostra un esempio di riferimento sui dispositivi OT, che inizialmente operavano in maniera analogica e isolata, ed ora sono sempre più digitali e interoperanti con il SI, in una integrazione IT/OT che amplia significativamente la superficie di vulnerabilità dell'intero SI.

La fig. 4.3-2 mostra un esempio di schema ICS, dove l'acronimo OPC sta per OLE for Process Control (OLE, Object Linking and Embedding), e PID sta per Proportional-Integral-Derivative.

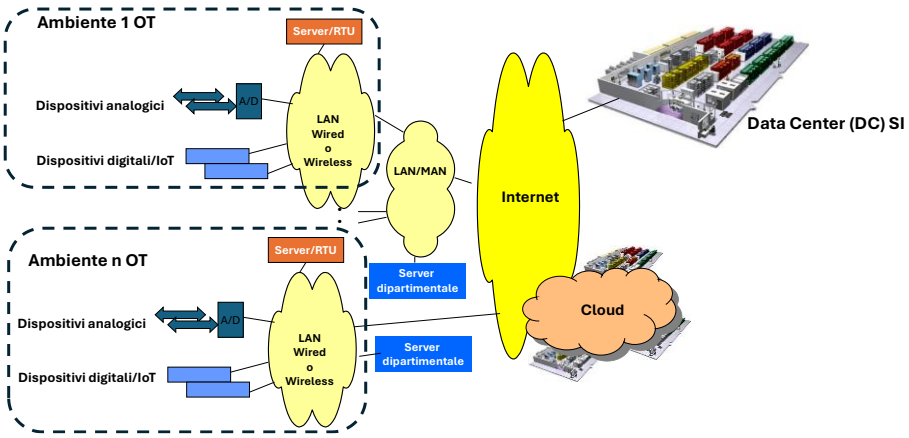


Fig. 4.3-1 (Fonte: Malabo)

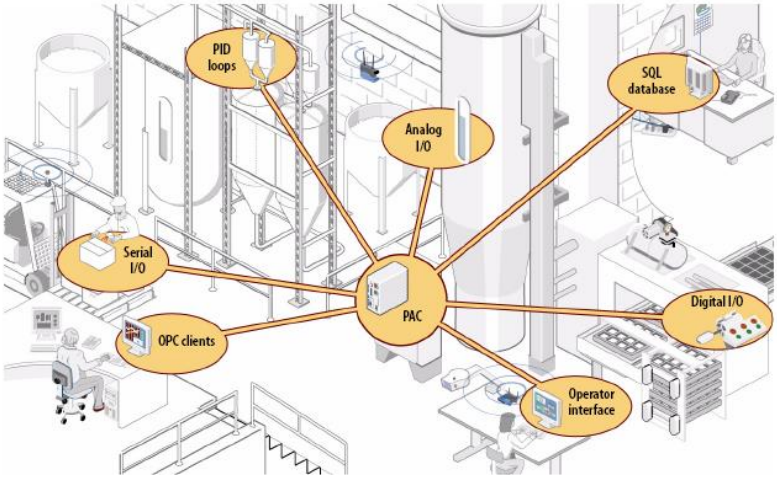


Fig. 4.3-2 (Fonte: OPTO 22)

Dopo questo inziale inquadramento, nel seguito sono analizzate le risposte avete nell'indagine.

La fig. 4.3-3 mostra che il **37%** di aziende/enti rispondenti **utilizza sistemi OT**, e la fig. 4.3-4 indica, tra questi, la percentuale **di chi ha subito attacchi** a questi sistemi: in pratica quasi la metà**, il 48,2%**.

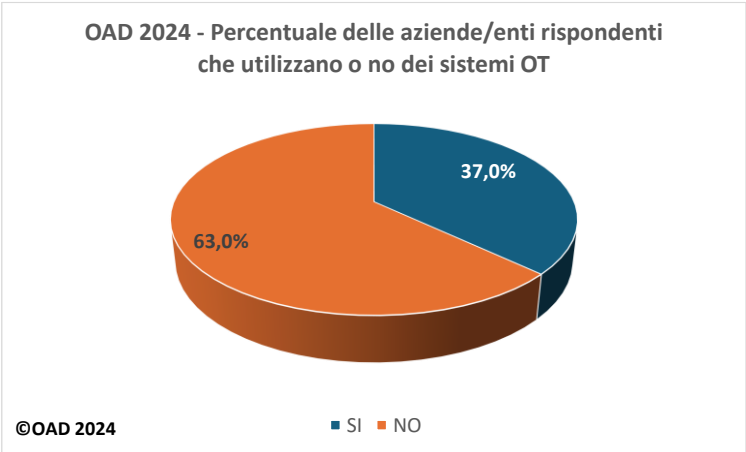


Fig. 4.3-3

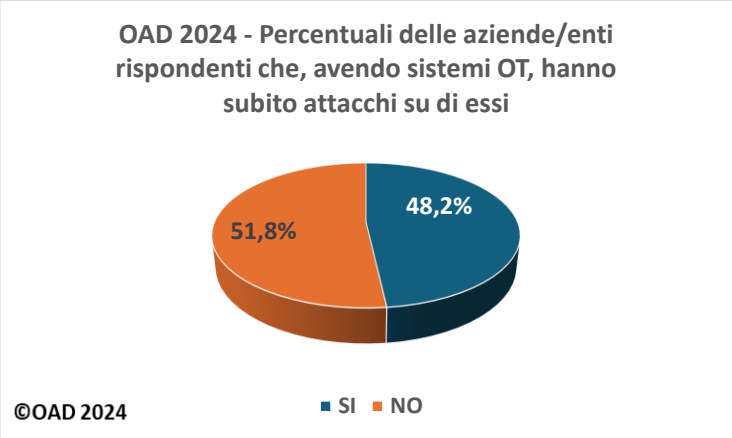


Fig. 4.3-4

La fig. 4.3-5 dettaglia, con risposte multiple, a quali dei vari tipi di sistemi OT in uso sono stati portati i più gravi attacchi. La maggior parte, **quasi il 60%**, ha riguardato **robot e sistemi robotizzati**, cui segue per il **37%** l'attacco a **sistemi SCADA**, il **33,3%** a **sistemi IoT**. Le altre tipologie di sistema hanno % inferiori a scalare.
Gli attacchi ai sistemi di **diagnosi e controllo sanitari** hanno riguardato il **7,4%** delle aziende/enti rispondenti.
Per la voce "Altri Dispositivi intelligenti" sono stati indicati chioschi informativi in villaggi turistici e sul territorio, sistemi di controllo del traffico nelle strade e sistemi per la automazione dei magazzini.

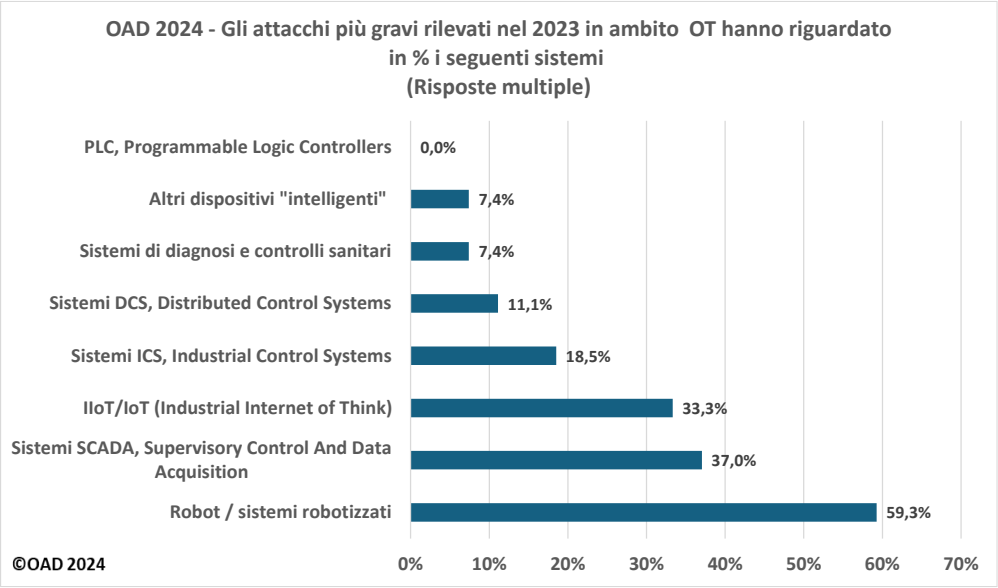


Fig. 4.3-5

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

La fig. 4.3-6, con risposte multiple, evidenzia, nell'area cerchiata in rosso, la distribuzione percentuale tra i rispondenti del livello di disservizio recato dall'attacco ritenuto più grave allo specifico sistema OT, quindi in ambito locale; il disservizio è indicato come tempo del blocco di funzionamento del sistema OT fino alla ripresa della sua attività dopo l'attacco. Tali blocchi sono stati molto alti: per circa 1/3 dei rispondenti il blocco è durato tra i 2 e 3 giorni, ma per quasi la metà è durato più di 3 giorni.
Sempre nella fig. 4.3-6, nell'area cerchiata in marrone, la distribuzione percentuale tra i rispondenti del livello di disservizio alle funzionalità dell'intero SI, o di sue parti/applicazioni, causati dal propagarsi dell'attacco e dei suoi impatti non solo locali. Dato che la maggior parte dei sistemi OT interagisce con applicazioni del SI, la propagazione dell'attacco ha causato **significativi disservizi anche sul SI**: il **40,7%** ha avuto un **blocco tra i 2 e 3 giorni**, e solo un **3,7%** un blocco durato **oltre 3 giorni**.

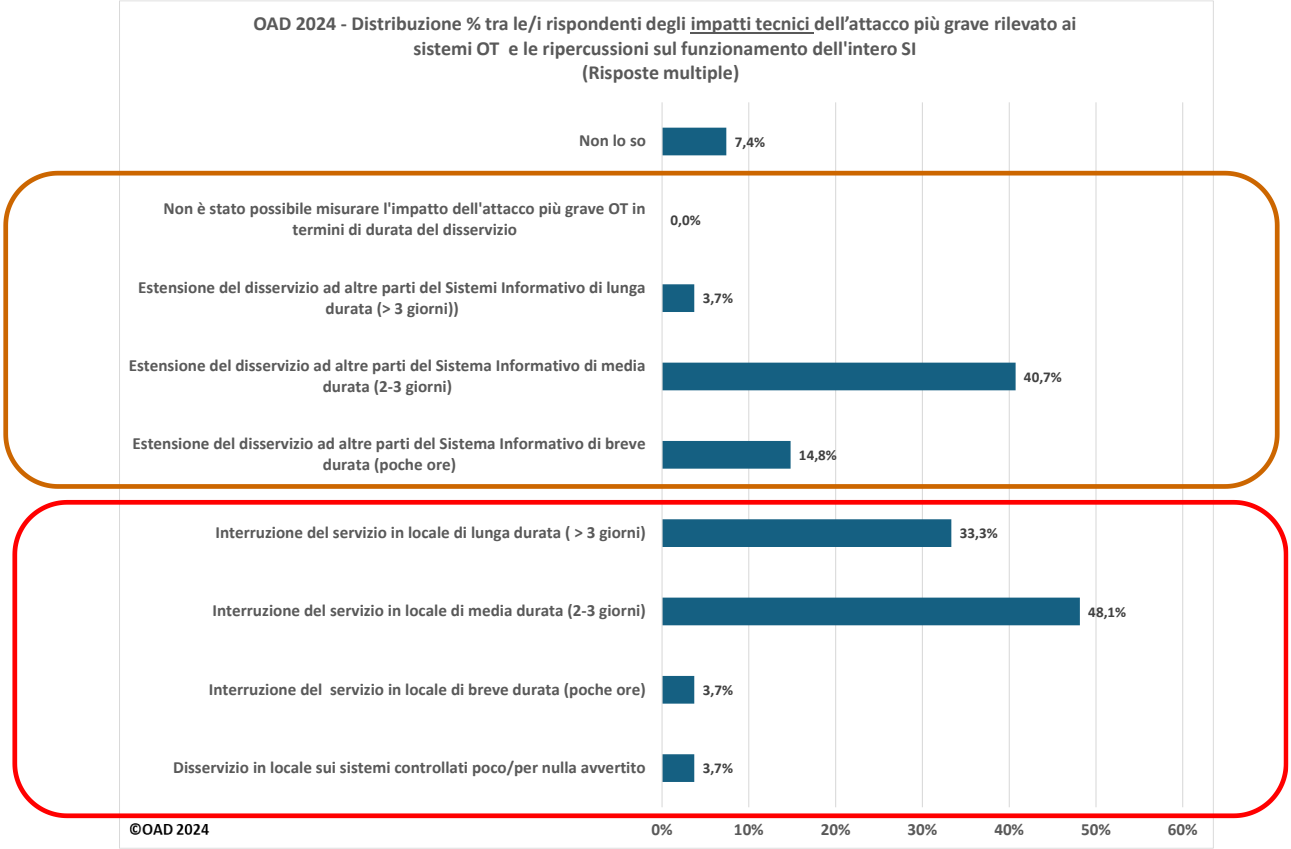


Fig. 4.3-6

Come mostrato in fig. 4.3-7, con risposte multiple, gli attacchi ai sistemi OT hanno provocato **danni economici** a chi li ha subiti: per quasi i 2/3, **il 63%**, il costo economico è stato **significativo sul budget del SI,** soprattutto per realizzare gli interventi elencati in fig. 4.3-10.
Ma solo per il **3,7%** questi costi ed i danni complessivi hanno **influito anche sul bilancio** dell'azienda/ente.

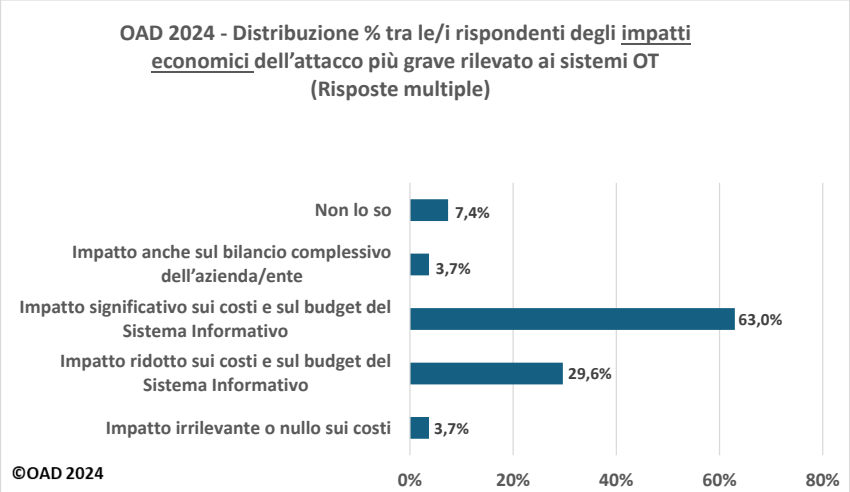


Fig. 4.3-7

Le probabili **motivazioni** per l'attacco più grave ai sistemi OT sono riportate in fig. 4.3-8, che vede al primo posto **il sabotaggio**, per **più dei 2/3 dei rispondenti**. E solo al secondo e terzo posto, e con percentuali ben inferiori, la **frode ed il ricatto**, che sono invece ai primi posti per gli attacchi ai sistemi web, come evidenziato in fig. 4.2-10. A giudizio dell'autore, quanto emerge è corretto, dato che non far funzionare i sistemi OT provoca nell'ambito manifatturiero il blocco della produzione, nella logistica il blocco del magazzinaggio, nell'ambito sanitario il blocco delle analisi mediche e degli interventi robotizzati, in altri settori merceologici il blocco di sistemi di informativa e di controllo. Effettuare tali attacchi è un sabotaggio delle attività e delle funzionalità dell'attaccato, con il primario obiettivo di danneggiarlo fortemente e di porlo, almeno temporaneamente, fuori mercato. Tra le motivazioni, il **vandalismo,** con un **25,9%,** ha un valore alto, ed anche questo, a giudizio dell'autore è un dato corretto. Infatti, ad esempio, i chioschi informativi ed i sistemi OT di controllo del territorio, tipicamente nelle Pubbliche Amministrazioni Locali non sono (e non possono essere) presidiati e sono talvolta oggetto di attacchi di vandali per il gusto di distruggere un "bene" pubblico. E forse lo possono anche fare perché istigati, e pagati, da chi vuole danneggiare facilmente qualche cosa dell'azienda/ente per motivi politici o personali.

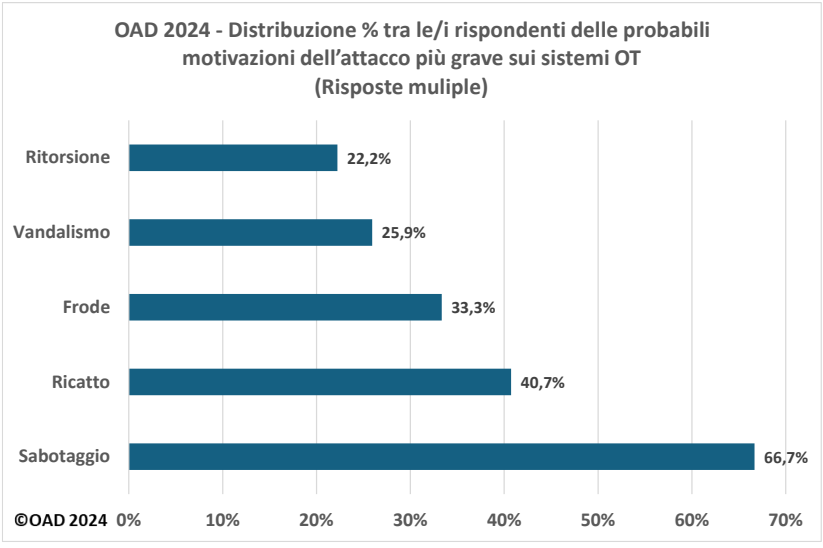


Fig. 4.3-8

La fig. 4.3-9 mostra che ben **l'81,5%** delle aziende/enti colpite dagli attacchi più gravi ai propri sistemi OT **comunica** questo fatto ai **propri fornitori e consulenti**, tipicamente per chiedere un loro intervento per la riparazione e, forse, per migliorare la loro protezione.
Rispetto agli attacchi agli ambienti web, si veda fig. 4.2-12, questa % è ben più alta, dato che l'intervento su sistemi OT è molto specialistico, e difficilmente le competenze per poterlo fare sono all'interno dell'azienda/ente colpita.
Percentuali assai inferiori per la denuncia alla Polizia Postale o all'ACN, probabilmente per le poche aziende/enti obbligati per legge o dalle polizze assicurative a tali comunicazioni.

La fig. 4.3-10, con risposte multiple, mostra, distribuiti percentualmente, gli **interventi che l'attaccato richiede ed effettua dopo aver subito l'attacco più grave**.
Congruentemente con la comunicazione di cui alla figura precedente, al **primo posto,** con un **70,4%** la richiesta di interventi **a fornitori e consulenti**, cui seguono con % alte la **sostituzione (e/o l'aggiornamento) delle risorse ICT vulnerabili** (66,7%) e con il **medesimo 37%** la messa in produzione di **nuovi strumenti di sicurezza** e **l'attivazione di indagini interne** per individuare le cause e gli attori dell'attcco. Nella voce "Altro", con un **18,5%** significativo, le/i rispondenti hanno indicato la formazione e l'addestramento degli utenti e degli amministratori dei sistemi OT.

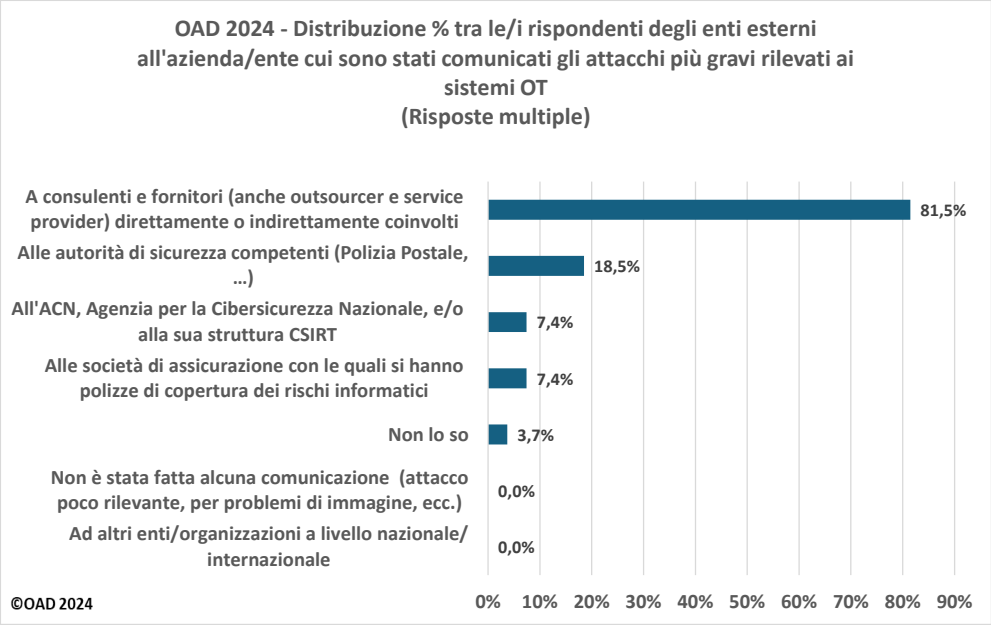


Fig. 4.3-9

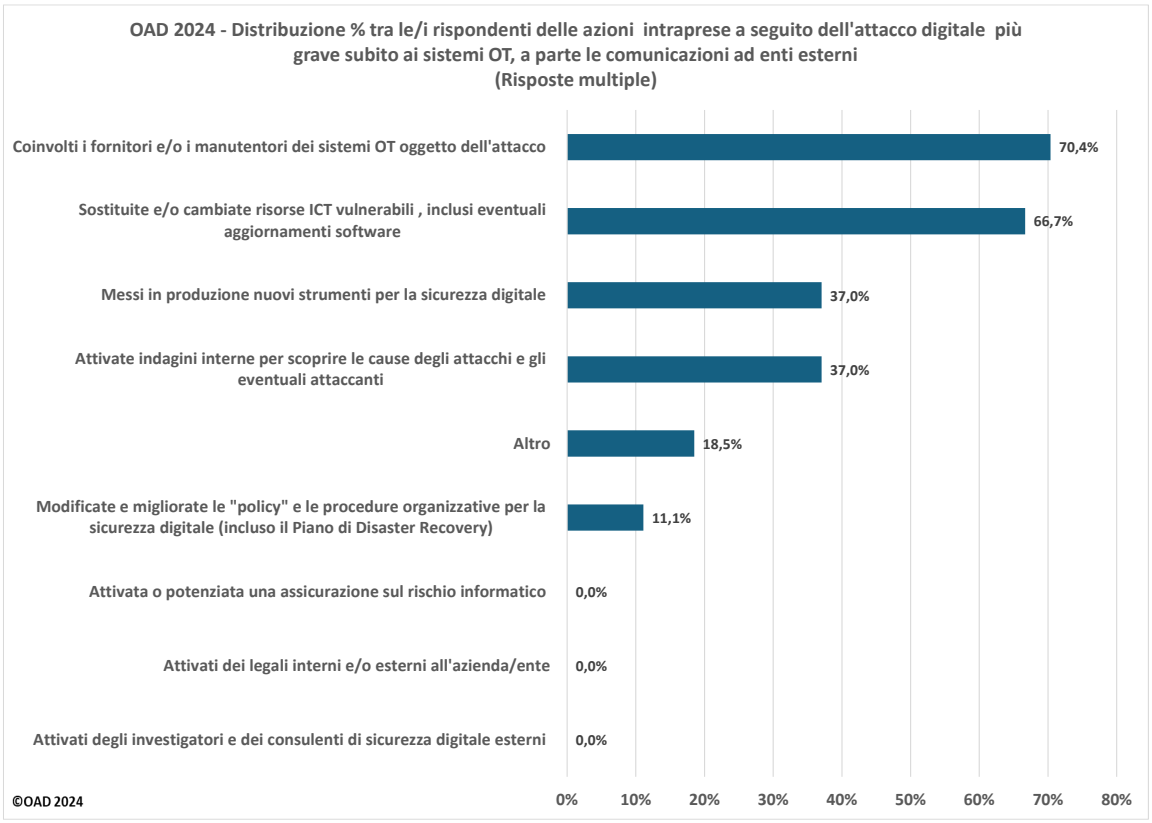

OAD 2024 - Distribuzione % tra le/i rispondenti delle azioni intraprese a seguito dell'attacco digitale più grave subito ai sistemi OT, a parte le comunicazioni ad enti esterni
(Risposte multiple)
Coinvolti i fornitori e/o i manutentori dei sistemi OT oggetto dell'attacco
70,4%
Sostituite e/o cambiate risorse ICT vulnerabili , inclusi eventuali aggiornamenti software
66,7%
Messi in produzione nuovi strumenti per la sicurezza digitale
37,0%
Attivate indagini interne per scoprire le cause degli attacchi e gli eventuali attaccanti
37,0%
Altro
18,5%
Modificate e migliorate le "policy" e le procedure organizzative per la sicurezza digitale (incluso il Piano di Disaster Recovery)
11,1%
Attivata o potenziata una assicurazione sul rischio informatico
0,0%
Attivati dei legali interni e/o esterni all'azienda/ente
0,0%
Attivati degli investigatori e dei consulenti di sicurezza digitale esterni
0,0%
©OAD 2024
0%
10%
20%
30%
40%
50%
60%
70%
80%

Fig. 4.3-10

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

Come indicato nel questionario online, come "prossimo" futuro è considerato l'arco temporale dalla fine del 2024 alla fine del 2026.

Come già evidenziato in §4.1 e nell'Allegato A, OAD distingue nettamente le tipologie di attacco, ossia che cosa si attacca, dagli strumenti di attacco. Questa logica viene applicata anche per richiedere quali sono gli attacchi più temuti nel prossimo futuro 2024-2026, e tendenzialmente le risposte sono influenzate, per le/i rispondenti, dagli attacchi subiti nel 2023.

La fig. 5-1, con risposte multiple, mostra che per quasi la metà dei rispondenti, il **49,6%**, la tipologia di attacco più temuta nel prossimo futuro è data dalle "**Modifiche non autorizzate ai dati e alle informazioni trattate dal sistema informativo**". E' in effetti l'attacco più grave dato che va ad alterare i dati trattati dal SI, dati che costituiscono un "asset", un bene aziendale tra i più essenziali nell'attuale era della società digitale. Percentualmente seguono, con il **40,2%**, il più generale "**Uso non autorizzato di risorse ICT**" e con il **31,7%** sia la "**Saturazione delle risorse ICT"** sia le "**Modifiche non autorizzate ai programmi applicativi e di sistema, e alle configurazioni**". Queste due ultime tipologie di attacco sono ai primi due posti degli attacchi più diffusi nel 2023 ai SI dei rispondenti, come indicato nella fig. 4.1-1, e tra le tipologie di attacco più usate per cyber warfare, soprattutto con attacchi DDoS e con ransomware.
Nella fig. 5-1 emergono alcuni dati che l'autore ritiene opportuno commentare.

- L'attacco alla **supply chain,** tipologia introdotta per la prima volta nel questionario OAD 2024, raggiunge un significativo **26%** (nella fig. 4.1-1 sugli attacchi rilevati nel 2023 è al **15%**), che conferma la criticità di questo attacco individuato tra i primi più gravi rischi del futuro da ENISA, come commentato in §3.1.
- Altrettanto alto, con un **26,8%**, il **furto "fisico"** di apparati fisici ICT , sia fissi che mobili, dai quali si può da un lato **estrarre dati** utili per ulteriori attacchi o per rivenderli sul mercato nero (si consideri il **30,1%** per il **furto di informazioni da sistemi mobili** ed il **27,2% da quelli fissi**, e si tenga presente che le informazioni si possono rubare dai sistemi ICT con varie tecniche, oltre che con il furto dell'hardware); e dall'altro si può rivendere i dispositivi ICT sul mercato dell'usato, nel quale il valore di moderni smartphone è alto.
- Rimane abbastanza alto, con un **24%**, il timore di attacchi ai **propri sistemi ICT terziarizzati**, soprattutto in cloud. Anche i principali provider di hosting e cloud, a livello mondiale, hanno subito attacchi digitali nonostante le potenti misure di sicurezza in essere, In Italia sono presenti numerosi provider di ben più piccole dimensioni, molti dei quali non hanno misure paragonabili a quelle dei "big". Rimane quindi abbastanza alto, e giustificato, il timore di attacchi ai provider tali da impattare le proprie parti di SI terziarizzate.
- Risulta irrisorio il timore **di attacchi ai sistemi in blockchain**: questa percentuale così bassa è dovuta al fatto che nel bacino delle aziende/enti rispondenti, pochissime usano sistemi in blockchain.
- Nella voce "Altro" i rispondenti hanno tutti indicato il timore di **attacchi ai sistemi di Intelligenza Artificiale** (IA) in uso.

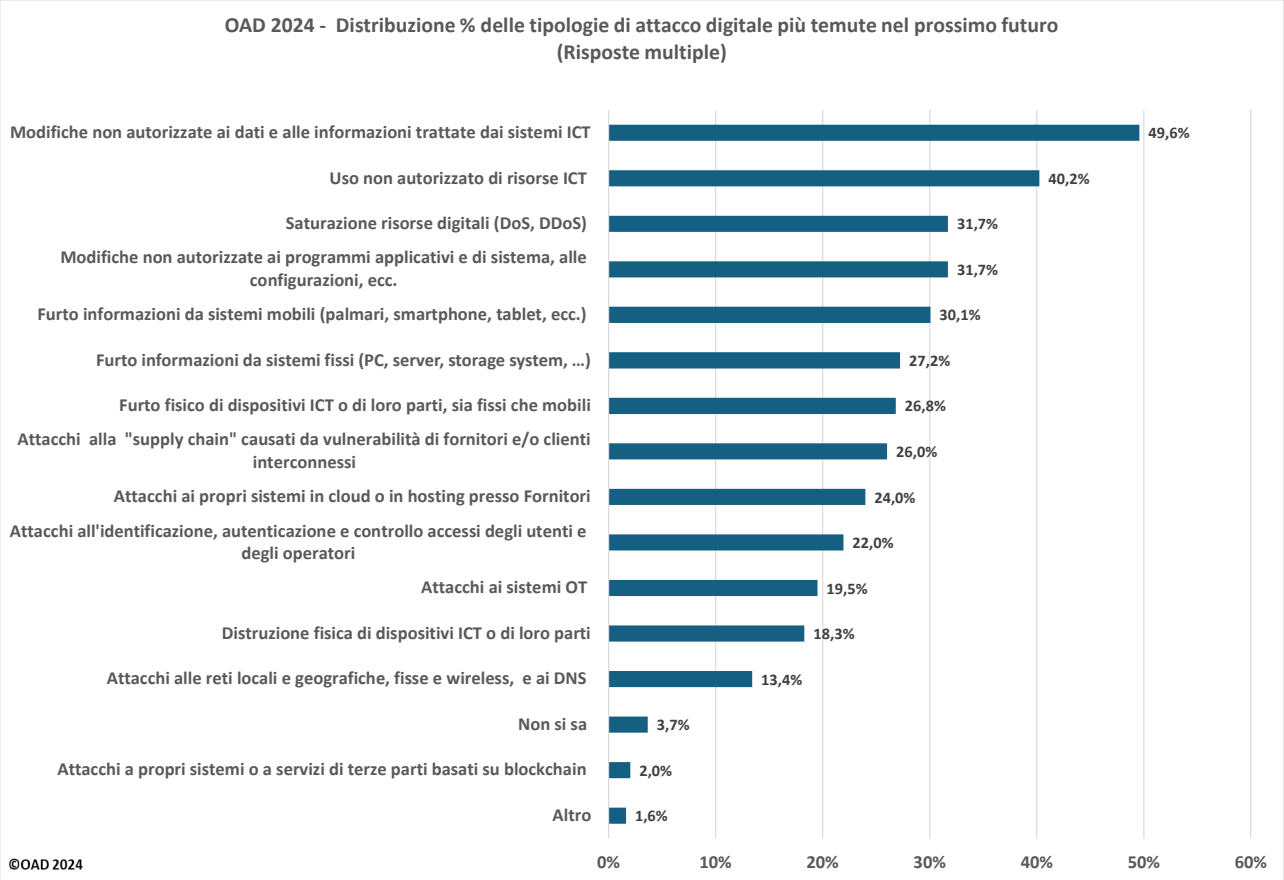


Fig. 5-1

La fig. 5-2, con risposte multiple, mostra **le famiglie di tecniche di attacco** più temute per il prossimo futuro. **Al primo posto**, per più della metà delle/dei rispondenti, "**l'utilizzo di più tecniche**", come ormai avviene per la maggior parte degli attacchi digitali. **Al secondo posto**, con il **47,6%**, la raccolta non autorizzata di informazioni, quale ad esempio il social engineering, che costituisce uno dei principali entry point per un attacco. Le altre tecniche seguono a scalare ma con valori % di circa la metà rispetto alle prime due. Al terzo posto, con un **24,8%**, si pone **l'uso di script e di programmi maligni**, nei quali rientrano i malware e ransomware.
Le famiglie di tecniche d'attacco più temute ai primi 3 posti sono le stesse, e nello stesso ordine pur con percentuali diverse, di quelle rilevate per tutti gli attacchi digitali, si veda fig. 4.1-2.
Nella voce "**Altro**", con un **13,4%** non trascurabile, le/i rispondenti hanno indicato l'uso di **nuove tecniche d'attacco basate sull'Intelligenza Artificiale**.

La fig. 5-3, con risposte multiple, evidenzia le **possibili motivazioni** che le/i rispondenti ipotizzano per gli attacchi digitali del prossimo futuro.
In cima alla lista **le frodi**, con un **67,5%** (nelle quali si includono i ricatti), seguite con un **41,1%** dal **sabotaggio.** Al terzo e 4 posto si trovano **l'hacktivism,** con il **31,3%** e la **guerra informatica,** con un **23,6%.** Percentuali abbastanza alte, considerando che il campione emerso di aziende/enti rispondenti è per la maggior parte di piccole realtà.
Questo indica che per il futuro le aziende/enti rispondenti iniziano ad essere preoccupate, oltre che da attacchi causati da frodi, ricatti e sabotaggi, anche da quelli causati dall'attivismo ideologico (che talvolta sconfina nel fanatismo) e dalle guerre informatiche che si stanno ampliando con le crescenti tensioni geopolitiche a livello mondiale e dalle guerre in atto, che a loro volta stanno estendendosi. (in particolare quella in Medio Oriente).

Hacktivism e guerre informatiche possono infatti effettuare attacchi “di massa”, come in qualche misura è stato fatto da gruppi filo-russi con attacchi ransomware.

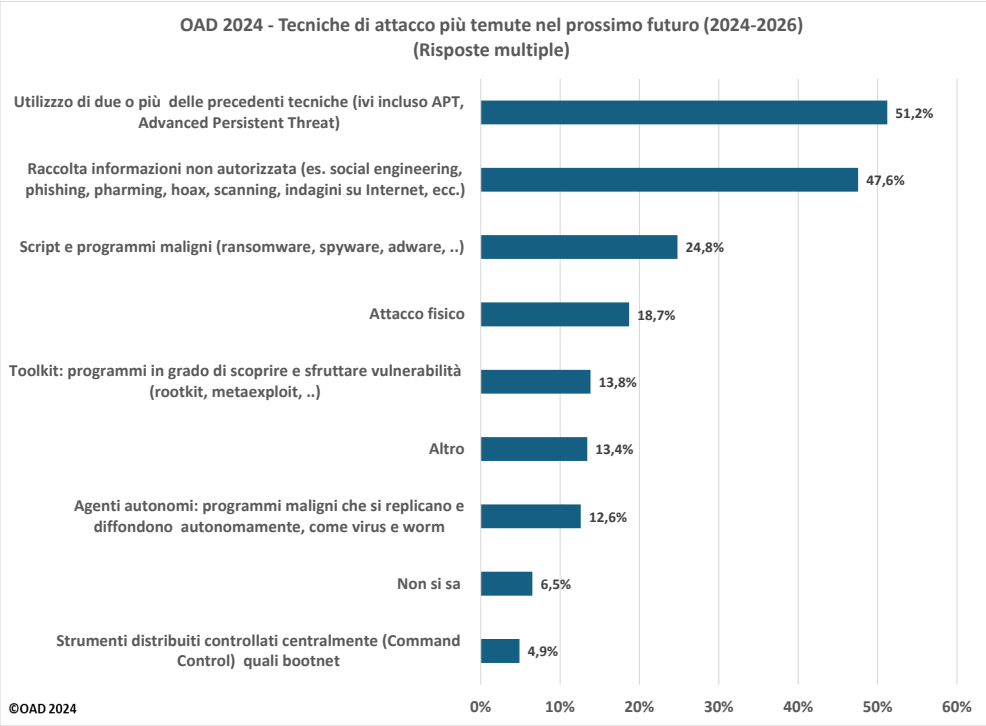


Fig. 5-2

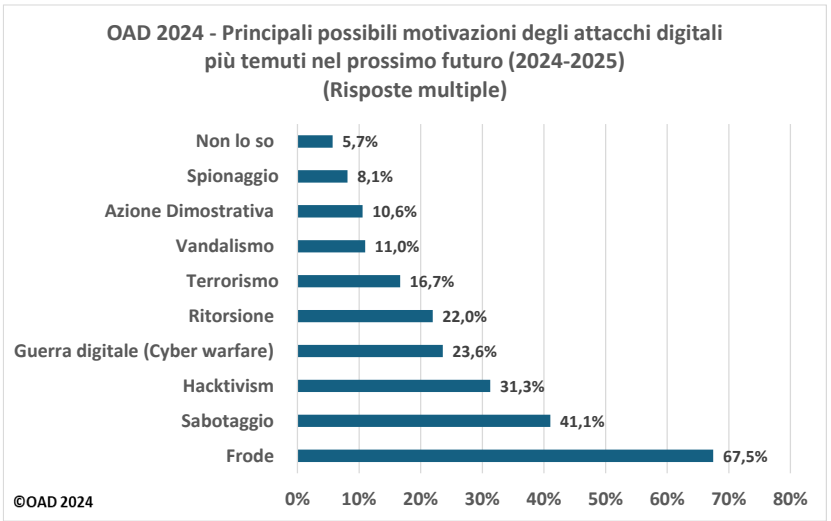


Fig. 5-3

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

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

Le risposte avute al questionario OAD 2024 sono state 345, in piccolissima crescita rispetto all'edizione precedente, e in leggera crescita rispetto alle più vecchie edizioni OAD, ma sostanzialmente dello stesso ordine di grandezza. Questo nonostante un ampio numero di associazioni patrocinanti OAD 2024, di cui molte sono state attive nella promozione presso i loro associati.
Si è comunque superato il minimo numero di risposte necessarie perché l'indagine via web abbia valore e sia, almeno come trend, paragonabile a quelle degli anni precedenti**.**

La Tabella in fig 6-1 mostra i raggruppamenti dei settori merceologici considerati nelle indagini OAD, che fanno riferimento alla classificazione ATECO[41], sulla cui base si sono raggruppati alcune classi e alla quale si sono aggiunte le Pubbliche Amministrazioni Centrali **(PAC)** e Locali **(PAL)**.

1.	Settore primario: agricoltura, allevamento, pesca, estrazione (Codici Ateco A e B)
2.	Industria manifatturiera e costruzioni: meccanica, chimica, farmaceutica, elettronica, alimentare, edilizia, ecc. (Codici Ateco C e F)
3.	Utility: Acqua, Energia, Gas ecc. (Codici Ateco D ed E)
4.	Commercio all'ingrosso e al dettaglio, incluso quello di apparati ICT (Codici Ateco G)
5.	Trasporti e magazzinaggio (Codice Ateco H)
6.	Attività finanziarie ed assicurative: assicurazioni, banche, istituti finanziari, broker, intermediazione finanziaria, ecc. (Codice Ateco M)
7.	Servizi turistici, di alloggio e ristorazione: agenzie di viaggio, tour operator, hotel, villaggi turistici, campeggi, ristoranti, bar, etc. (Codice Ateco I e N79)
8.	Attività artistiche, sportive, di intrattenimento e divertimento: teatri, biblioteche, archivi, musei, lotterie, case da gioco, stadi, piscine, parchi, discoteche, etc. (Codice Ateco R)
9.	Stampa e servizi editoriali (Codice Ateco J58)
10.	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)
11.	Servizi ICT: consulenza, produzione software, service provider ICT, gestione Data Center, servizi assistenza e riparazione ICT, etc. (Codici Ateco J62, J63, S95.1)
12.	Telecomunicazioni e Media: produzione musicale, televisiva e cinematografica, trasmissioni radio e televisive, telecomunicazioni fisse e mobili (Codici Ateco J59, J60, J61)
13.	Sanità e assistenza sociale: ospedali pubblici o privati, studi medici, laboratori di analisi, etc. (Codice Ateco Q)
14.	Istruzione: scuole e università pubbliche e private (Codice Ateco P)
15.	Associazioni, associazioni imprenditoriali e sindacati (Codice Ateco S94)
16.	PAC, Pubblica Amministrazione Centrale
17.	PAL, Pubblica Amministrazione Locale

Fig. 6-1

[41] 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

6.1 L'Azienda/Ente rispondente

La fig. 6.1-1 riporta i 22 settori merceologici considerati nel questionario OAD 2024, incluse le Pubbliche Amministrazioni.
Si sono considerati separatamente i "Service Provider ICT" rispetto a tutte le altre categorie attinenti il **mondo ICT,** ed anche alcune sotto-categorie con numerosi associati della categoria "**Servizi professionali e di supporto alle imprese**", come quelle degli avvocati, dei notai, dei commercialisti, degli amministratori di condominio**.**
Queste distinzioni avevano l'obiettivo di facilitare e stimolare la compilazione del questionario OAD 2024 per queste aziende e per questi professionisti, per poter poi effettuare delle analisi più specifiche per i loro settori merceologici. Il non raggiungimento di un numero significativo di compilazioni del questionario per questi settori, come anche per gli altri, non ha consentito di effettuare delle analisi settoriali.

Service Provider hosting/cloud (Codice Ateco J 63.11.30) (AO01)
Altri servici ICT, esclusi Provider hosting/cloud: consulenza, produzione software, servizi assistenza e riparazione ICT, etc. (Codici Ateco J62, J63, S95.1) (AO02)
Settore primario: agricoltura, allevamento, pesca, estrazione (Codici Ateco A e B) (AO03)
Industria manifatturiera e costruzioni: meccanica, chimica, farmaceutica, elettronica, alimentare, edilizia, etc. (Codici Ateco C e F) (AO04)
Utility: Acqua, Energia, Gas, etc. (Codici Ateco D ed E) (AO05)
Commercio all'ingrosso e al dettaglio, incluso quello di apparati ICT (Codici Ateco G) (AO06)
Trasporti e magazzinaggio (Codici Ateco H) (AO07)
Attività finanziarie ed assicurative: assicurazioni, banche, istituti finanziari, broker, intermediazione finanziaria, etc. (Codici Ateco M) (AO08)
Servizi turistici, di alloggio e ristorazione: agenzie di viaggio, tour operator, hotel, villaggi turistici, campeggi, ristoranti, bar, etc. (Codici Ateco I e N79) (AO09)
Attività artistiche, sportive, di intrattenimento e divertimento: teatri, biblioteche, archivi, musei, lotterie, case da gioco, stadi, piscine, parchi, discoteche, etc. (Codici Ateco R) (AO10)
Stampa e servizi editoriali (Codici Ateco J58) (AO11)
Telecomunicazioni e Media: produzione musicale, televisiva e cinematografica, trasmissioni radio e televisive, telecomunicazioni fisse e mobili (Codici Ateco J59, J60, J61) (AO12)
Sanità e assistenza sociale: ospedali pubblici o privati, studi medici, laboratori di analisi, etc. (Codici Ateco Q) (AO13)
Istruzione: scuole e università pubbliche e private (Codici Ateco P) (AO14)
Associazioni, associazioni imprenditoriali e sindacati (Codici Ateco S94) (AO15)
PAC, Pubblica Amministrazione Centrale (AO16)
PAL, Pubblica Amministrazione Locale (AO17)
Avvocati (Servizi Professionali Codice Ateco 6.9.10.10) (AO18)
Amministratori di condominio (Servizi Professionali Codice Ateco 68.32.00) (AO19)
Commercialisti (Servizi Professionali Codice Ateco 6.9.20.11) (AO20)
Notai (Servizi Professionali Codice Ateco 6.9.10.20) (AO21)
Altri Servizi professionali e di supporto alle imprese: attività immobiliari, consulenza imprenditoriale, ricerca scientifica, noleggio, call center, etc. (Codici Ateco L, M, N77, N78, N80, N81, N82) (AO22)

Fig. 6.1-1

La fig. 6.1-2 mostra la distribuzione percentuale dei rispondenti per le macro famiglie di settori merceologici considerati. E mostra alcune importanti novità rispetto alle edizioni precedenti.
Al primo posto si posiziona il settore dell'**Istruzione**, con un **23,59%**, grazie soprattutto alla promozione per la compilazione del questionario fatta da AICA, che ha collaborato ed ha patrocinato l'indagine. Nelle precedenti edizioni di OAD il primo posto dei settori rispondenti era quasi sempre dei "Servizi ICT", che talvolta si alternava con quello della "Industria manufatturiera e costruzioni", più spesso al secondo posto.
Il settore **Servizi ICT** si posiziona al secondo posto in OAD 2023, con **un 13%** se si sommano i "Service Provider hosting/cloud" con gli "Altri servizi ICT". Sia gli uni che gli altri sono stati poco partecipi nella compilazione del questionario 2024, nonostante il patrocinio di Anitec-Assinform.
Dopo di loro si posiziona il settore **Servizi professionali e di supporto alle imprese** con un **12,3%**, che somma anche le sottocategorie degli avvocati, dei notai, dei commercialisti, degli amministratori di condominio che singolarmente hanno contribuito con troppe poche compilazioni perché potessero essere analizzate a sé stante. Segue poi con quasi un **11%** il settore della **Industria manufatturiera e costruzioni.**
Tutti gli altri settori merceologici considerati hanno avuto delle aziende/enti che hanno compilato il questionario, grazie soprattutto allo sforzo promozionale di AIPSI e di alcune associazioni patrocinanti, ma ottenendo percentuali sul totale dal 5% in giù.

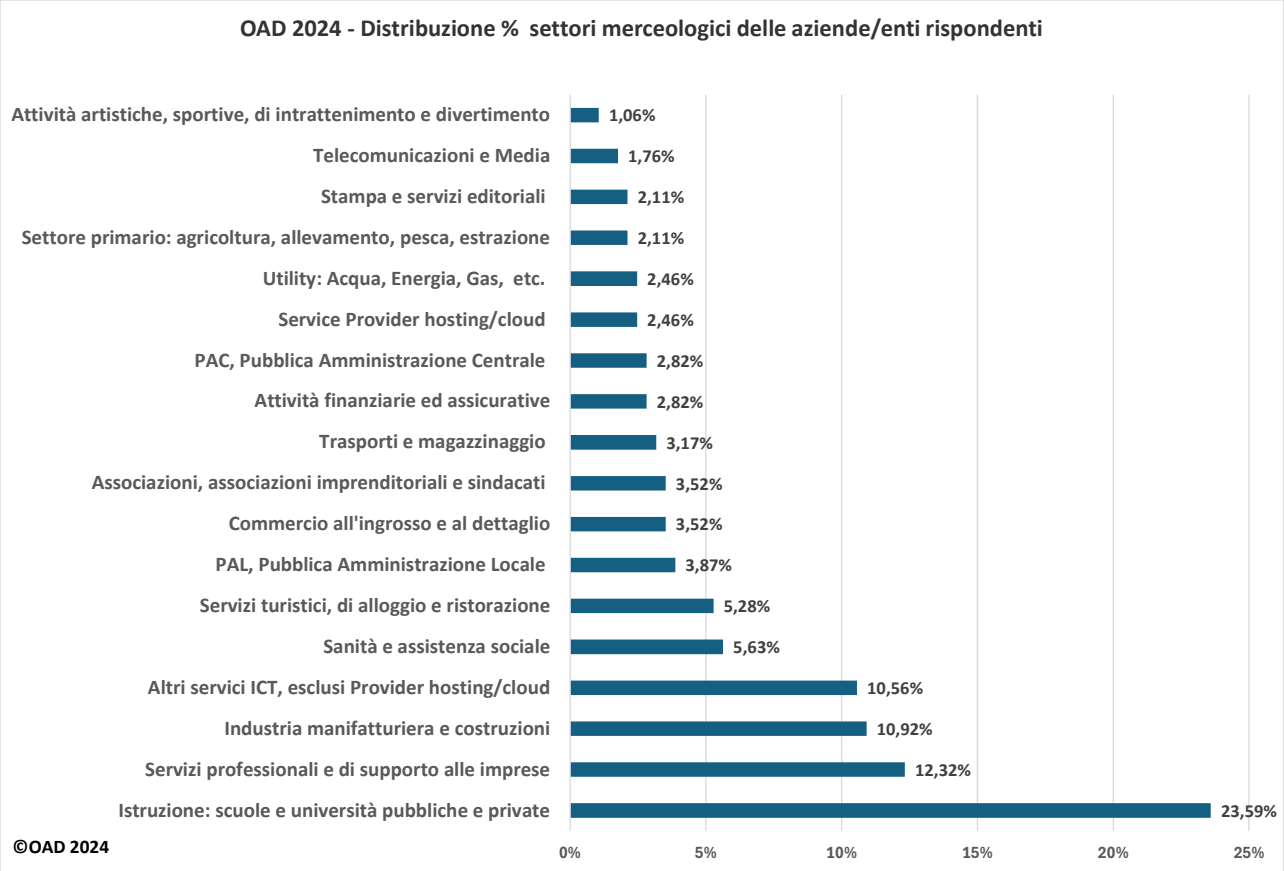


Fig. 6.1-2

Per le PAL, il **72,7%** di quelle che hanno risposto (il 3,87% sul totale) sono **Comuni** di ogni dimensione, dalle città metropolitane ai piccoli comuni, il **18,2%** sono **Regioni ed enti regionali**, il **9,1% Provincie ed enti provinciali**.
Volutamente non si è voluto considerare un dettaglio analogo per le PAC, il 2,82% sul totale, perché altrimenti sarebbero potute essere individuate singolarmente, ledendo il principio di anonimità garantito da OAD.

Per le dimensioni di un'organizzazione per numero di addetti, come per le ultime edizione di OAD il questionario 2024 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. 6.1-3 mostra la ripartizione percentuale delle aziende/enti rispondenti in base al numero dei loro dipendenti. Hanno risposto il **69,8%** di **piccole e medie organizzazioni**, ossia quelle con meno di 250 dipendenti (le PMI, Piccole Medie Imprese, in ambito aziende private). Significativa, con un **22,9%**, la presenza tra queste delle piccolissime organizzazioni con **meno di 10 dipendenti**, che, come indicato in §3.7.1, costituiscono la stragrande maggioranza delle imprese, private e pubbliche, in Italia.

Tale ripartizione è confermata anche dalla correlazione tra aziende/enti rispondenti e loro fatturato (per le PA le entrate del loro ultimo bilancio)[42], i cui risultati sono in fig. 6.1-4. A parte il 38,1% dato da aziende/enti che non possono/vogliono fornire questo dato, pur con la totale anonimità garantita da OAD, il **21,5%** ha un fatturato **sotto il milione di Euro**, cifra che include gran parte delle piccole e piccolissime aziende.

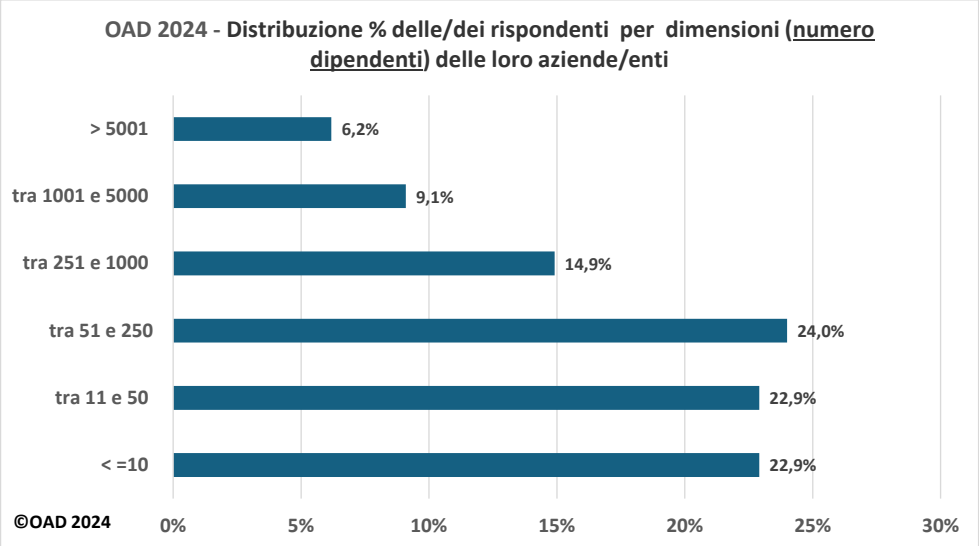


Fig. 6.1-3

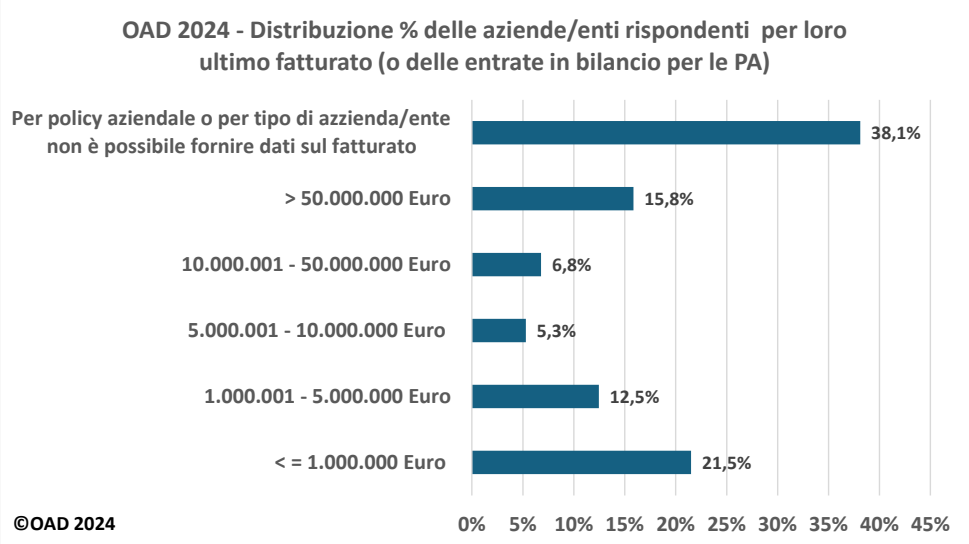


Fig. 6.1-4

[42] OAD 2024 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 €.

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 suo SI (per questo tema si veda fig. 6.2-2).
Come mostrato nella fig. 6.1-5, quasi il **90%** delle aziende/enti rispondenti **opera prevalentemente in Italia**, e solo il **10%** circa **anche all'estero**.

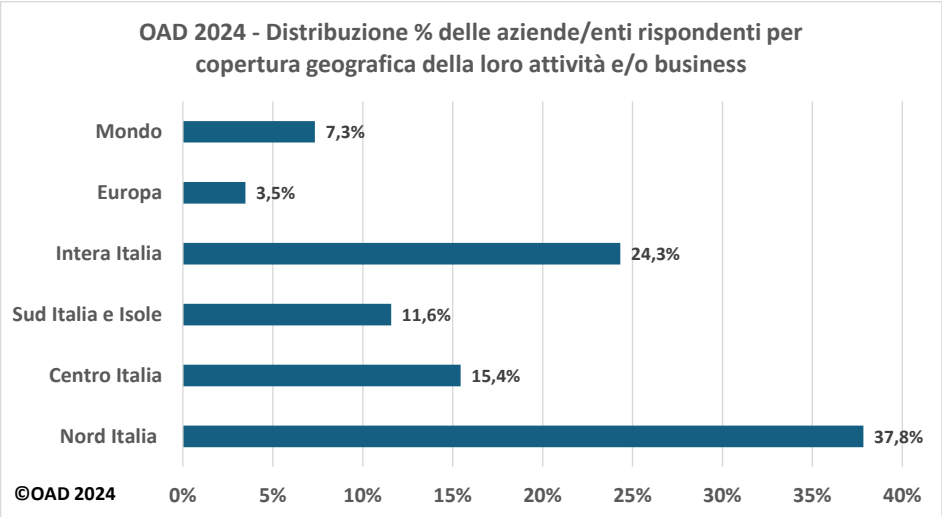


Fig. 6.1-5

6.2 Tipologia, ruolo e principali caratteristiche dei sistemi informativi

La fig. 6.2-1 mostra che il Sistema Informativo (SI) è **gestito e controllato totalmente in Italia** per l'**85,4%** delle aziende/enti rispondenti, e per il **63,4%** è di **piccole-medie dimensioni** senza un Data Center. Quest'ultima è la caratteristica tipica di un SI di una piccola o media organizzazione, che costituiscono la stragrande maggioranza in Italia.

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

La fig. 6.2-2 mostra, come distribuzione percentuale delle risposte avute, dove è situato a livello regionale in Italia la sede principale del SI, sia essa un Data Center o una computer room "primaria".
Grazie ai vari e ripetuti solleciti di AIPSI, l'indagine OAD 2024 è riuscita a coprire tutte le regioni d'Italia, ma la **maggior parte dei "centri" dei SI** delle aziende/enti rispondenti è in **Lombardia** e in **Lazio**.

Per comprendere il fabbisogno di sicurezza digitale per il SI oggetto delle risposte (necessario anche per effettuare la macro valutazione del livello di sicurezza del SI oggetto delle risposte al questionario), è stato chiesto, a livello qualitativo, quale è l'importanza del SI, e quindi della sua sicurezza, per il business e per le attività dell'azienda/ente rispondente.

La fig. 6.2-3 evidenzia che per il **70,1%** delle aziende/enti rispondenti **il SI è essenziale** per il funzionamento delle loro attività e dei loro processi, e pertanto la sua sicurezza digitale dovrebbe essere di alto livello e allo stato dell'arte. **P**er il**8,8%** il **SI** è solo di "**supporto**" all'operatività dell'azienda/ente, e questo anche se il 69,8% delle organizzazioni rispondenti sono di piccole e medie dimensioni, come mostrato in fig. 6.1-3.

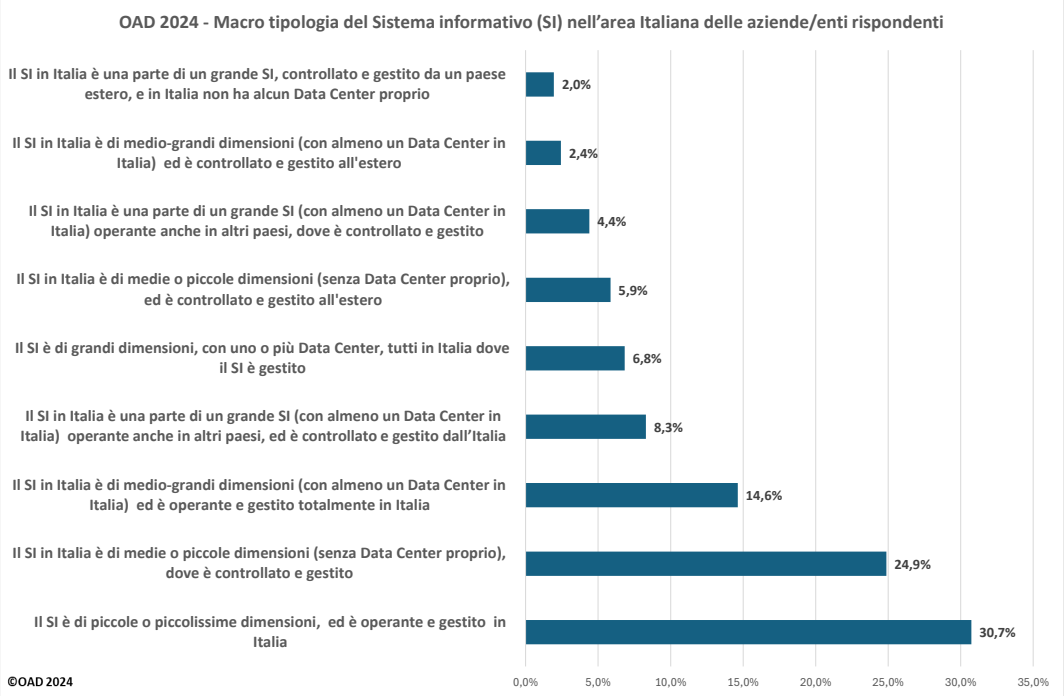


Fig. 6.2-1

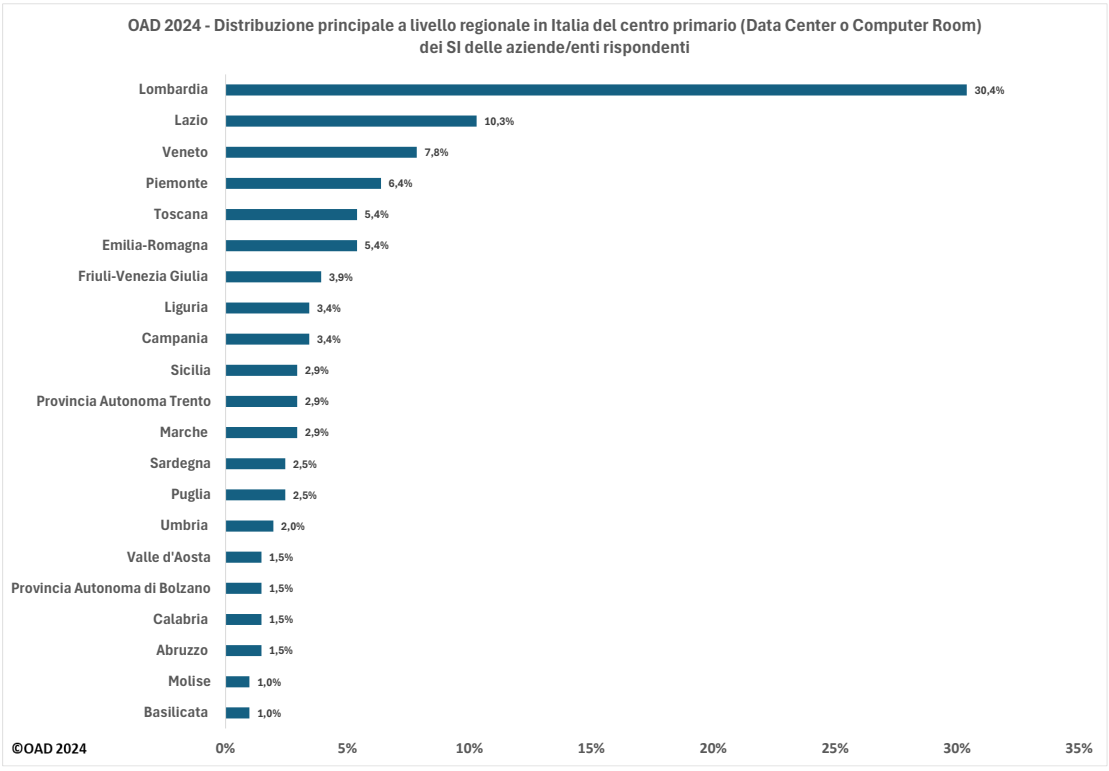


Fig. 6.2-2

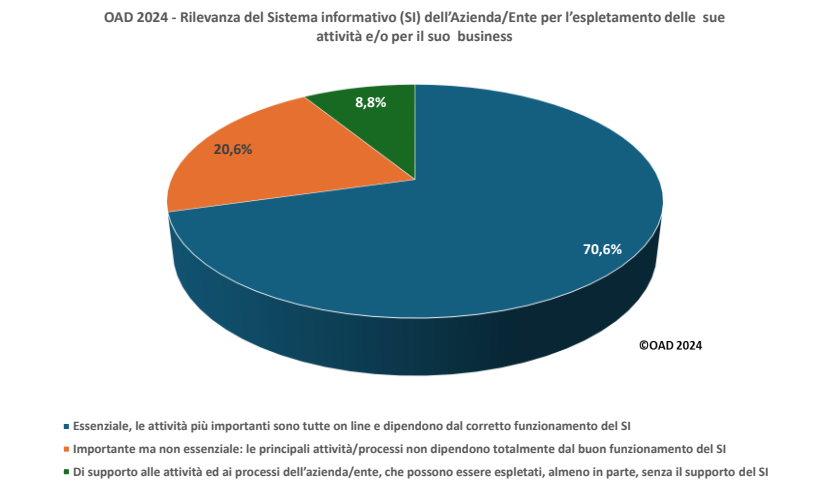


Fig. 6.2-3

Un'altra caratteristica importante per la sicurezza digitale di un SI è il trattamento di dati personali, che lo obbliga ad ottemperare, tecnicamente ed organizzativamente, alla normativa sulla privacy, il GDPR, con misure specifiche per i dati personali "sensibili"[43].

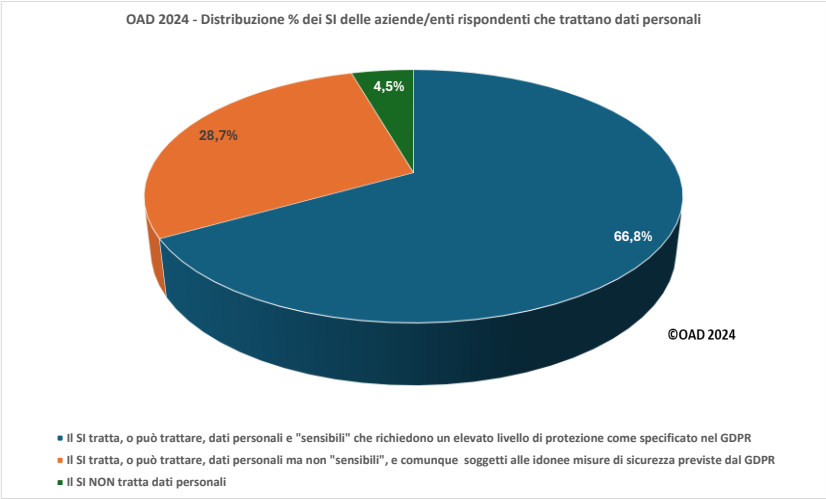


Fig. 6.2-4

La fig. 6.2-4 evidenzia che solo il **4,5% dei SI** oggetto delle risposte **non tratta dati personali**; il **95,5% li tratta** e di questi il **66,8%** tratta, o potrebbe trattare, **dati sensibili**.

Un SI può trattare molte altre informazioni importanti e confidenziali, come ad esempio segreti industriali, piani di ricerca e sviluppo di prodotti innovativi, dati finanziari ed economici, elenchi di clienti e fornitori con

[43] 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 e diffusione, il termine "dato sensibile" viene comunque usato nel presente Rapporto.

condizioni di vendita ed acquisto, verbali con decisioni importanti, accordi commerciali ed offerte di grande valenza economica.

Il tema delle informazioni riservate, e quindi critiche per l'azienda/ente che le possiede, è correlato a quello delle infrastrutture "critiche" che forniscono servizi essenziali per il funzionamento di un intero paese.
L'Unione Europea (UE), nell'obbiettivo di potenziare ed omogeneizzare la sicurezza digitale dell'intera UE, ha emanato una serie di normative, quali **NIS/NIS2, DORA, CER**, etc., trattate in §3.6, che varie aziende ed enti pubblici **devono già o** dovranno **nel prossimo futuro** seguire ed implementare, per garantire in ogni paese dell'UE i più elevati livelli di sicurezza e segretezza digitale.

La fig. 6.2-5 mostra quanti dei SI oggetto delle risposte 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 **10,6 %** dei SI è dichiarato dai rispondenti come "**critico**" in quanto gestisce infrastrutture critiche e/o fornisce servizi essenziali per l'Italia, e rientra quindi tra i SI oggetto delle nuove normative europee quali NIS2**.** Il **34,2%** dichiara di gestire informazioni molto critiche e confidenziali, anche se il SI non è soggetto alle normative EU tipo NIS/NIS2. La maggioranza delle aziende/enti rispondenti, il **55,3%** tratta informazioni necessarie al loro funzionamento, ma non ritenute molto critiche.

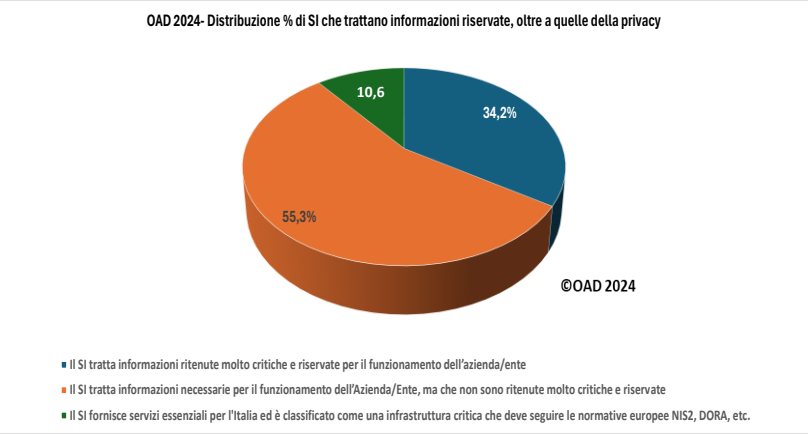


Fig. 6.2-5

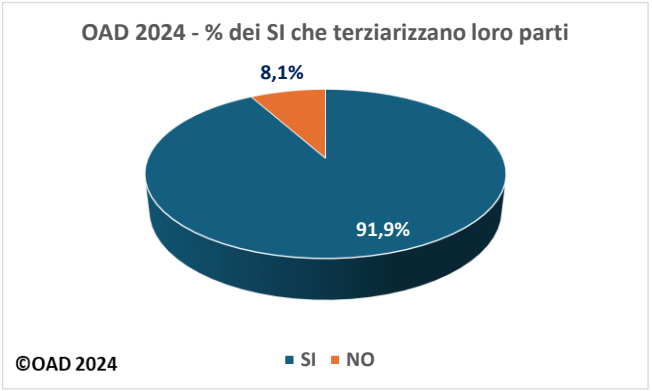


Fig. 6.2-6

Come evidenziato nella fig. 6.2-6, la quasi totalità dei SI dei rispondenti, il **91,9%** utilizza **servizi ICT terziarizzati**, ed il più delle volte erogati da fornitori diversi. Indipendentemente dalle dimensioni e dalle funzioni espletate con i vari applicativi, i SI dei rispondenti sono quindi quasi tutti ibridi, ossia in parte on premise (in locale) ed in parte terziarizzati, ad esempio in multi cloud: realtà che comporta una maggior complessità per la sicurezza digitale e la sua gestione.

Il 91,9% dei SI ibridi evidenzia il trend dell'accettazione e diffusione nell'uso di servizi ICT terziarizzati, confrontando i dati emersi e man mano cresciuti nei diciassette anni di indagini OAD/OAI a partire dal 2007[44].

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 per la gestione dell'intero SI, o di sue parti, e della sua sicurezza digitale: in tale logica sono disponibili offerte per MSS[45], Managed Security Services e per CSaaS[46], Cyber Security as a Service, che potranno essere utilizzate dalle realtà piccole e piccolissime.

Dato che la terziarizzazione dei sistemi e dei servizi ICT, in particolare con il cloud, è un elemento che fortemente caratterizza un **SI** e la sua sicurezza digitale, si è voluto correlare questo dato con **le dimensioni, per numero di addetti,** delle aziende/enti rispondenti.

La fig. 6.2-7 mostra tale correlazione e si sottolinea che per una corretta interpretazione della correlazione, si deve tener conto che le percentuali emerse dipendono anche dal numero di risposte ricevute.
Dalla figura emerge che le strutture organizzative con meno di 250 dipendenti, le PMI per le aziende, utilizzano applicazioni e servizi terziarizzati per il **69,2%**.

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

Le fig. 6.2-8 e 6.2-9 mostrano la situazione per i **SI** oggetto delle risposte:

- la **gestione operativa del SI** è effettuata solo internamente per **24,4%** dei rispondenti, tutti gli altri terziarizzano o in toto, il **38,6%,** o solo per alcune parti, il **37,1%**, tipicamente per gli applicativi ed i servizi che già sono in uso terziarizzati;
- la **gestione operativa della sicurezza digitale** del SI è effettuata solo internamente dal **19,8%** dei rispondenti, tutti gli altri la terziarizzano o completamente, il **41,6%**, o solo per alcune parti, il **38,6%**, tipicamente per la gestione della sicurezza degli applicativi e dei servizi che già sono terziarizzati.

[44] Si veda in merito un recente articolo dell'autore dal titolo "*Come evolvono gli attacchi cyber in Italia: le indagini OAD di AIPSI*", pubblicato su Agenda Digitale: https://www.agendadigitale.eu/sicurezza/evoluzione-degli-attacchi-digitali-in-italia-lanalisi-delle-indagini-oad-di-aipsi/

[45] 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.

[46] 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.

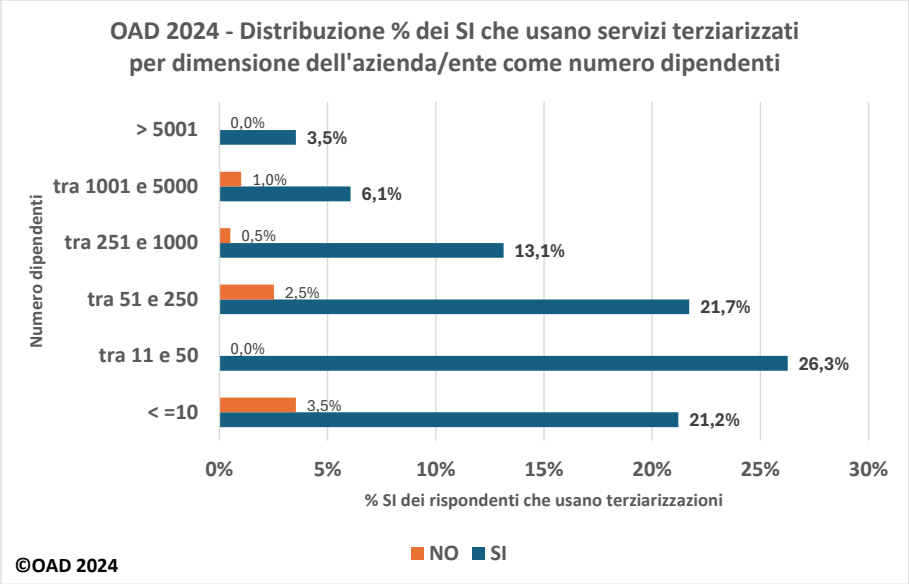


Fig. 6.2-7

Il dato percentuale della "completa" terziarizzazione della gestione operativa della sicurezza digitale è alto e significativo: le piccole organizzazioni, salvo eccezioni, non possono essere in grado di gestire autonomamente la sicurezza digitale, e devono fare pertanto ricorso a consulenti o a società specializzate. Proprio per le piccole realtà saranno sempre più significativi i servizi tipo MSS e CSaaS, come già indicato in precedenza, a parte il problema del loro prezzo, spesso troppo alto perché le realtà più piccole li possano usare.

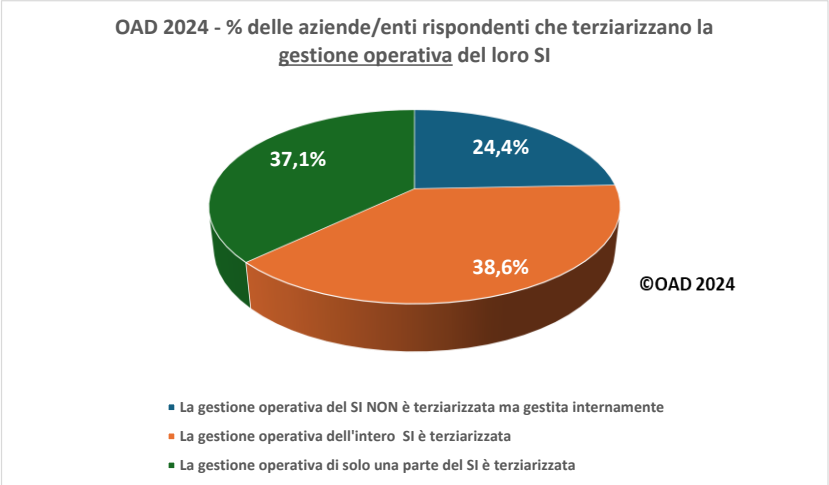


Fig. 6.2-8

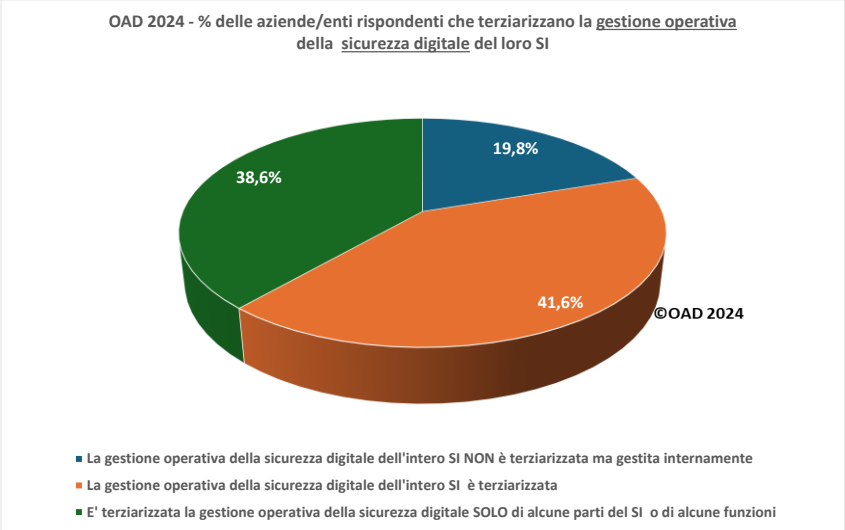


Fig. 6.2-9

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 2024.

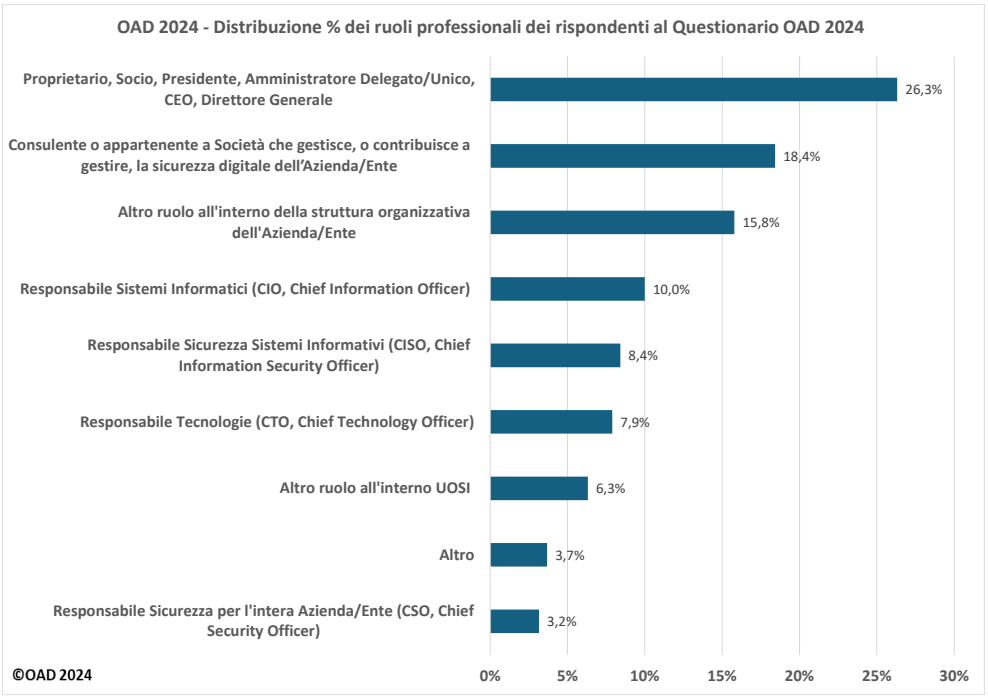


Fig. 6.3-1

Al primo posto, con il **26,3%**, il **proprietario/socio** o **i vertici manageriali** dell'azienda/ente, al secondo posto, con un **18,6%**, la persona "esperta ed esterna", consulente autonomo o dipendente di una società

specializzata, cui l'azienda/ente rispondente ha terziarizzato, in toto o in parte, la gestione del sistema informativo e/o della sua sicurezza. Questo dato conferma la tendenza alla terziarizzazione della gestione del SI e/o della sua sicurezza, come evidenziato nelle precedenti fig. 6.2-8 e 9.
Al terzo posto, con il **15,8%**, un **addetto** nella struttura **UOSI**[47]. Al quarto posto, con un **10%**, le/i rispondenti che si sono qualificati come **CIO**, che rappresenta ed include per le piccole-piccolissime organizzazioni anche l'Amministratore di sistema interno, ed al quinto, con un **8,4%**, i **CISO**.
Nella voce "Altro" è stato indicato il ruolo di **DPO**, Data Protection Officer, e di **Auditor del SI**.

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

Relativamente basse le percentuali di CISO e di CIO, figure professionali presenti in Italia prevalentemente nelle medio-grandi organizzazioni: ed anche in alcune di queste il ruolo di CISO non è definito, ed è attuato de facto dal CIO e/o da consulenti esterni.

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 del personale per l'intera azienda/ente, ruoli che sono definiti ed operativi soprattutto nelle grandi organizzazioni.

[47] UOSI, Unità Organizzativa Sistemi Informativi. Questo acronimo è usato dall'autore per indicare la struttura organizzativa interna (se esiste) che gestisce il SI e di cui è responsabile il CIO.

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

Nel questionario dell'indagine OAD 2024 le domande sulle misure di sicurezza erano **opzionali**, si potevano cioè saltare, anche se erano raccomandate soprattutto per le piccole/medie organizzazioni perché potessero ottenere, alla fine della compilazione del questionario, una macro valutazione del livello di sicurezza del sistema informativo oggetto delle loro risposte al questionario. Valutazione effettuata contestualizzando le misure di sicurezza digitale in essere con le esigenze di sicurezza digitale dell'azienda/ente, con riferimenti e relative pesature al settore merceologico, al ruolo più o meno essenziale del sistema informativo nel supporto alle attività dell'organizzazione, e alla necessità complessiva di sicurezza digitale. Per maggiori dettagli si rimanda **all'Allegato A** del presente rapporto.

Hanno risposto alle domande sulle misure di sicurezza il **35,4%** delle/dei rispondenti (fig. 7-1).
E' una percentuale piuttosto bassa, dovuta, a giudizio dell'autore, a due principali fattori:

- l'ulteriore l'impegno, in termini di competenze specifiche e di tempo (mediamente una mezz'ora in più rispetto alle altre domande "obbligatorie") per compilare questa parte opzionale non è stato riconosciuto dai più come interessante e/o opportuno per:
  - una verifica delle misure in essere per la sicurezza digitale del SI oggetto delle risposte, che per alcuni poteva essere anche un veloce aggiornamento sulle principali misure da considerare (soprattutto per le piccole aziende/enti);
  - avere in automatico una macro valutazione qualitativa del complessivo livello di sicurezza del SI, contestualizzato alle macro necessità di sicurezza richieste dalle attività e dal business dell'azienda/ente rispondente;
- il timore di non avere le informazioni sulle misure in essere del SI, e/o avere difficoltà ad averle per rispondere al questionario, dato che buona parte dei rispondenti non hanno specifiche competenze tecniche, essendo persone di vertice o con altri ruoli nell'azienda/ente, come evidenziato nella fig. 6.3-1.

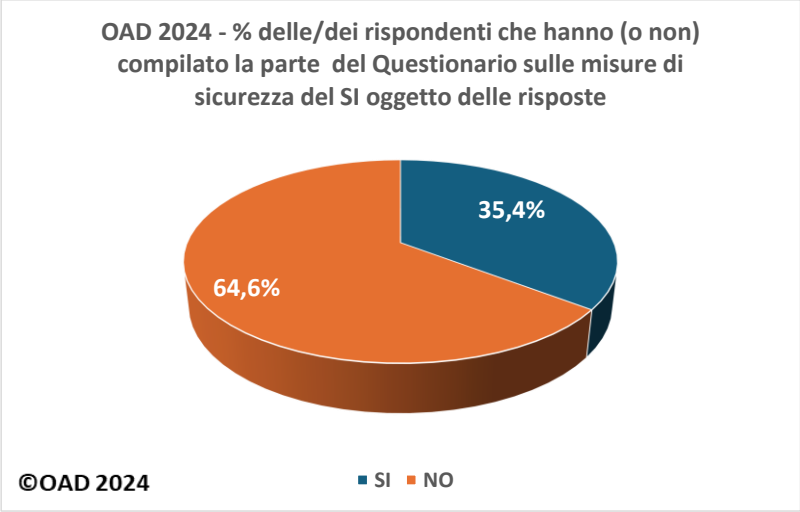


Fig. 7-1

La fig. 7-2 dettaglia il ruolo professionale di chi ha compilato anche la parte opzionale sulle misure di sicurezza in essere nel SI oggetto delle risposte.

Si spartiscono il primo posto tre famiglie, con la stessa percentuale del **17,4%**: i **vertici aziendali**, i **consulenti esterni** ed i **CIO**. Le prime due sono ai primi due posti anche sul totale dei rispondenti al questionario, come evidenziato nella fig. 6.3-1. Nella fig. 7-2 seguono i **CISO** con il **14,5%** come rispendenti alle domande opzionali. Le altre figure professionali hanno percentuali decrescenti sotto il 10%. Più che la percentuale specifica, è significativo per OAD 2024 che tutte le figure professionali considerate hanno compilato la parte tecnica opzionale, seppur in numero limitato.
La relativamente alta percentuale dei vertici aziendali è dovuta all'alta percentuale di organizzazioni con meno di 50 dipendenti, come negozi, studi professionali, officine e piccole fabbriche, piccole PAL, dove chi decide sul sistema informativo, per quanto piccolo possa essere, è la proprietà o chi dirige e controlla l'azienda, lo studio professionale, etc.). La relativamente alta percentuale di consulenti esterni rispondenti è anch'essa dovuta alla larga partecipazione all'indagine OAD di PMI e di enti di analoga dimensione, quasi il 70% sul totale (si veda fig. 6.1-3), che debbono farsi aiutare, o completamente terziarizzare, la gestione del proprio SI e della sua sicurezza. I CIO, come rispondenti, assommano ad un 10%, di poco superiore all'8,4% dei CISO, e tendenzialmente, a giudizio dell'autore, avevano un interesse maggiore, rispetto ai CISO, a scoprire quale livello di sicurezza del SI da loro gestito fornisse il questionario OAD alla fine della compilazione.

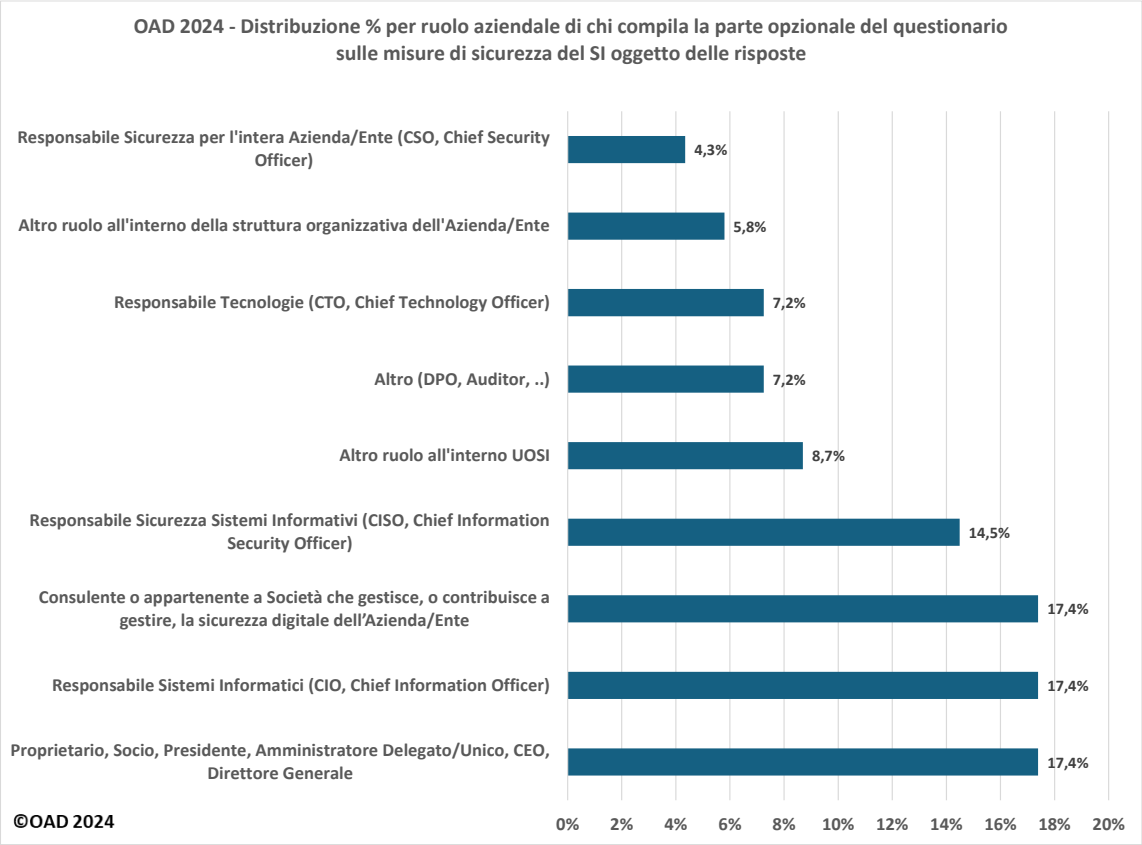


Fig. 7-2

La fig. 7-3 mostra la ripartizione percentuale di chi ha risposto alle domande per dimensione d'azienda/ente come numero di dipendenti: i dati confermano le considerazioni sopra esposte. Le organizzazioni al di sotto dei 250 dipendenti (per le aziende le PMI) sono la maggioranza, **62,3%**, ma anche le organizzazioni più grandi hanno risposto alla parte opzionale del questionario.

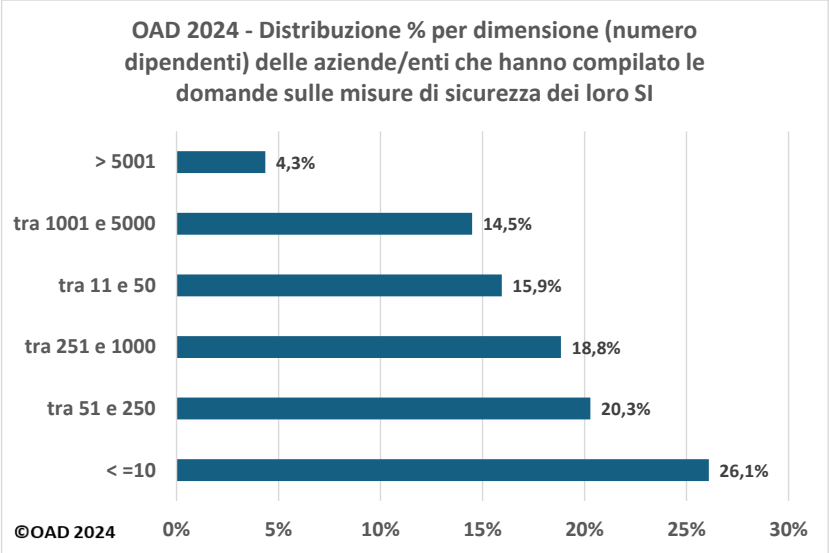


Fig. 7-3

La figura 7-4 correla percentualmente quanti hanno risposto alle domande sulle misure di sicurezza per settore merceologico, incluse le PA. Pur avendo risposto a queste domande poco più di 1/3 delle aziende/enti rispondenti, la loro distribuzione copre la maggior parte dei settori merceologici, incluse le PA.
Percentualmente al primo posto, con un **21,5%**, sono le **aziende ICT**, nell'indagine OAD 2024 suddivise tra i fornitori di hosting/cloud, che hanno però risposto solo per il 4,3%, e tutte le altre aziende del settore ICT. Il settore istruzione è al secondo posto, con il **15,9%**: risulta al primo posto in % tra tutti i settori rispondenti nella fig. 6.1-2. 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.

Nel complesso il mix di rispondenti a questa parte opzionale delle misure di sicurezza copre sia i vari settori merceologici che le aziende/enti di diverse dimensioni come numero di addetti.
I risultati che emergono hanno quindi validità come indicatori della situazione della sicurezza digitale nei SI dei rispondenti, e non certo come analisi della diffusione dei vari strumenti di sicurezza digitale in Italia: per questo occorre fare riferimento ad alcune indagini di mercato.

Il presente Capitolo 7 rileva gli strumenti di sicurezza in uso nei sistemi informativi (SI) delle aziende/enti rispondenti, le cui macro caratteristiche sono riportate nel precedente Capitolo 6, così da poter meglio comprendere in quali ambiti e contro quali livelli di sicurezza digitale sono stati attuati gli attacchi rilevati ed analizzati nel Capitolo 4.

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.

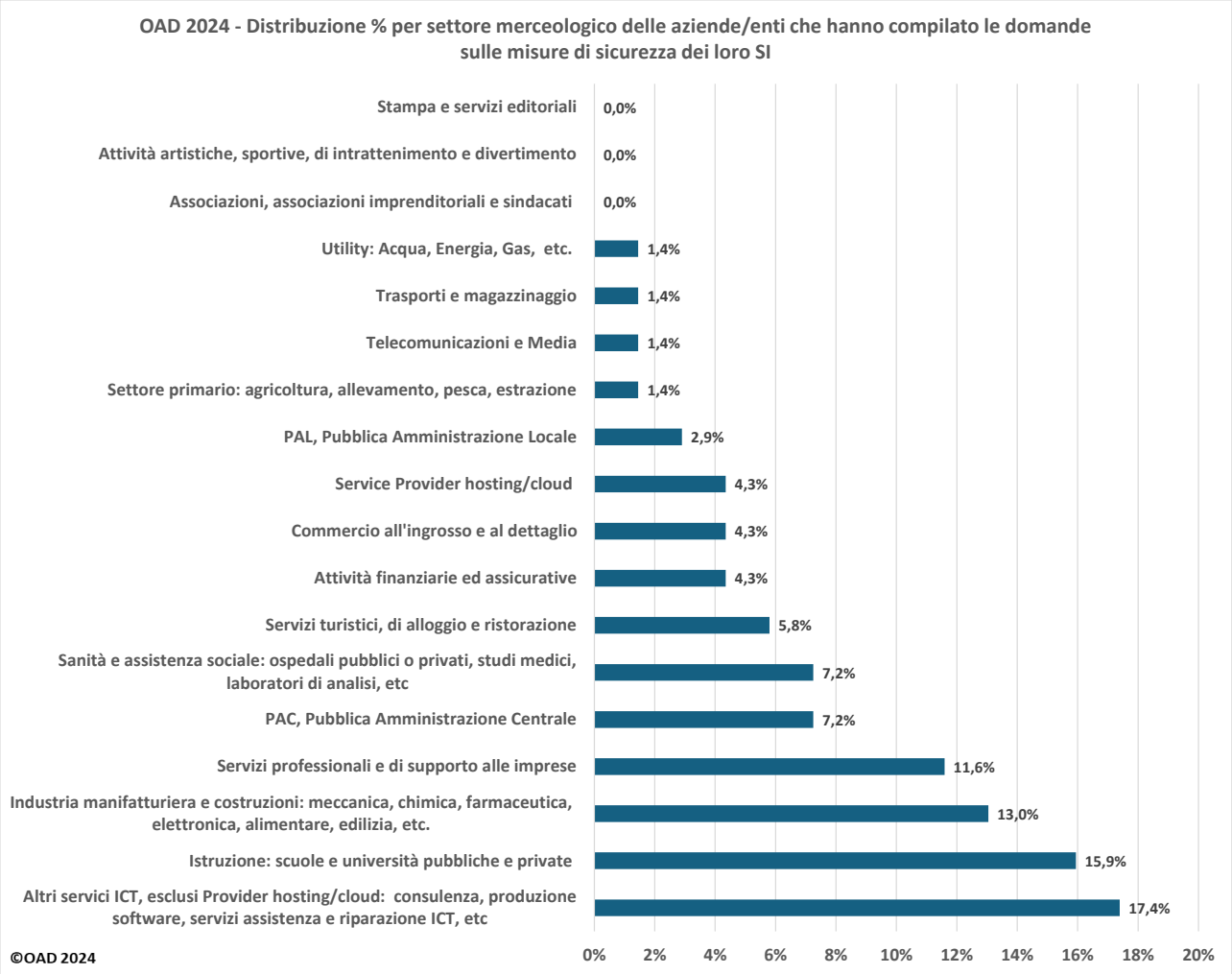


Fig. 7-4

7.1 Le misure organizzative per la sicurezza digitale dei SI

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 come oneri burocratici e/o come spese di consulenza non necessarie: di interesse, di fatto, solo per le grandi organizzazioni. Al contrario, esse **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[48], DORA[49], CER[50], etc), a partire dal GDPR per la privacy, richiedono tutti l'attuazione di gran parte delle misure organizzative considerate in OAD 2024. 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 sulle misure per la sicurezza digitale.

In termini di ruoli e competenze per la sicurezza digitale è importante e di riferimento il documento di ENISA **ECSF**, European Cybersecurity Skills Framework, che specifica 12 figure professionali e relativi profili[51], la prima delle quali è il **CISO, Chief Information Security Officer.**

7.1.1 La struttura organizzativa per la sicurezza digitale ed il ruolo di CISO

La prima misura organizzativa per la sicurezza digitale è data dalla definizione ed assegnazione del ruolo e delle responsabilità di chi la deve gestire nell'ambito dell'azienda/ente, con l'eventuale relativa struttura organizzativa, piccola o grande, interna o esterna. In funzione del tipo di azienda/ente, in particolare delle sue dimensioni, della sua attività, del settore merceologico di appartenenza, delle certificazioni e delle normative che deve seguire, esistono varie modalità di assegnazione di questo ruolo.

La fig. 7.1.1-1 mostra che nel **38,5%** delle aziende/enti rispondenti è definito ed espletato internamente il **ruolo di CISO**, la cui profilatura di riferimento è definita dall'ECSF di ENISA. Tale ruolo è invece assegnato ed espletato **dal CIO** nel **29,2%** dei casi rispondenti. Nel **20%** dei casi è **terziarizzato** a consulenti o a società specializzate. Nel **10,8%** delle aziende/enti rispondenti il ruolo del CISO non è definito ed assegnato, e in caso di bisogno/problemi è il vertice dell'azienda/ente che decide che cosa e come fare. Solo l'**1,5%**, dichiara che il ruolo di CISO non è definito e designato, ma è di fatto svolto da persone di strutture diverse da quella UOSI, Unità Organizzativa Sistemi Informativi, la struttura che risponde al CIO. In taluni casi è svolto dal DPO, oppure dal CSO o dal CTO, o ancora dall'ufficio legale dell'azienda/ente.

[48] NIS2 (Network and Information Security), è la Direttiva UE 2022/2555 per i fornitori di servizi essenziali-infrastrutture critiche, ed è un aggiornamento ed un ampliamento rispetto alla precedente NIS.

[49] DORA, Digital Operational Resilience Act, è il Regolamento UE 2022/2554 per potenziare le misure di sicurezza digitale in ottica resilienza nel mondo finanziario.

[50] CER, Critical Entities Resilience Directive, è la Direttiva UE 2022/2557 per potenziare le misure di sicurezza digitale in ottica resilienza per le entità critiche.

[51] I 12 profili per la sicurezza digitale specificati in ECSF sono: CISO, cyber incident responder, cyber legal - policy & compliance officer, cyber threat intelligence specialist, cybersecurity architect, cybersecurity auditor, cybersecurity educator, cybersecurity implementer, cybersecurity researcher, cybersecurity risk manager, digital forensics investigator, penetration tester.
Per un approfondimento sul tema si veda anche il recente articolo dell'autore "*Ruoli e competenze per la sicurezza digitale: da ENISA ... alla realtà italiana*" pubblicato su Office Automation n. 4/2024: https://www.soiel.it/sfogliabili/officeautomation/2024/4/show_rivista.php#

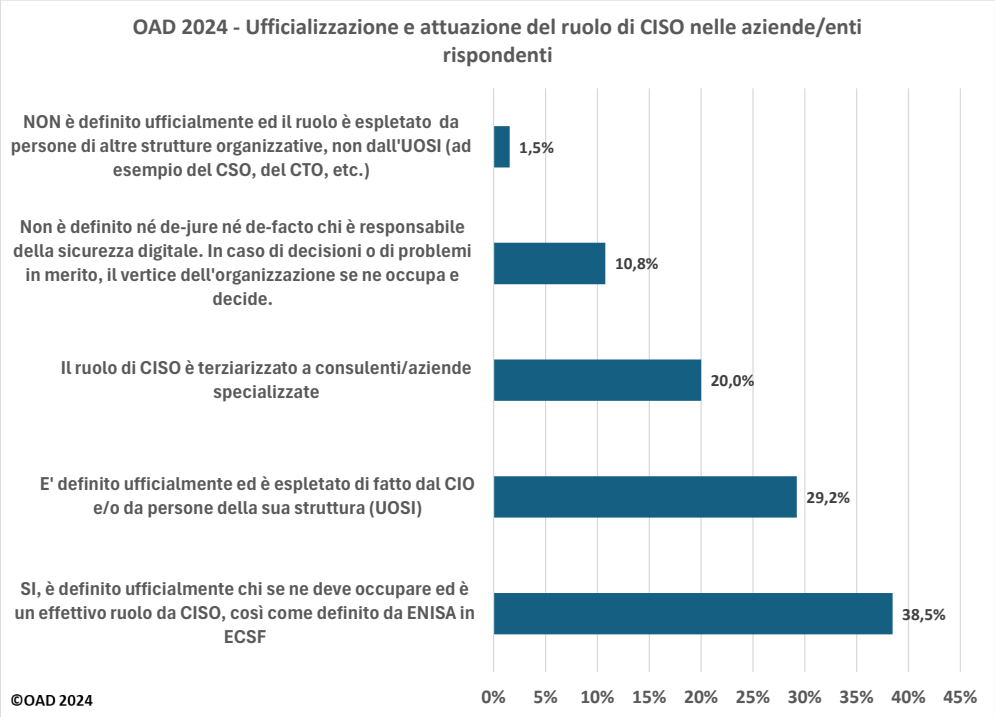


Fig. 7.1.1-1

7.1.2 Policy e procedure organizzative per la sicurezza digitale

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

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

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

Policy e procedure organizzative scritte, fatte conoscere ed aggiornate periodicamente, non sono da considerare una inutile e costosa burocrazia, e nemmeno attività solo per aziende/enti di grandi dimensioni: sono necessarie ed utili per formalizzare e divulgare come usare e gestire le risorse ICT e la loro sicurezza ad utenti finali e privilegiati, e fornire specifiche indicazioni alle terze parti che possono essere coinvolte nella gestione e/o nel governo del sistema informativo. Sono inoltre essenziali per dimostrare l'accountability[52], così come richiesto dal GDPR e dalle altre normative dell'Unione Europea nell'ambito della sicurezza digitale, quali NIS2, DORA, etc.

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

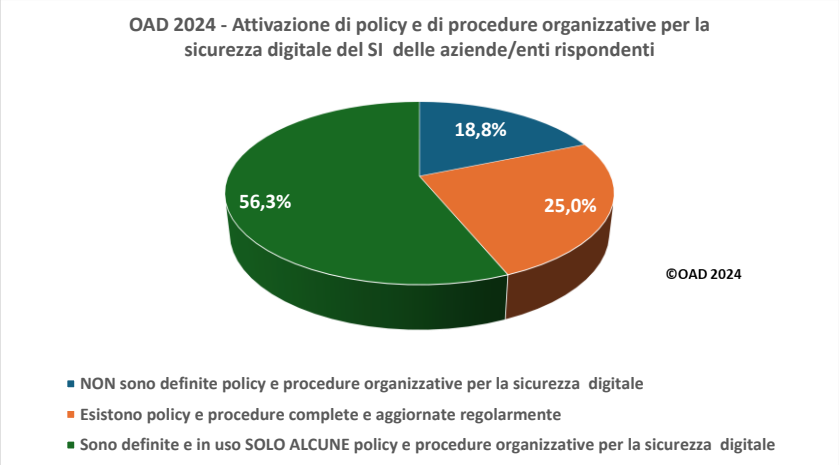


Fig. 7.1.2-1

La fig. 7.1.2-1 evidenzia che la stragrande maggioranza delle aziende/enti rispondenti, l'**81,3%** ha **definito ed usa policy e procedure organizzative per la sicurezza digitale,** ma di questi il **56,3%** 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, (che include anche la gestione delle password), la gestione dell'help desk e del "trouble ticketing".[53]

A conferma di questo, il questionario OAD 2024 ha posto la domanda sull'esistenza di policy, e soprattutto di procedure, per la gestione di incidenti sul SI e sulla sua sicurezza.

La fig. 7.1.2-2 fornisce la risposta tra quanti hanno dichiarato di avere delle policy/procedure, ed evidenzia che il **73,1%** dichiara di aver definito ed attuato queste misure organizzative. La figura mostra anche che il **3,8%** ammette di non saperlo. Come già commentato in precedenza, conoscenze specifiche su aspetti tecnici o organizzativi o legali del SI della propria azienda/ente possono mancare, a seconda di chi compila il questionario: se questi non ha potuto o voluto chiedere a colleghi, ha ammesso di non saperlo.

Si vedrà, nelle pagine di questo capitolo (ma anche in altri del presente Rapporto OAD 2024), 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 che non si sono inventati risposte su argomenti che non conoscevano; ed aumenta la validità e l'autorevolezza dell'intera indagine.

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

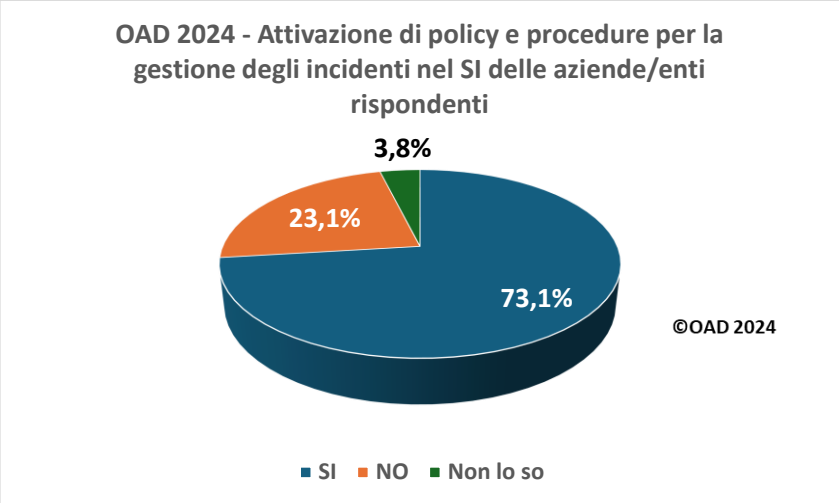


Fig. 7.1.2-2

Un'altra procedura organizzativa nella gestione del sistema informativo e della sua sicurezza è **l'assistenza agli utenti**, fondamentale soprattutto per segnalare problemi sulla sicurezza digitale e per SI 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 con diversi livelli di approfondimento[54] 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 ed il §7.2.7 sul Disaster Recovery).

La fig. 7.1.2-3 mostra che il **28,8%** delle aziende/enti rispondenti **non ha** alcuna procedura e nessun servizio di **assistenza agli utenti**, situazione tipica per le piccole organizzazioni. Per i rispondenti che le hanno, il **38,5**% utilizza un mix di servizi erogati in parte internamente ed in parte tramite Terze Parti. Il **25%** eroga e gestisce l'assistenza agli utenti tutta al proprio interno, mentre il **7,7%** l'ha completamente terziarizzata.

Per la gestione degli incidenti gravi, e non solo riguardanti il sistema informativo, le grandi organizzazioni dedicano uno specifico team, l'**ERT**, Emergency Response Team (o nomi simili), che tipicamente coinvolge non solo il personale dell'UOSI, Unità Organizzativa Sistemi Informativi, ma anche responsabili di altre direzioni e "business unit" dell'azienda/ente.
E' l'ERT che interviene in caso di disastri, e non solo del SI, per l'attuazione del Piano di Disaster Recovery e ripristinare al più presto la continuità operativa dell'azienda/ente che ha subito il disastro (si veda §7.2.7).

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

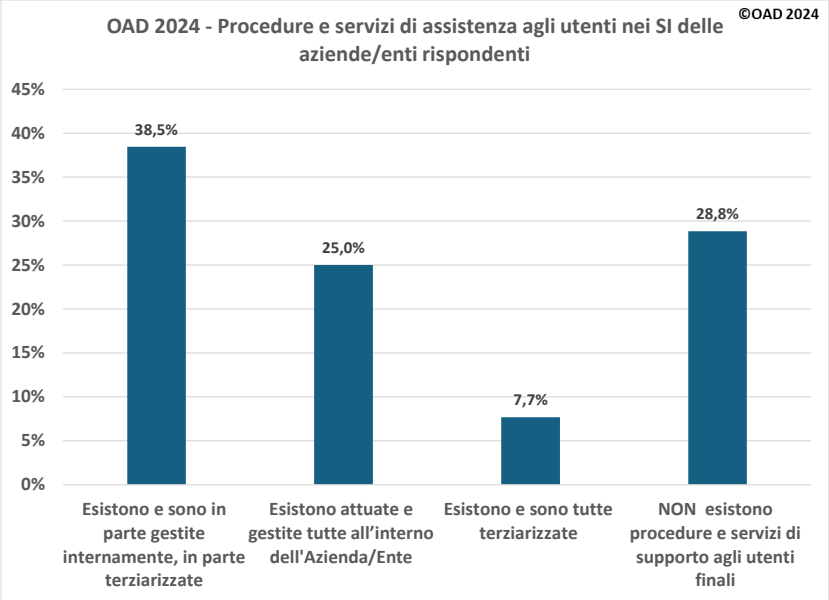


Fig. 7.1.2-3

Come mostrato in fig. 7.1.2-4, la metà, il **50%,** delle aziende/enti rispondenti dichiara di avere un ERT con definite e in uso le relative procedure organizzative, ma di questi solo il **15,4%** effettua periodicamente prove e simulazioni di casi di disastri: ed è quindi solo questo nucleo di aziende/enti capace realmente di attivare un Disaster Recovery del sistema informativo (SI) in caso di disastro.

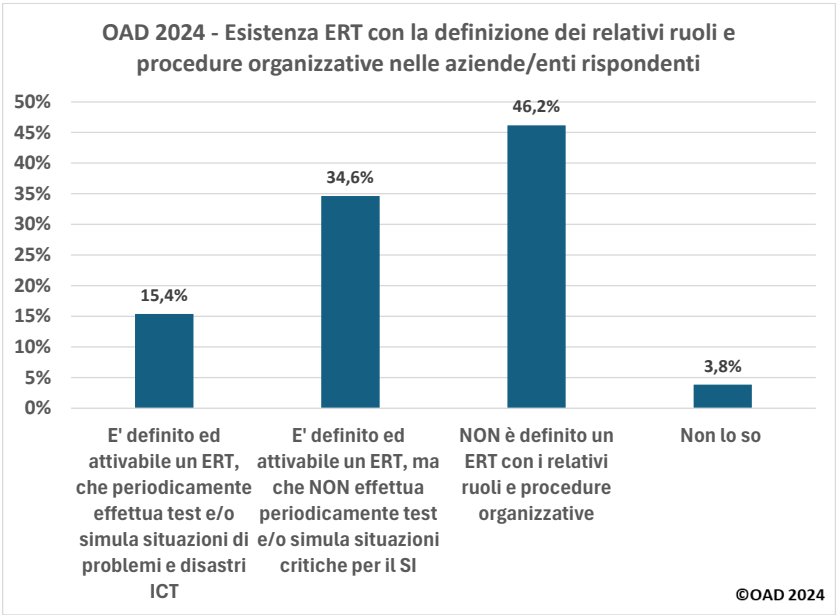


Fig. 7.1.2-4

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 la quasi totalità aggiorna componenti e procedure ERT o **periodicamente** o a **seguito di importanti riorganizzazioni** e/o importanti modifiche evolutive del sistema informativo.

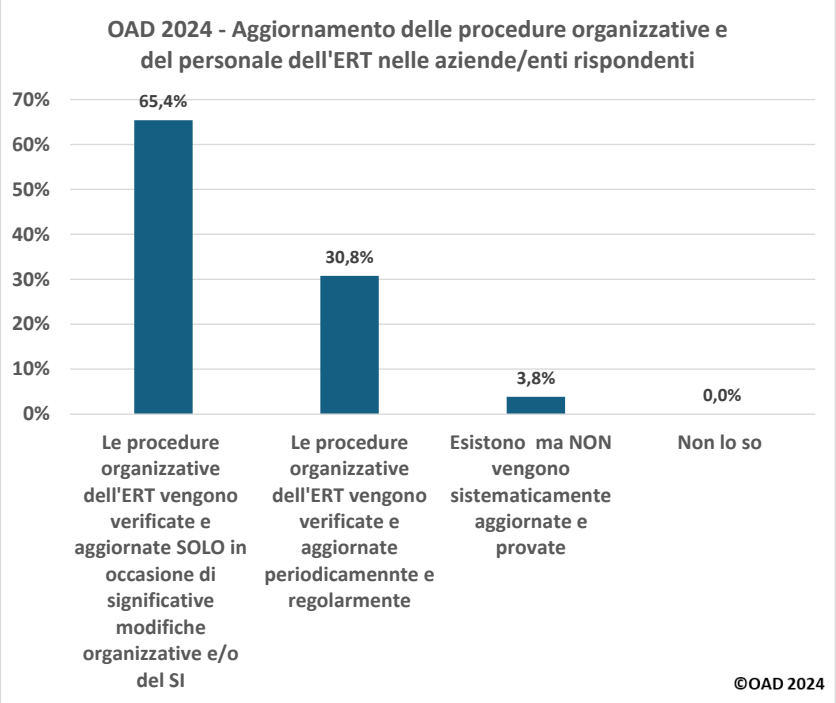


Fig. 7.1.2-5

7.1.3 Analisi dei rischi digitali e dei possibili impatti

L'analisi dei rischi digitali e dei lori impatti sul sistema informativo (SI), e più in generale sull'intero business e/o attività dell'azienda/ente, è basilare per la progettazione delle misure di sicurezza contestualizzate sulla specifica realtà dell'azienda/ente. L'analisi dei rischi è inoltre richiesta per la conformità a varie norme e leggi, a partire dal GDPR e dal NIS2.

Sono ormai consolidate da anni varie metodiche, best practice e framework per effettuare tali analisi, pur con differenti livelli di dettaglio: dallo standard ISO 27005 a NIST SP 800-30, da CRAMM[55] a MEHARI[56] e a Octave-Allegro[57].

I rischi digitali dipendono dalle vulnerabilità tecniche, organizzative e delle persone che usano e gestiscono i sistemi informatici e più in generale ogni dispositivo ICT; per una corretta individuazione dei rischi digitali occorre quindi effettuare un'analisi delle **vulnerabilità digitali**, di cui in §7.2.7 e alla fig. 7.2.7-9.

[55] CRAMM, CCTA Risk Analysis and Management Method, creato dalla Central Computer and Telecommunications Agency del Governo UK, ora chiamato Cabinet Office. Si veda anche: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cramm.html

[56] MEHARI, MEthod for Harmonized Analysis of Risk, è un metodo opensource di assessment ed analisi dei rischi ICT: https://www.meharipedia.org/

[57] Octave-Allegro è la metodica semplificata di analisi e gestione dei rischi ICT della Carnegie Mellon University https://insights.sei.cmu.edu/library/introduction-to-the-octave-approach/, promossa dal Department of Defense U.S. https://apps.dtic.mil/sti/pdfs/AD1092648.pdf

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[58] 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 (§3.4.1) e consente di classificare, descrivere e simulare specifici attacchi informatici e intrusioni: il suo è crescente nei team dei CISO, di pronto intervento (chiamati spesso Red Team o Emergency Team) e nei SOC.

Come evidenzia la fig. 7.1.3-1, quasi i 3/4, il **73,4%** delle aziende/enti rispondenti **effettua l'analisi dei rischi digitali**, e di questi il **42,2%** la effettua periodicamente e sistematicamente.
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/NIS2 a DORA (si veda §3.6), impongono a chi è obbligato a seguirle, una analisi dei rischi digitali approfondita e periodica, dato che essa è la base per l'individuazione e l'implementazione delle misure di sicurezza che prevengano i rischi individuati o limitino comunque l'impatto sul business e sul sitema informativo in caso di loro occorrenza.

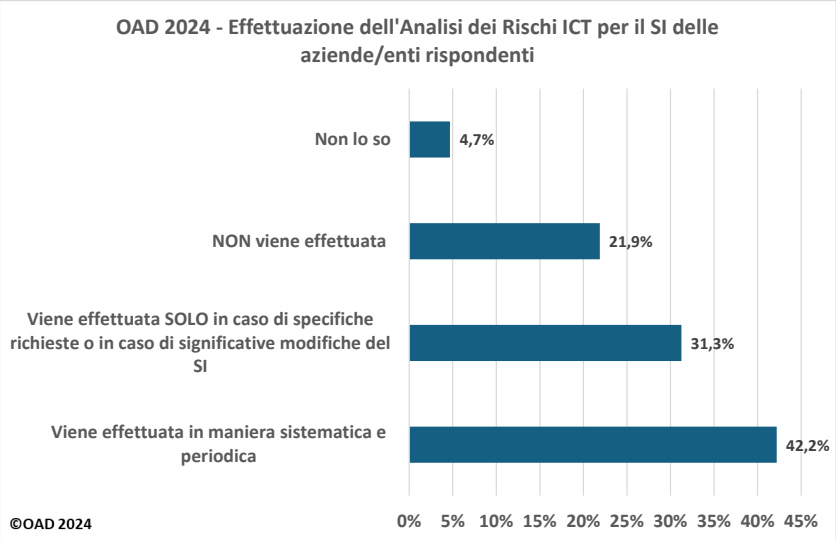


Fig. 7.1.3-1

Data l'importanza dell'analisi dei rischi, il OAD 2024 ha voluto approfondire il tema. La prima analisi è stata la verifica di quali aziende/enti non la effettuano, considerando le loro dimensioni, come numero di dipendenti.

La fig. 7.1.3-2 mostra tale correlazione e conferma, come prevedibile, che non la effettuano soprattutto le piccole e piccolissime organizzazioni. La figura evidenzia che non la effettuano anche grandi e grandissime organizzazioni, con il **28,6%,** una percentuale troppo alta a giudizio dell'autore, per il quale probabilmente tale numero deriva da un lato dalla correlazione tra dati emersi appartenenti a gruppi di rispondenti numericamente piccoli (pericolo evidenziato anche nei risultati di altre correlazioni sui dati OAD 2024), dall'altro che molto probabilmente chi ha indicato che la sua azienda/ente non effettua l'analisi dei rischi digitali ha sbagliato.

[58] 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.

Un'ulteriore approfondimento nell'ambito dell'analisi dei rischi riguarda l'analisi dei possibili impatti sui processi ed attività dell'azienda/ente, analisi chiamata **BIA**, Business Impact Analysis. Questa analisi dovrebbe essere effettuata anche i per i rischi ICT.

La fig. 7.1.3-3 mostra che la **BIA è effettuata** da quasi il **90%** delle aziende/enti rispondenti che effettuano l'analisi dei rischi ICT. L'alta percentuale emersa, indipendente dalle dimensioni dell'azienda/ente e dal suo settore merceologico, è anche un risultato di quasi trent'anni di normative sulla privacy, culminate con il GDPR attualmente in vigore, che hanno fortemente promosso, se non richiesto, una puntuale analisi dei rischi e degli impatti causati da una loro occorrenza almeno sui dati personali

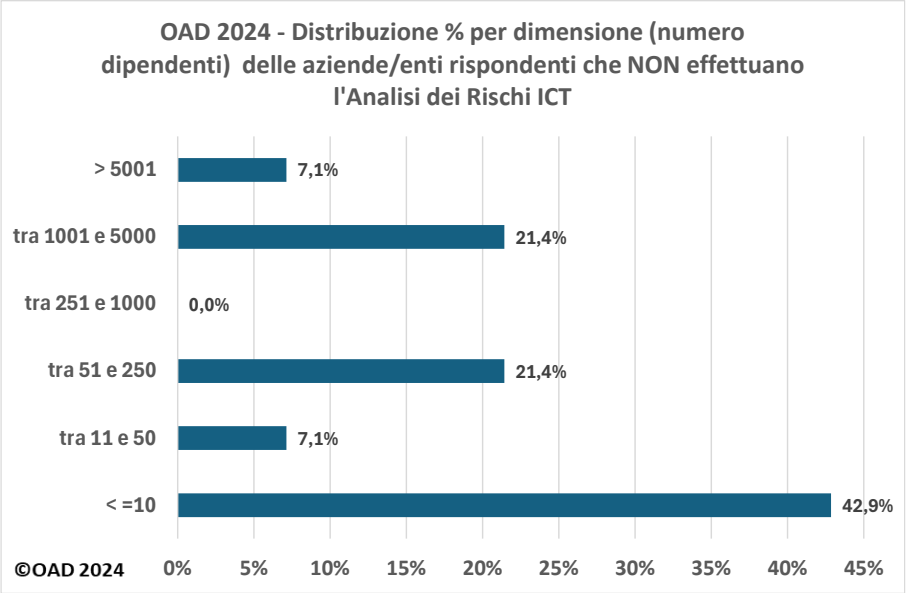


Fig. 7.1.3-2

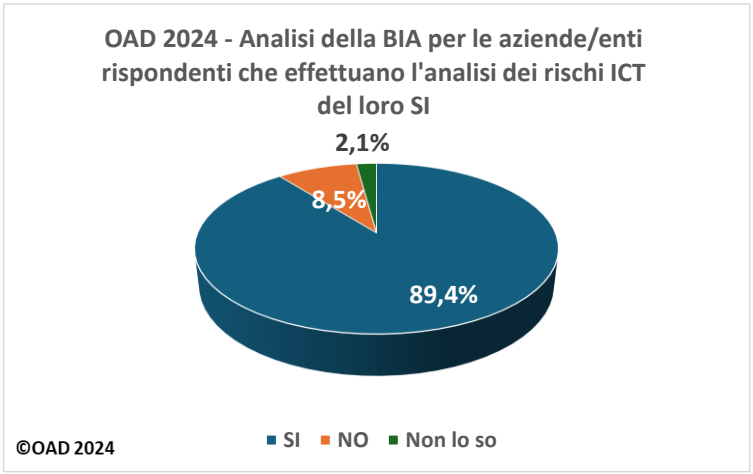


Fig. 7.1.3-3

Così come per il più generale rischio aziendale, anche per il rischio informatico (o ICT o digitale) si possono stipulare **polizze assicurative** per l'intero sistema informativo, o per le sue parti che trattano i dati più critici per l'azienda/ente. Normalmente l'attivazione di una polizza assicurativa sui rischi digitali avviene dopo che l'azienda/ente ha implementato e messo in esercizio le necessarie misure di sicurezza, tecniche ed organizzative, per far fronte ai possibili rischi digitali. L'ente assicurativo, infatti, richiede e verifica con suoi esperti che siano in atto tutte le misure di sicurezza idonee, e allo stato dell'arte dell'informatica, altrimenti non stipula il contratto o chiede premi altissimi.

Per il campione emerso dall'indagine OAD 2024, la fig. 7.1.3-4, il **34,9%** delle aziende/enti rispondenti ha **stipulato una polizza assicurativa** sul proprio sistema informativo, ma di questi il **25,4%** lo ha stipulato solo per alcune delle sue parti più critiche.

La complessità nello stipulare una polizza informatica ed il suo costo, che è fortemente aumentato negli ultimi anni con il crescere del rischio di essere attaccati, sono elementi che attualmente rendono tali polizze fruibili prevalentemente da grandi organizzazioni.

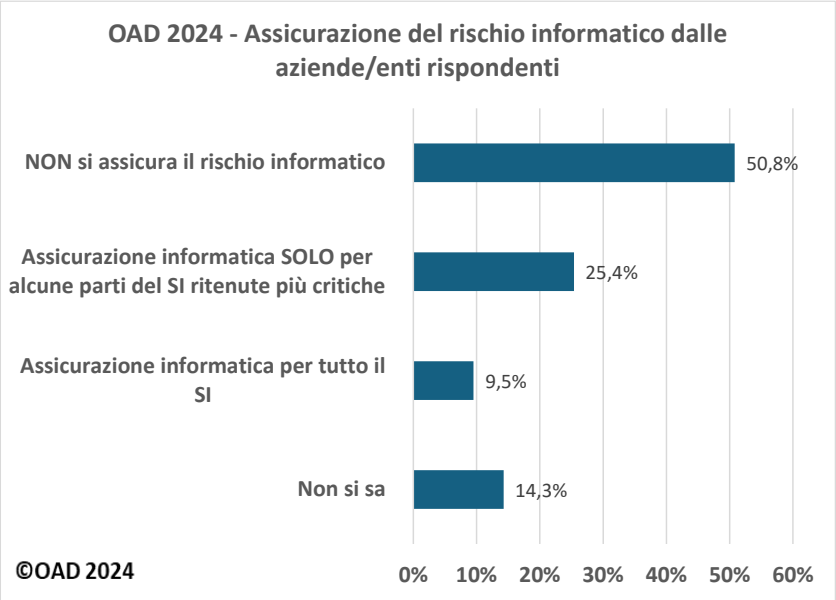


Fig. 7.1.3-4

7.1.4 Auditing sulla sicurezza digitale

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

La fig. 7.1.4-1 indica che il **60,9%** dei rispondenti **effettua auditing per la sicurezza digitale**, e più della metà di questi, il **32,8%**, lo effettua periodicamente **in maniera regolare**. Valori percentuali alti, soprattutto considerando le numerose piccole organizzazioni rispondenti, e per le quali, se non sono del settore ICT, l'auditing della sicurezza digitale non è certo una priorità.

Per chi effettua l'auditing del SI, la fig. 7.1.4-2, indica che la maggior parte, **53,8%**, lo effettua in maniera mista **con personale interno e con esperti esterni**. Il **35,9%** lo effettua solo con personale esterno, ossia terziarizza completamente questa funzione, ed il **10,3%** lo gestisce solo internamente.

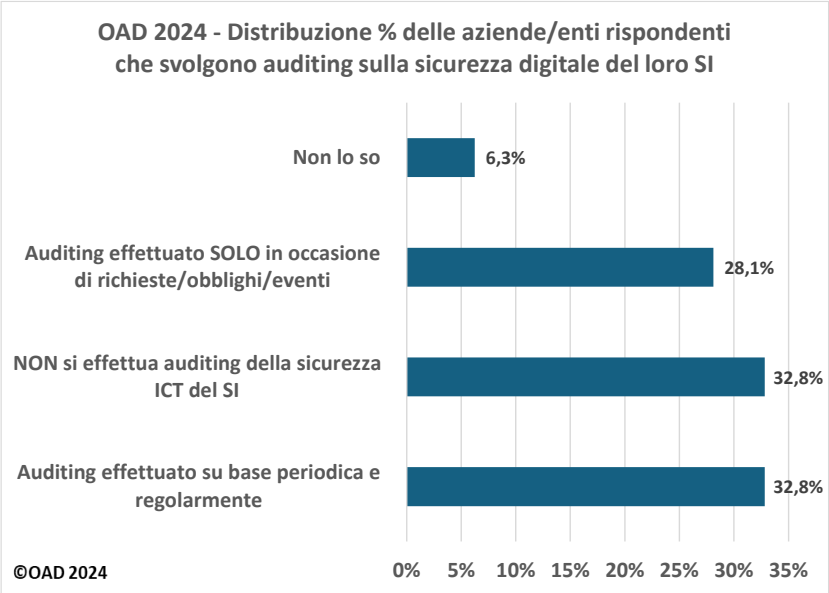


Fig. 7.1.4-1

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 e-CF (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 dai fornitori ICT, 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 SI o di sue parti. Esempi di queste ultime includono, ad esempio, ISO 27001 e 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 individuali sulla sicurezza digitale da parte dell'azienda/ente per il suo personale interno che se ne occupa.
Il **64,5%** delle aziende/enti rispondenti non le richiede per il proprio personale coinvolto nella sicurezza digitale del sistema informativo. Le richiede il **35,5% ,** più di 1/3, ma di questi il **27,4%** le richiede solo per i ruoli e le figure professionali più importanti e di riferimento, quali ad esempio il CISO. Da sottolineare che l'8,1% le richiede per tutto il suo personale coinvolto nella sicurezza digitale.

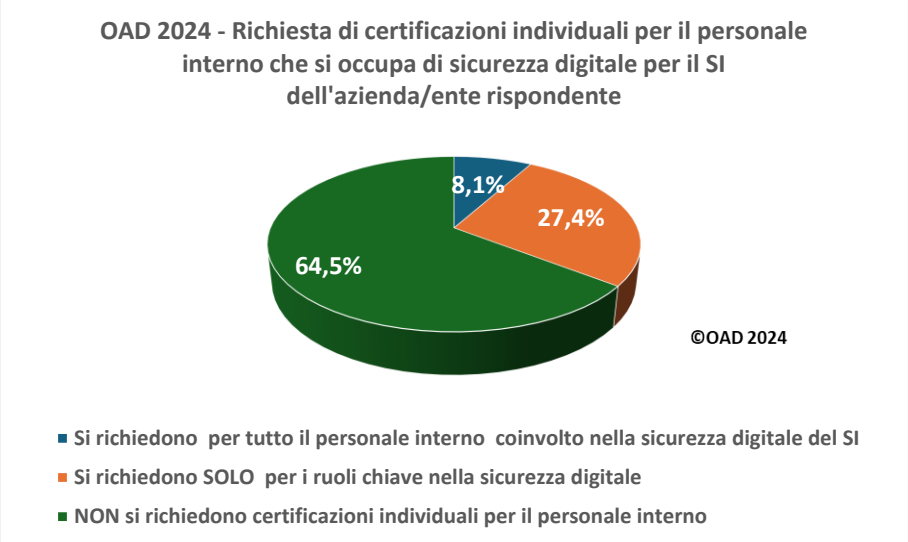


Fig. 7.1.5-1

Nei capitoli e nei paragrafi precedenti si è più volte evidenziata **la tendenza a terziarizzare, in tutto in parte, la gestione della sicurezza digitale**, talvolta, e in crescendo, con più fornitori.

Questa terziarizzazione multipla, (simile al "multi cloud", ma per i servizi e sistemi di sicurezza digitale), richiede reali ed adeguate misure di sicurezza da parte dei vari fornitori, che altrimenti potrebbero diventare, con le loro vulnerabilità, i punti di ingresso per l'attacco all'azienda/ente target finale. I provider di hosting/cloud sono tra i più a rischio per i "supply chain attack". I loro fornitori ed i loro clienti possono essere i punti iniziali di attacchi che poi si possono propagare ad altri loro clienti e fornitori.
In generale, avere una o più specifiche certificazioni sulla sicurezza del SI a livello aziendale per i clienti ed i fornitori collegati informaticamente nella supply chain è un elemento, non l'unico, per una prima garanzia che questi interlocutori dispongono di un adeguato livello di sicurezza digitale.
L'azienda/ente dovrebbe chiedere queste certificazioni ai suoi interlocutori che interagiscono con il suo SI.

La fig. 7.1.5-2 mostra che il **42,72** delle aziende/enti rispondenti le richiede ai fornitori coinvolti, di questi il **25%** le richiede sia a livello aziendale che delle singole persone che interagiscono con il personale dell'azienda/ente.

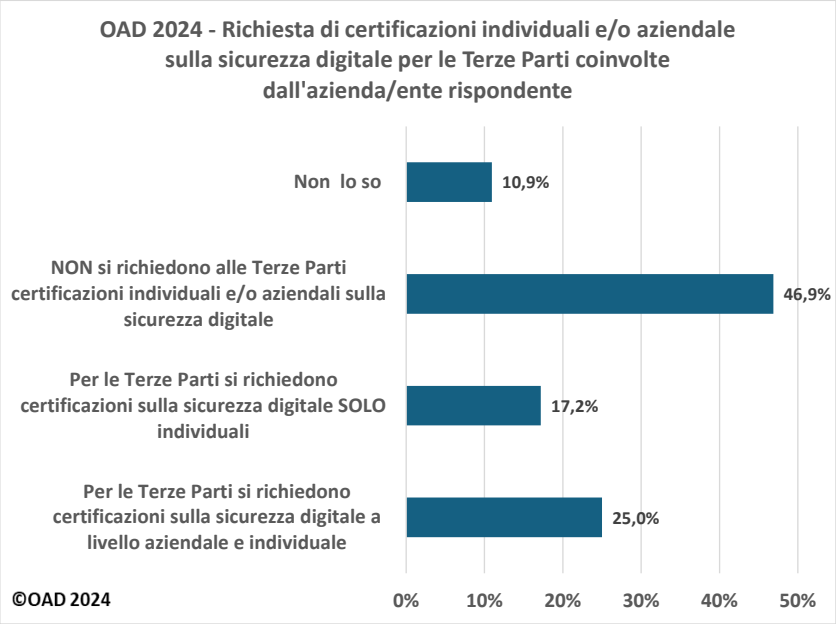


Fig. 7.1.5-2

Importanti le 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 sono già o saranno a breve obbligatorie per poter soddisfare le norme delle già citate normative europee sulla cybersicurezza.

Quante sono tra le aziende/enti rispondenti a OAD 2024 quelle che già hanno certificazioni aziendali sulla sicurezza digitale?
La fig. 7.1.5-3 fornisce la risposta: il **51,6%** non ne ha, e questa percentuale alta fa riferimento alle piccole e piccolissime organizzazioni che hanno riposto al questionario. Il **45,3%** ha certificazioni sulla sicurezza digitale e di questi il **40,6%** per l'intera organizzazione ed il suo SI.
Queste percentuali sono alte, tenendo conto anche del tipo di aziende/enti rispondenti, e confermano come le imprese rispondenti siano nel complesso nella fascia media-alta in termini di livello di sicurezza digitale del loro SI.

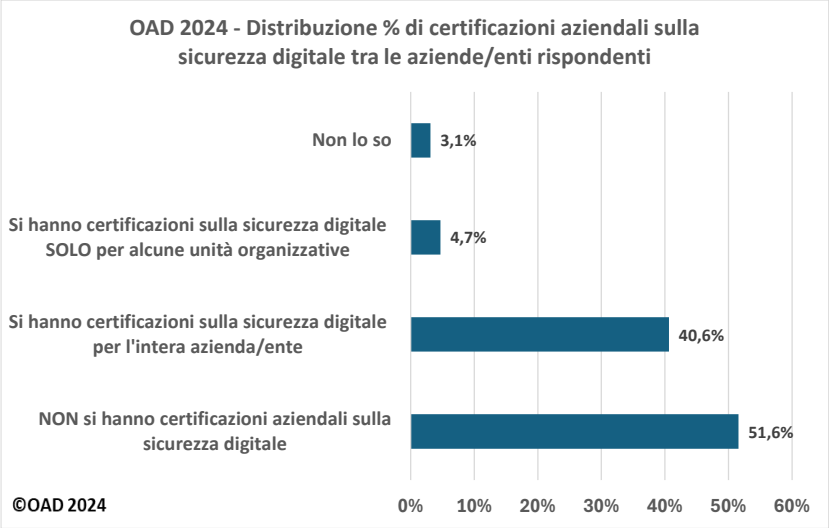


Fig. 7.1.5-3

7.2 Le misure tecniche di sicurezza digitale

Lo schema di riferimento del questionario OAD 2024 (e delle ultime precedenti edizioni) sulle misure tecniche di sicurezza digitali in uso nei SI delle aziende/enti rispondenti, è articolato nelle seguenti principali classi (chiamate anche "famiglie" di misure):

- Architettura complessiva delle misure della sicurezza digitale, integrata (o non) con l'intera architettura del SI oggetto delle risposte
- 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 ICT alternativi.

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

7.2.1 Architetture per la sicurezza digitale

Come mostrato nella fig. 7.2.1-1, **1/3 dei rispondenti** circa **non fa riferimento ad alcuna architettura per il progetto e l'implementazione della sicurezza digitale del SI**. Per gli altri il **25%** la usa **solo** per le parti più **critiche** del SI.

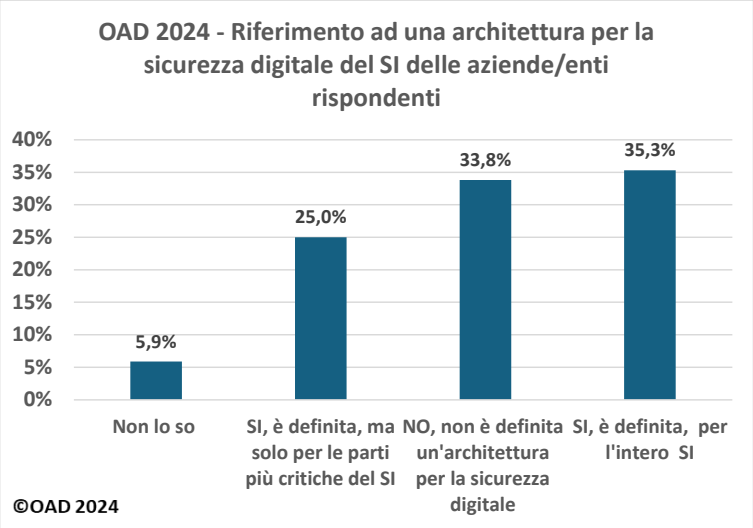


Fig. 7.2.1-1

La fig. 7.2.1-2 mostra **quali** sono le **architetture per la sicurezza digitale** usate come riferimento per il SI delle aziende/enti dei rispondenti.

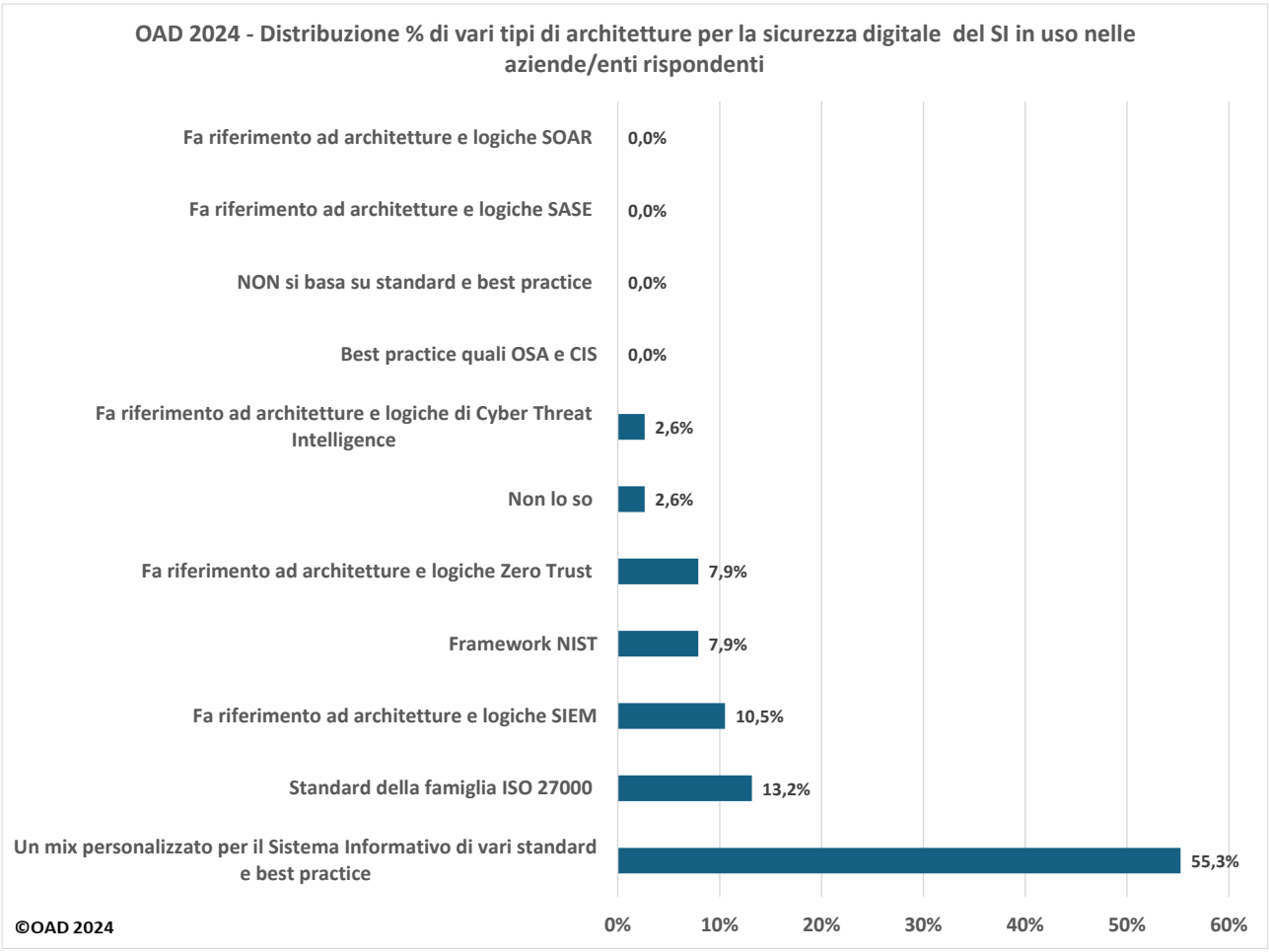


Fig. 7.2.1-2

Più della metà, il **55,3%**, ha adottato e personalizzato **soluzioni che includono diverse logiche e architetture per la sicurezza digitale**. Al secondo posto, con un **13,7%,** il riferimento agli standard della famiglia **ISO 27000**, sicuramente per le aziende/enti che hanno o vorranno avere certificazioni di questo tipo per la sicurezza digitale del loro SI.
Architetture SIEM, Zero Trust ed il Framework NIST seguono con percentuali inferiori.

L'architettura della sicurezza digitale gioca un ruolo basilare per garantire l'alta affidabilità e disponibilità del SI . Come indicato nella fig. 7.2.1-3, quasi **l'80%** dei SI sono in **alta affidabilità**, ma di questi meno della metà, il **35,3%**, garantisce **l'alta affidabilità per tutte le risorse ICT** , mentre il **44,1%** la garantisce solo alle **risorse ICT più critiche** ed importanti.

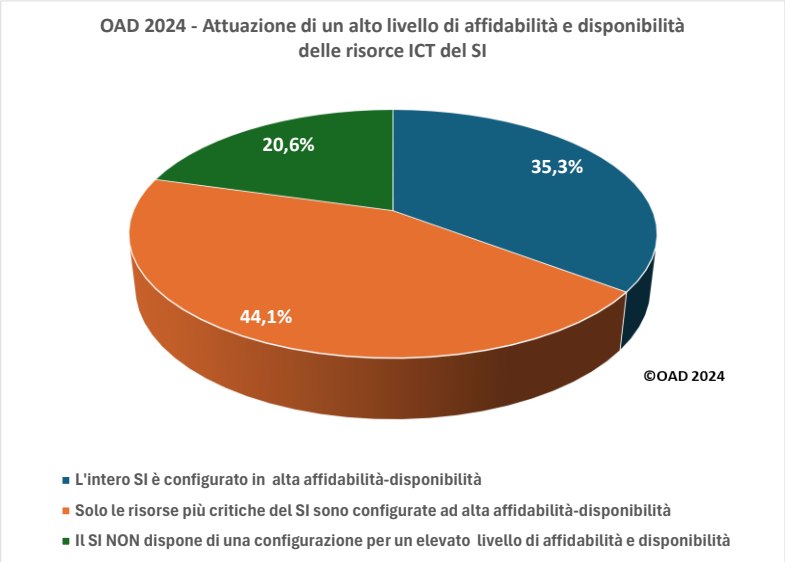


Fig. 7.2.1-3

Nella valutazione del livello di affidabilità di un Data Center il riferimento è lo standard ANSI/TIA 942[59] per il quale si può avere la certificazione TIA del livello implementato.

La fig. 7.2.1-4 mostra i livelli di affidabilità del principale Data Center in Italia del SI (se esite) secondo lo standard ANSI/TIA 942 per le aziende rispondenti.
Più di 1/3, il **36,7%**, dichiara di avere un livello **Tier III** per il proprio SI, ed il **23,3%** di un **Tier IV.**
Il **60%** delle aziende/enti rispondenti a questa domanda **dispone quindi di un Data Center in Italia** con un **elevato livello di affidabilità**. Questo alto livello di affidabilità è congruente con il ruolo del SI che è essenziale

[59] 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.

per la maggior parte delle aziende/enti rispondenti (fig. 6.2-3), ed in taluni casi " risorsa critica" che rientra nelle già citate normative europee quali NIS2, DORA e le altre (si veda fig. 3.6-1 e §3.6).

La fig. 7.2.1-5 indica che solo il **30%** dei Data Center in Italia dei SI delle aziende/enti rispondenti **è certificato ANSI/TIA 942.**

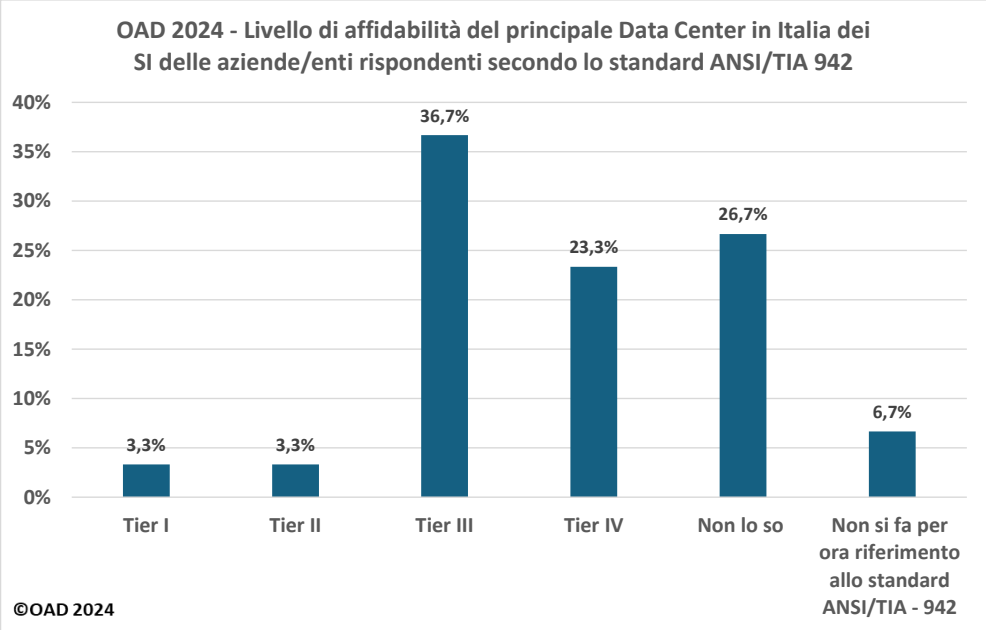


Fig. 7.2.1-4

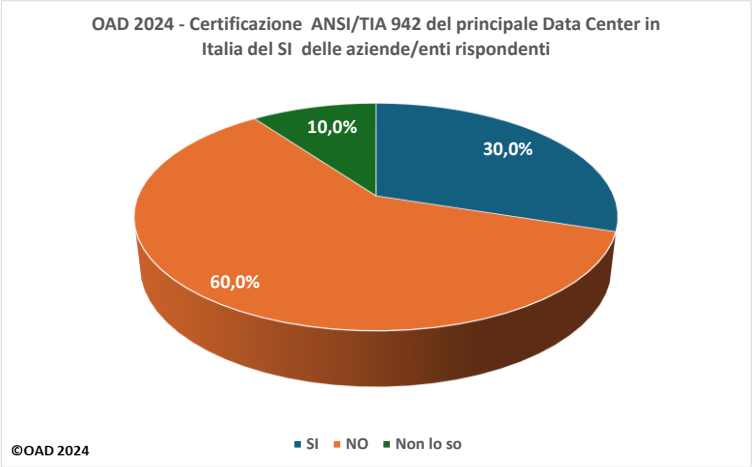


Fig. 7.2.1-5

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 viene chiamata da OAD computer room[60], 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 ICT presenti. In altri casi tali dispositivi sono "distribuiti" nelle diverse stanze degli uffici, così come lo sono i PC degli utenti, ed i controlli dell'accesso fisico sono gli stessi usati per l'accesso a questi locali; in altri casi ancora, tutti i sistemi ICT, a parte i dispositivi d'utente, sono terziarizzati. Presso i provider di hosting/cloud l'accesso fisico non è normalmente consentito ai clienti, se non per l'housing, ma con specifici e severi controlli.

La fig. 7.2.2-1 mostra la situazione emersa dalle aziende/enti rispondenti: per quasi l'**80%** dei casi sono previste misure per il controllo dell'**accesso fisico** di persone nei locali con sistemi ICT, a parte l'eventuale Data Center, per il quale è scontato che siano presenti misure di controolo per gli accessi del personale.

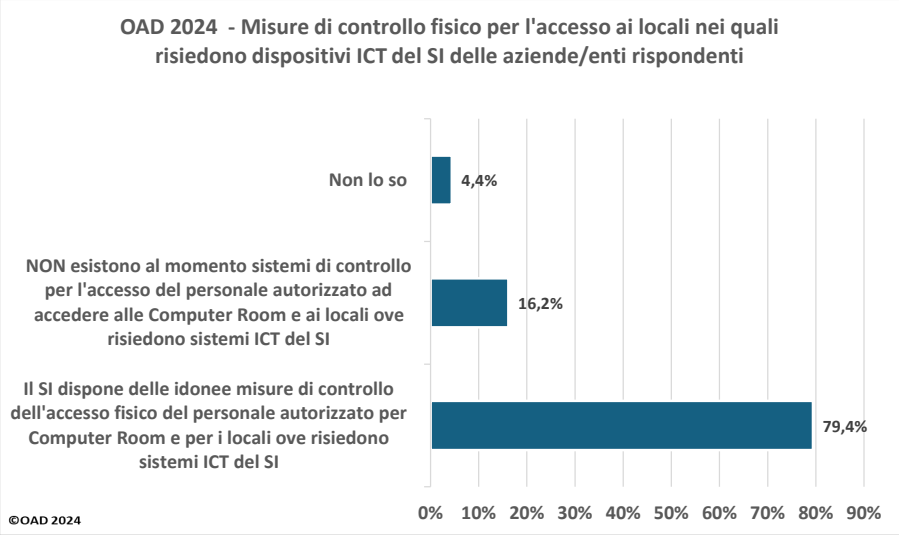


Fig. 7.2.2-1

Sempre escludendo i Data Center, la fig. 7.2.2-2 mostra che nel **75%** dei casi emersi dall'indagine sono in funzione **sistemi di controllo perimetrale**[61] nei locali/computer room ove risiedono sistemi ICT, e di questi il

[60] Le computer room, nel caso di sistemi informativi distribuiti sul territorio, sono gli ambienti dipartimentali dei sistemi informativi di medie o grandi dimensioni.
[61] 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.

il **39,7%** 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.

Un'altra importante misura di sicurezza fisica è l'utilizzo di **sistemi di controllo e prevenzione di interruzioni dell'energia elettrica** per l'alimentazione dei sistemi ICT nelle computer room e negli altri locali in caso di black out energetico con l'attivazione di gruppi di continuità, indicati con l'acronimo UPS (Uninterruptible Power Supply). Esistono diversi tipi di UPS, da quelli più piccoli, basati su batterie in grado di alimentare per un tempo relativamente breve i sistemi ICT in caso di black out (tipicamente consentono lo spegnimento regolare dei sistemi), a quelli di maggiori dimensioni con generatori di corrente elettrica a motore benzina/gas, che possono alimentare i sistemi ICT per giorni e giorni (basta ricaricare il serbatoio); questi ultimi sono normalmente usati per i Data Center, mentre per computer room e locali con sistemi ICT sono normalmente usati sistemi UPS statici a batteria. Volutamente il questionario non è entrato in dettagli tecnici, e si è limitato a chiedere l'eventuale utilizzo di UPS nelle computer room.
Come indicato nella 7.2.2-3, a parte i Data Center (per il quali si dà per scontato che siano in funzione gruppi di continuità), più di 2/3 delle aziende/enti rispondenti, l'**86,8%**, dispone di UPS nei locali/computer room, ma di questi il **52,9%** li ha in funzione solo per i sistemi ICT più critici.

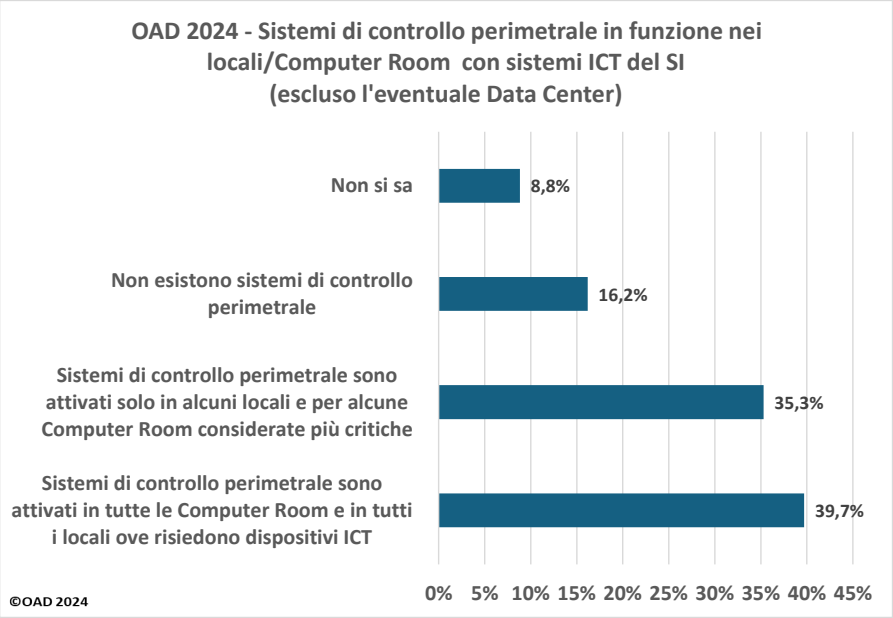


Fig. 7.2.2-2

Oltre che nei Data Center, la sistemazione in rack[62] dei vari sistemi ICT (switch, router, server, etc.) presenti nei locali dell'azienda/ente è importante non solo quale sicurezza fisica, ad esempio con la chiusura a chiave della porta anteriore/posteriore dei rack, ma anche per una loro razionale organizzazione, in particolare per la sistemazione dei cavi in uscita verso gli apparati di rete, che facilita la loro manutenzione ordinaria e straordinaria.
I **rack** sono utilizzati nelle computer room e nei locali ove funzionano dispositivi ICT del SI (non si considera nel questionario il loro utilizzo all'interno dell'eventuale Data Center, dandolo per scontato) nei quali sono **installati ed usati** per **il 73,5%** delle aziende/enti rispondenti.

[62] 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.

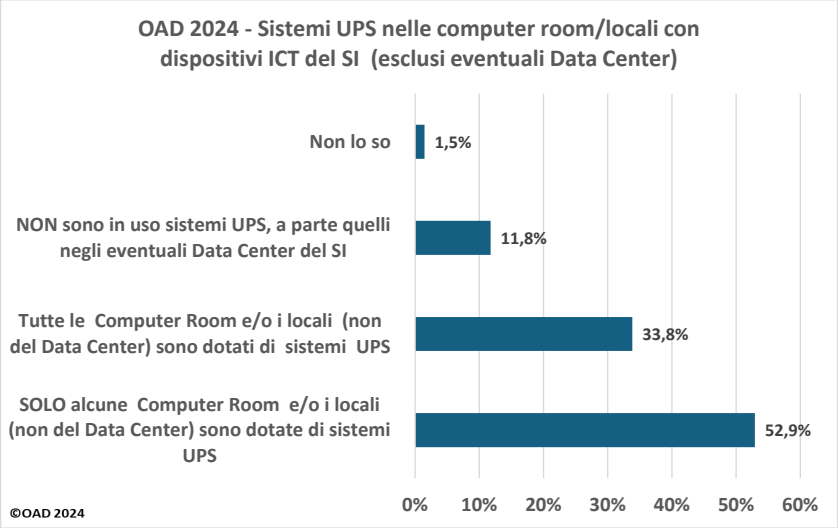


Fig. 7.2.2-3

La fig. 7.2.2-4 dettaglia le principali modalità d'uso dei rack: per il **30,9%,** sono usati per tutti i dispositivi ICT in tutte le computer room e gli altri locali ove operano, mentre per il **29,4**% sono utilizzati solo per i dispositivi più critici, quali ad esempio router, switch, server e sistemi di storage periferici.

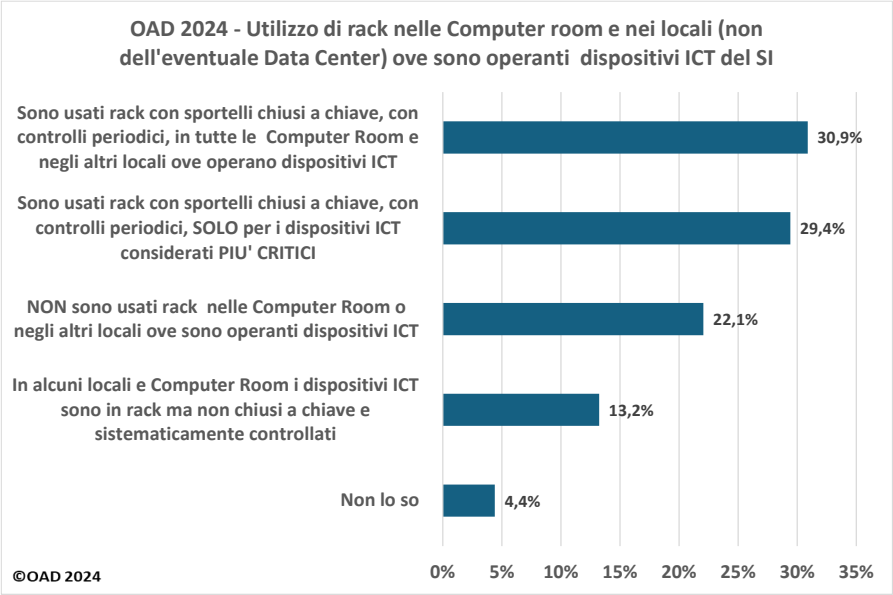


Fig. 7.2.2-4

Per ridurre la possibilità di furto di dispositivi ICT fissi, in particolare lap top e stampanti di piccole dimensioni presenti o lasciate negli uffici, possono essere attivati strumenti di fissaggio e blocco di questi dispositivi sulle scrivanie e sui ripiani ove risiedono. Questa misura di sicurezza fisica **non è utilizzata** dalla maggior parte delle aziende/enti rispondenti, come riportato nella fig. 7.2.2-5. Il **21,7%** utilizza questi strumenti, ma di questi **13,3%** solo per i PC, le workstation e le stampanti più importanti e costose.

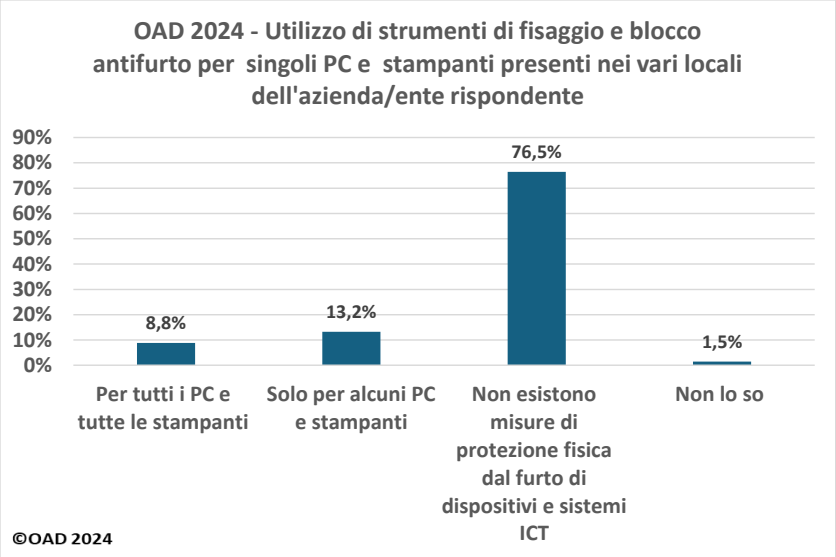


Fig. 7.2.2-5

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[63] sono fondamentali per l'effettiva protezione di un sistema informativo, tenendo anche conto che gli attacchi digitali all'IAA sono nell'indagine OAD 2024 al quarto posto come diffusione, si veda fig. 4.1-1, e furono ai primi posti nelle precedenti indagini OAD dal 2017 al 2021 (dal sito https://www.oadweb.it/it/rapporti-e-relativi-convegni.html si possono scaricare tutti i Rapporti OAD).

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[64], obbligatorio per gli utenti delle pubbliche amministrazioni), l'identificazione biometrica e la grafometria, gli strumenti di gestione e controllo degli accessi quali i diffusi Active Directory e l'LDAP, l'uso delle ACL, Access Control List, per la verifica dei privilegi degli utenti abilitati all'accesso alle applicazioni. Viene sempre più spesso usata per gli utenti finali l'autenticazione "**quasi forte**" che oltre ai dati dell'account utilizza una **OTP**, One Time Password, inviata o in posta elettronica o come messaggio, tipicamente SMS, sul cellulare dell'utente.

La fig. 7.2.3-1 mostra la distribuzione percentuale tra i SI delle aziende rispondenti della diffusione **dell'autenticazione forte/quasi forte** per gli utenti privilegiati. Solo il **11,8%** degli utenti privilegiati la usa per l'accesso a tutti i sistemi del SI, la **maggior parte invece usa un mix** di tecniche di autenticazione a seconda del tipo di sistema e applicazione, oltre che della sua importanza e criticità.

Anche per **l'autenticazione degli utenti finali**, come mostrato nella fig. 7.2.3-2, la maggior parte dei SI, il **58,8%**, richiede l'utilizzo di diverse tecniche di autenticazione a seconda del tipo di applicativo,

[63] 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.

[64] 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.

prevalentemente in funzione della sua criticità e riservatezza per le informazioni trattate, e in certi casi per lo stesso ruolo dell'utente finale.

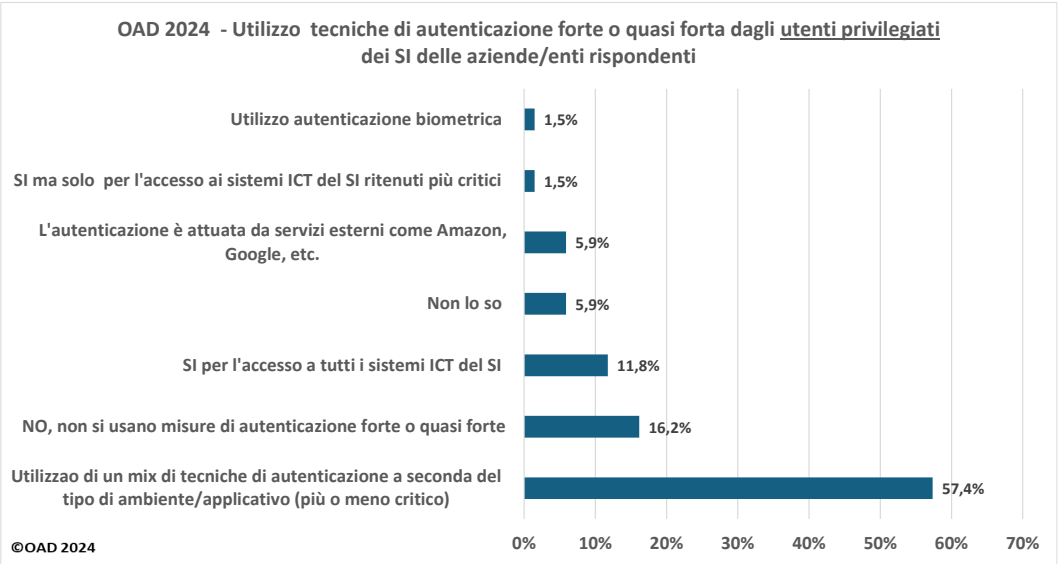


Fig. 7.2.3-1

Poco meno del 30% utilizza le tradizionali tecniche di autenticazione debole e solo il **5,9%** utilizza l'autenticazione forte per ogni ambiente applicativo.
Da notare come nessuno dei SI dei rispondenti utilizzi SPID come strumento di autenticazione al proprio interno (questo anche per il limitato numero di PA rispondenti al questionario OAD 2024).
Ancora trascurabili le percentuali di chi sta introducendo autenticazioni biometriche, quali FIDO2, anche per la necessità ad oggi, nell'ambito Unione Europea (UE), di avere l'autorizzazione ad usarle da parte dei vari Garanti nazionali della privacy.

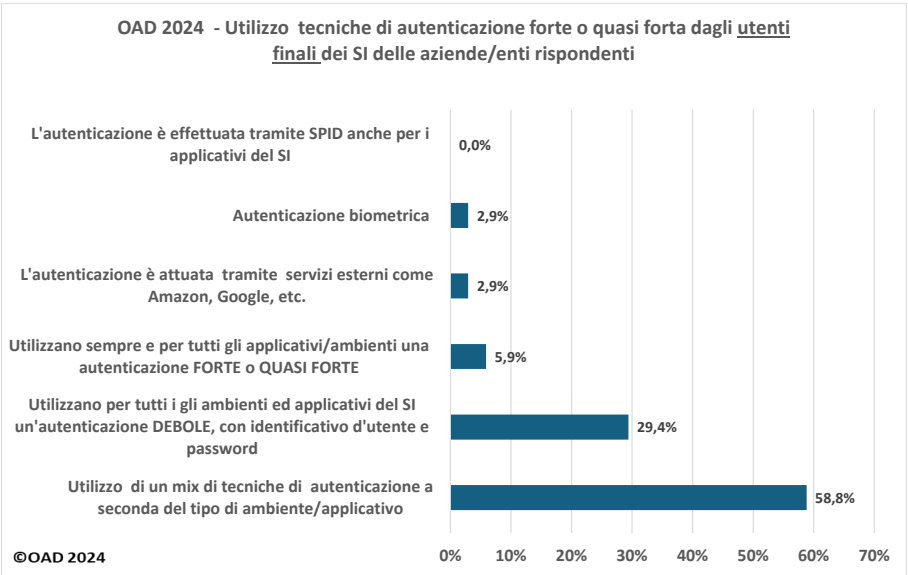


Fig. 7.2.3-2

L'uso delle password è ancora assai diffuso, i sistemi passwordless[65] si basano tutti su tecniche di identificazione biometriche, che richiedono (richiederebbero) l'autorizzazione all'uso da parte delle Autorità Garanti della privacy, o il cambio di alcune regole nell'attuale normativa sulla privacy.

Il tipo e la gestione delle password degli utenti finali e privilegiati è un annoso problema, di fatto per la gran parte ancora aperto. Una password dovrebbe essere lunga come minimo 12-14 caratteri, e al suo interno avere caratteri speciali[66], non tutti però usabili in varie applicazioni. Problema parzialmente rimediabile con autenticazioni forti/quasi forti e con l'uso di PIN[67], che sono codici facili e corti da ricordare e da usare associati a token (smart card, chiavette USB, smartphone). In prospettiva l'eliminazione delle password avverrà tramite sistemi passwordless basati sull'identificazione biometrica, come ormai avviene sempre più spesso per l'accesso a banche, assicurazioni e ad altri servizi via Internet.

Come mostrato in fig. 7.2.3-3 la **gestione delle password** per un SI è **centralizzata** per tutti gli utenti nel **54,3%** dei sistemi informativi, ed è invece lasciata alle decisioni del singolo utente, privilegiato o finale, nel **22,1%**. Nel **17,6%** dei sistemi informativi è centralizzata solo la gestione delle password degli utenti privilegiati. Un piccolo numero di sistemi informativi sta usando/provando tecniche passwordless.

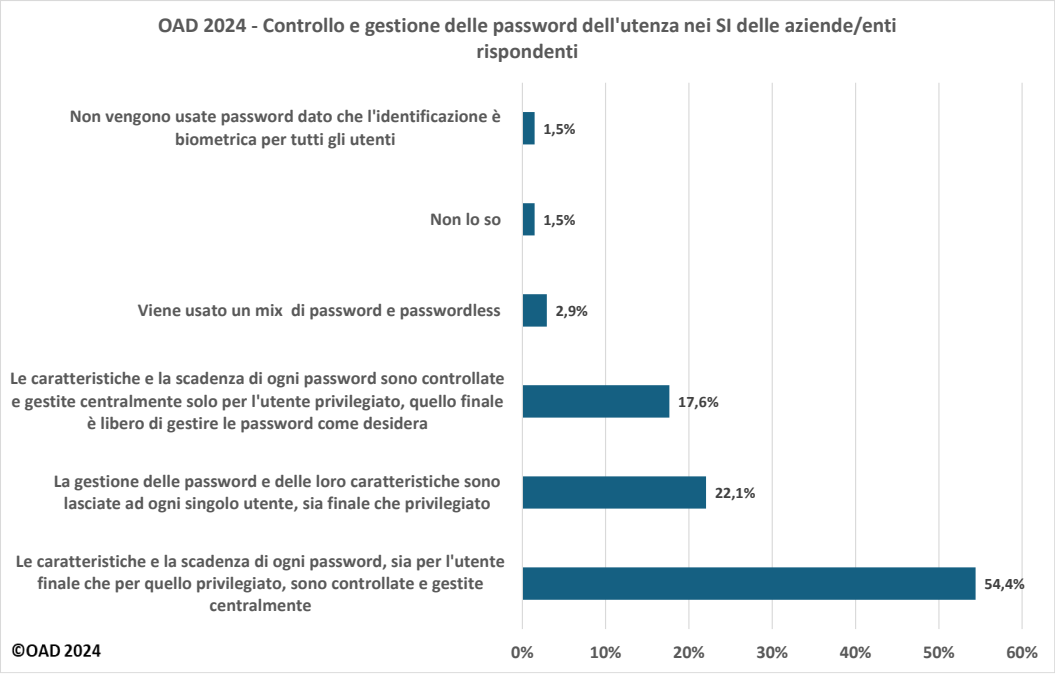


Fig. 7.2.3-3

[65] Varie tecniche biometriche sono già disponibili e stanno diffondendosi nei moderni cellulari tramite riconoscimento facciale e di impronte digitali. Come già evidenziato nel capitolo, il loro uso, in particolare in ambito business, deve seguire le normative sulla privacy ed avere l'autorizzazione dell'Autorità Garante. Tra le principali tecniche e metodiche per l'autenticazione biometrica è di riferimento il Progetto open source FIDO2, https://fidoalliance.org/fido2/

[66] Il termine "caratteri speciali" è usato con definizioni diverse a seconda del contesto (lingua, caratteri stampabili, caratteri di controllo, standard ASCI-UTF-Unicode etc.). e questo porta ad una certa confusione. Senza entrare in dettagli, per l'utente finale di un SI i caratteri speciali da inserire in una password includono tipicamente caratteri non alfanumerici quali ad esempio ~!@#$ %^&*_-+=`|\(){}[]:;"'<>,.?/ .

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

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 **29,9%**, dei sistemi informativi dei rispondenti ha tutte le connessioni ad Internet dupplicate/ennuplicate per garantirne una alta affidabilità e disponibilità, mentre il **23,9%** 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, il **71,6% dei SI monitora e controlla centralmente** funzionalità, prestazioni e livelli di sicurezza digitale delle proprie LAN, che utilizzano per la loro sicurezza specifici strumenti quali DMZ, Firewall, IPS/IDS, VPN, e così via. Il **28,4%** non controlla centralmente le proprie reti, ma di questi solo il **9%** non utilizza specifici strumenti di sicurezza digitale come quelli indicati. Interessante sottolineare come nessuno dei SI dei rispondenti con controllo centralizzato delle proprie reti **non** utilizza specifici strumenti di sicurezza.

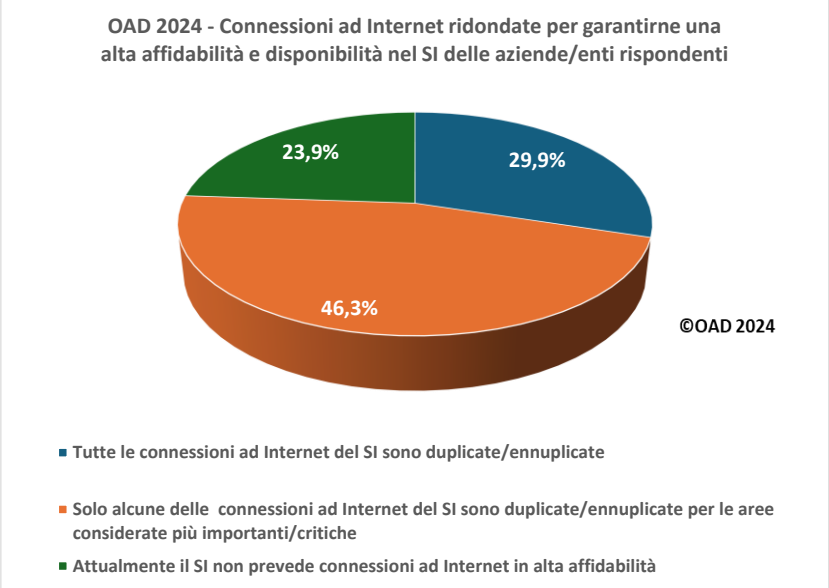


Fig. 7.2.4-1

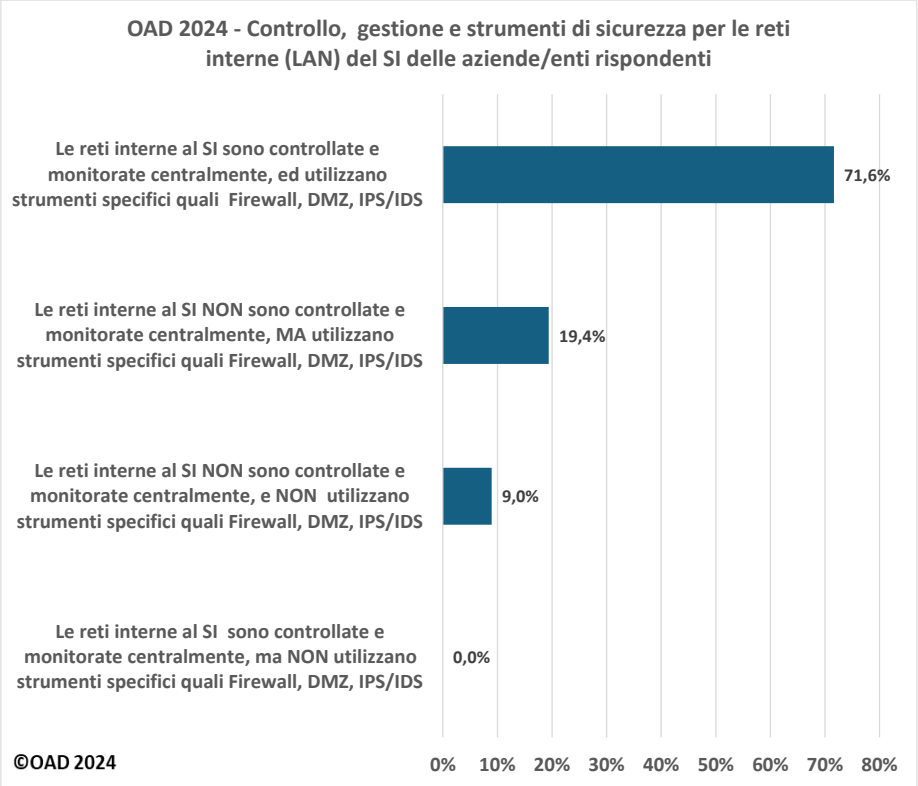


Fig. 7.2.4-2

La fig. 7.2.4-3 evidenzia che per il **80,6%** dei SI delle aziende/enti rispondenti **è crittografato** solo il traffico esterno per/da Internet, tipicamente per i siti web con HTTPS, e per il **14,9% è criptato** sia il traffico con Internet che quello interno sulle LAN.
Un **4,5%** dei SI rispondenti non usa crittografia nemmeno con Internet, non usa quindi HTTPS. Questa, per l'autore, è una percentuale troppo alta anche con una maggioranza di piccole imprese come rispondenti, dato che le funzionalità HTTPS sono presenti su tutti i tipi di browser. Probabilmente chi ha selezionato questa risposta o ha sbagliato o ha fatto riferimento al proprio sito web che non supporta ancora l'HTTPS.

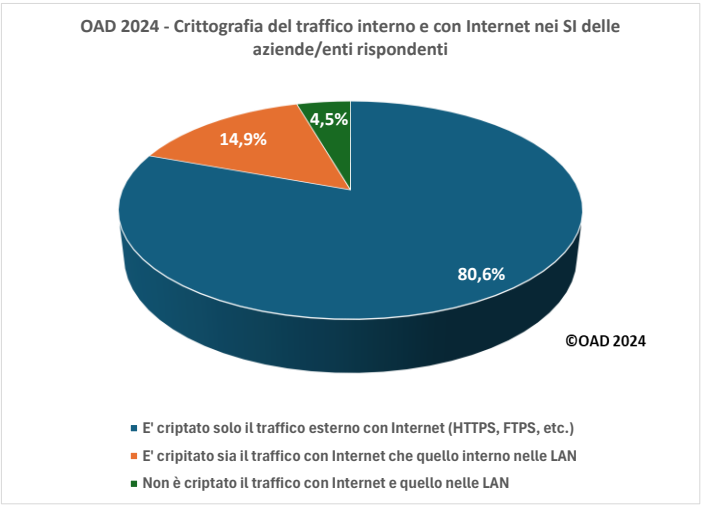


Fig. 7.2.4-3

La fig. 7.2.4-4 mostra quali SI delle/dei rispondenti usano logiche ed architetture SASE[68] per potenziare il livello di sicurezza delle loro reti, e con fornitori di SASE in cloud, di far fronte ad attacchi tipo Dos/DDos
Il **61,2%** di SI delle aziende/enti rispondenti **non utilizza soluzioni SASE** , ma il **28,4% sì**. Relativamente alta la percentuale dei "non so", dovuta quasi certamente ad una non conoscenza di questo tipo di soluzioni.

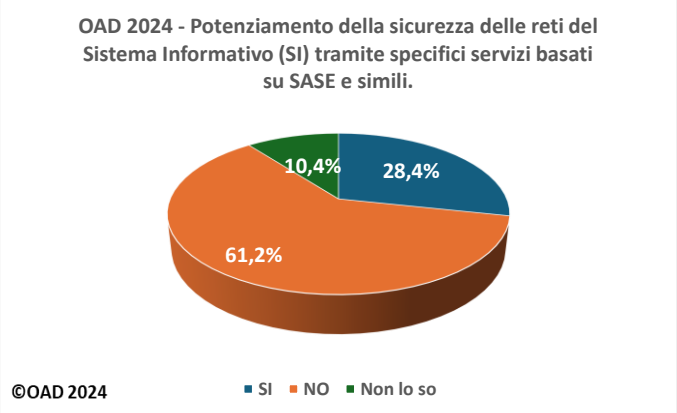


Fig. 7.2.4-4

7.2.5 Misure di sicurezza delle applicazioni nei SI

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. La specifica responsabilità del fornitore di software (e più in generale di una qualsiasi prodotto ICT) nel garantire per esso gli idonei livelli di scurezza digitale rientra nel già citato Cybersecurity Act dell'UE (si veda §3.4): ogni prodotto software, o con software interno (emebedded) perché possa essere venduto dovrà essere certificato da appositi enti dell'UE, in un logica tipo Common Criteria europeizzati.
Al di la sicurezza intrinseca del software, essa può essere corrotta anche da errate installazioni e configurazioni, e da moduli aggiuntivi per l'integrazione e l'interoperabilità con altre applicazioni.
Inoltre, come già riscontrato nelle precedenti indagini OAD, alcune società acquirenti di software commerciali non rinnovano poi, spesso per motivi economici, 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.
Sul complesso ed ampio ambito della sicurezza degli applicativi software, OAD 2024 volutamente ha posto nel questionario poche domande ma tali da poter rilevare la tendenza delle aziende/enti rispondenti.

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

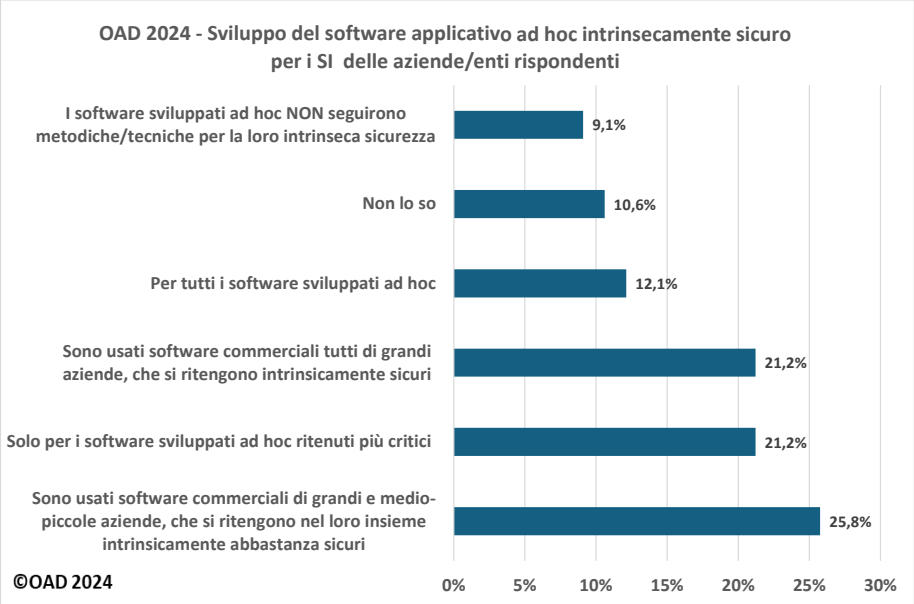


Fig. 7.2.5-1

La fig. 7.2.5-1 mostra che il **33,3%** 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 **21,2%** dichiara che tale sviluppo digitalmente sicuro è stato effettuato solo per gli applicativi più importanti e più critici per l'azienda/ente. il **47%** delle aziende/enti rispondenti **non ha sviluppato software ad hoc**, ma ha acquisito e posto in produzione **prodotti commerciali** che sono ritenuti intrinsecamente sicuri o abbastanza sicuri.

La seconda domanda riguarda **la verifica ed il test della sicurezza del codice software sviluppato ad hoc prima della sua messa in produzione**, e le risposte emerse sono riportate nella fig. 7.2.5-2: il **40,9%** del software sviluppato ad hoc viene verificato/testato prima della sua messa in produzione, e di questi il **28,5%** riguarda verifiche e test solo del software considerato più importante e critico.

Il controllo delle autorizzazioni per l'accesso nei vari applicativi e che cosa poter fare, ossia **la profilatura degli utenti per ogni applicativo**, è un altro elemento basilare per la loro sicurezza. La fig. 7.2.5-3 evidenzia che **quasi nel 90% dei SI** delle aziende/enti rispondenti sono attivi strumenti di controllo degli accessi e delle autorizzazioni, ma di questi solo il **41,5%** è effettuato per tutti gli applicativi.

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 **l'80%** dei sistemi informativi li usa, ma il **47,7 %** solo davanti ai server che supportano gli applicativi più importanti e/o più critici per l'azienda/ente rispondente.

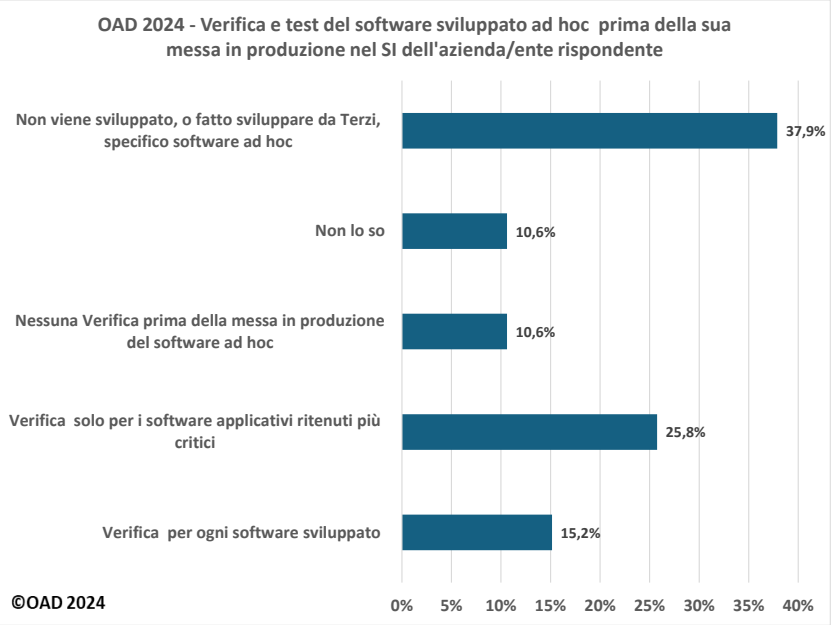


Fig. 7.2.5-2

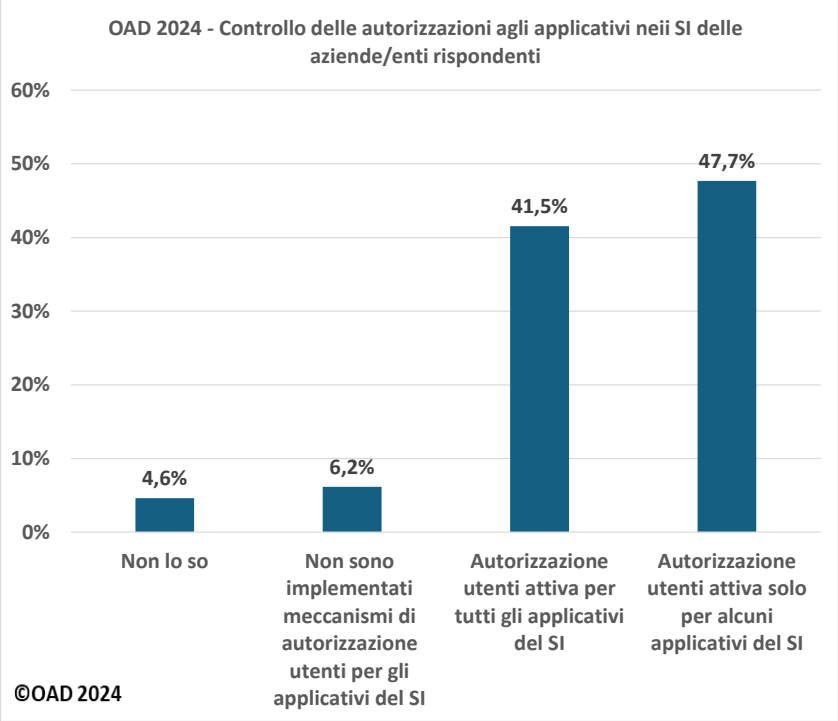


Fig. 7.2.5-3

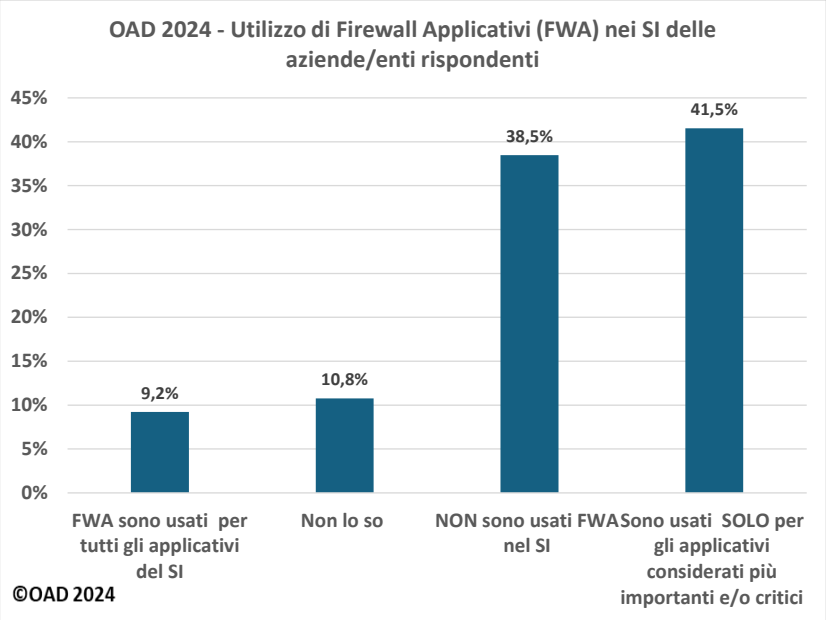


Fig. 7.2.5-4

Un altro aspetto fondamentale per la sicurezza digitale degli applicativi è la loro **continua e sistematica manutenzione correttiva**: tempestivo aggiornamento delle versioni rilasciate, installazione tempestiva di fix e patch, e così via.

La fig. 7.2.5-5 mostra che l'**84,7%** delle aziende/enti rispondenti gestisce la manutenzione correttiva degli applicativi, e di questi il **58,5%**, ossia ben più della metà, la effettua per tutti gli applicativi operanti nel SI.

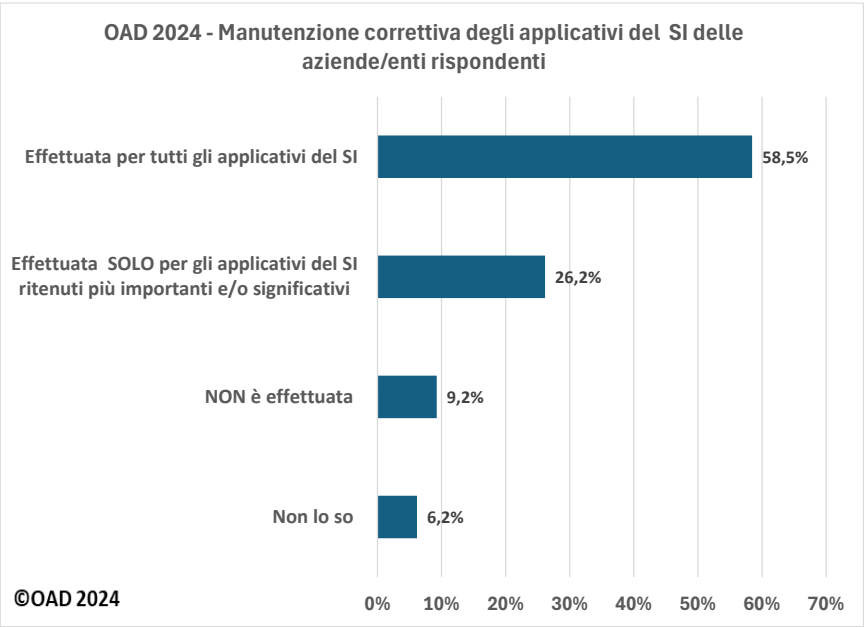


Fig. 7.2.5-5

7.2.6 Misure tecniche di sicurezza digitale per la protezione dei dati

I dati trattati 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.

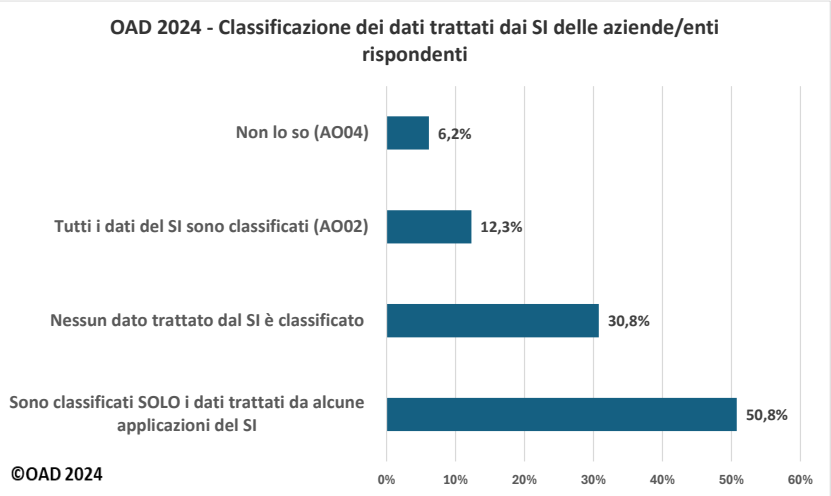


Fig. 7.2.6-1

La situazione della **classificazioni dei dati** per i SI oggetto dell'indagine è evidenziata nella fig. 7.2.6-1. Il **63,1%** delle aziende/enti rispondenti dichiara di aver classificato i dati, e di questi il **50,8%** dichiara di averlo fatto solo per i dati trattati da alcune applicazioni: tipicamente i dati personali e quelli confidenziali per il business e/o per le attività. Stupisce che per il **30,6%** dei SI non sia stato (ancora) classificato alcun dato, pur essendoci leggi sulla privacy da più di 25 anni! Per approfondire, si è correlata questa risposta negativa alle dimensioni delle aziende/enti rispondenti, ed il risultato è mostrato in fig. 7.2.6-2.

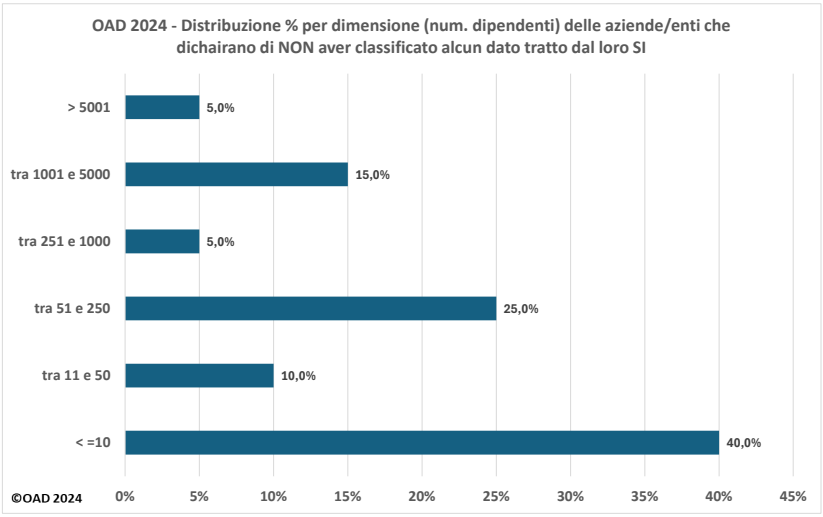


Fig. 7.2.6-2

Il **75% che** dichiara di **non aver classificato** i dati trattati dal SI appartiene ad organizzazioni al di sotto dei 250 dipendenti, e con una forte %, in pratica **la metà**, di quelle piccolissime al di sotto dei 10 dipendenti.
Rimane comunque strano e preoccupante che il restante 25% sia di grandi organizzazioni. L'autore si augura che la/il rispondente o non conoscessero la situazione della loro azienda/ente, o non sapessero il significato di "classificare i dati"[69].

La **crittografia**, con 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. 7.2.6-3 riporta la situazione sul trattamento dei dati personali, in particolare di quelli "sensibili"[70]: il **43,8%** dei sistemi informativi delle aziende/enti rispondenti criptano i dati personali e quelli sensibili.
La % piuttosto alta di chi non sa rispondere dipende, a giudizio dell'autore, dai molti rispondenti che non sono figure tecniche, e che quindi ignorano una simile informazione (e non l'hanno richiesta a chi eventualmente la sapeva nell'ambito della loro organizzazione).

Vengono poi **criptati dati** ritenuti riservati e confidenziali, non di tipo personale, dal **62,9%** delle aziende/enti rispondenti, come mostrato nella fig. 7.2.6-4. Una percentuale alta, che da un lato indica come i SI dei rispondenti abbiano un buon livello di misure di sicurezza, dall'altro come gli strumenti per criptare dati e soprattutto file siano ormai assai diffusi e relativamente facili da usare.

Le chiavette USB sono un comodo strumento per copiare file, e date le loro attuali grandi capacità di storage, anche per copiare directory di qualche Tera Byte. Quasi tutti i dispositivi ICT, dai PC ai server, dagli storage alle unità di rete, hanno porte USB per default aperte ed utilizzabili, che dovrebbero invece essere controllate/bloccate.

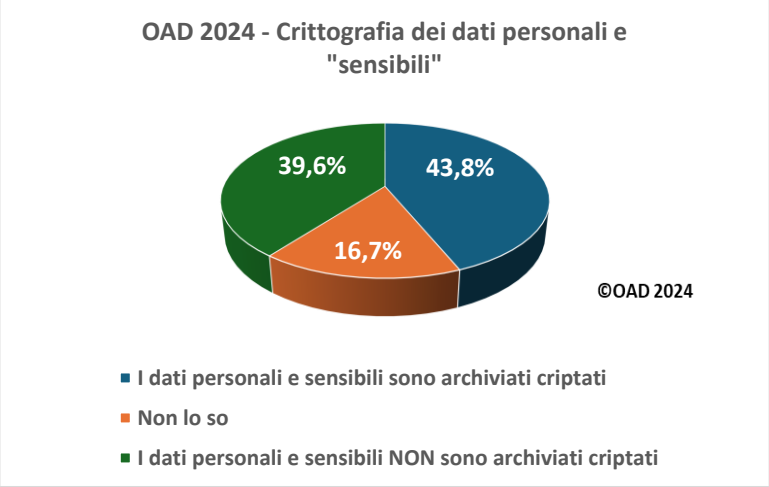


Fig. 7.2.6-3

[69] "Classificare i dati" significa effettuare un assessment dei dati tratti per applicazione, ed associare a ciascuno di loro il livello di segretezza idoneo, quale ad esempio Confidenziale, Riservato, Uso interno, Pubblico. In funzione del livello di segretezza del dato, dovranno essere implementati gli strumenti di sicurezza perché l'applicativo ed il SI li possano assicurare.
[70] Il termine di "dato sensibile" non è più citato nella direttiva GDPR, ma lo era nelle precedenti; esso è di comoda "sintesi", ben conosciuto anche al di fuori degli addetti ai lavori, e si riferisce a dati personali di tipo sanitario, religioso, politico, sindacale, etc.

Le chiavette sono un utile strumento per fare delle copie dei propri file, archiviandoli in esse criptati per sicurezza (è facile perderle … o farsele rubare), ma per questo anche utili per rubare "fisicamente" significative quantità di file.

La fig. 7.2.6-5 mostra che la maggior parte, **il 67,7%**, delle porte USB nei dispositivi ICT dei SI oggetto dell'indagine sono **liberamente utilizzabili**, anche se è possibile bloccarle configurando opportunamente lo stesso dispositivo.

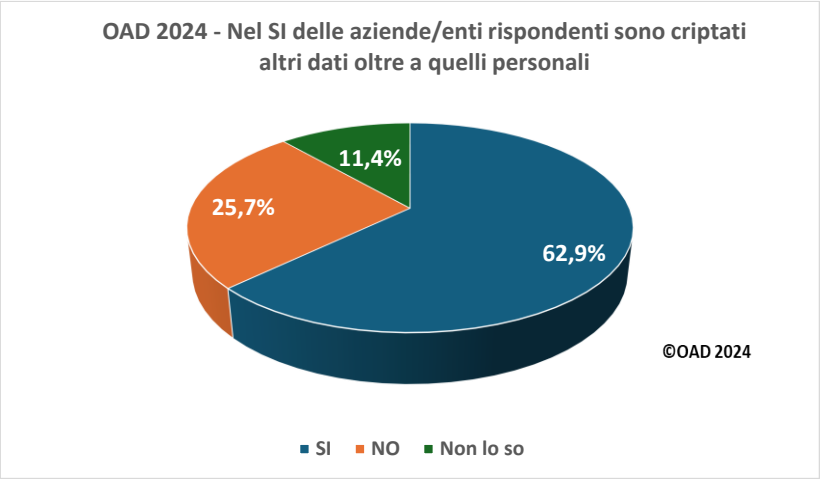


Fig. 7.2.6-4

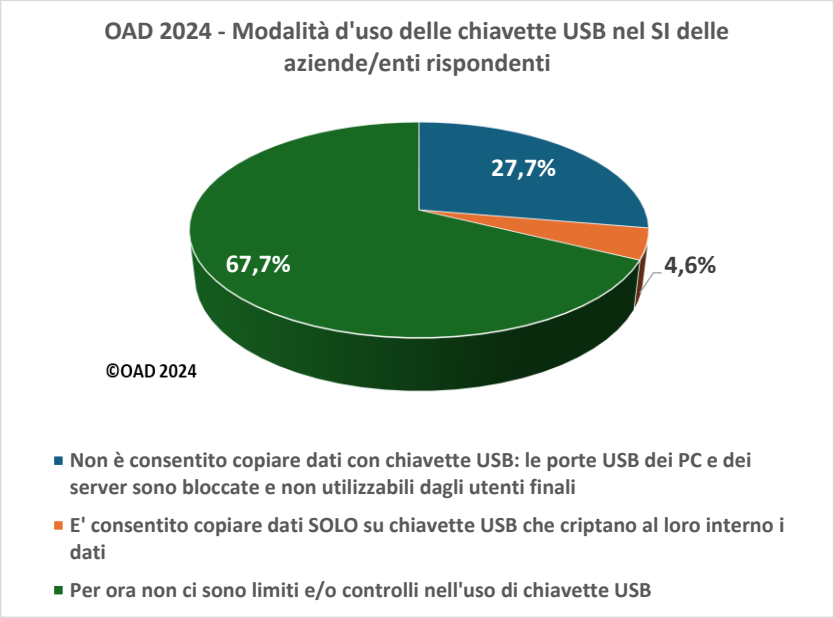


Fig. 7.2.6-5

Il **backup** è una essenziale misura per la protezione dei dati e dei programmi di un SI, e nelle prime indagini OAD si era rilevato come molte aziende/enti rispondenti lo effettuassero parzialmente e/o in maniera poco professionale.

La fig. 7.2.6-6 riporta i dati emersi dalla presente indagine, che sono significativamente migliorativi: il **44,6%** 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 **35,4%** effettua regolarmente i backup, ma non cripta le copie e non trasferisce questi dati su media removibili, allocandole poi in diverse sedi.
Solo il **3,1%** non gestisce in maniera omogenea ed automatizzata il backup, ed il **6,2%** lascia la responsabilità del backup al singolo utente, tipica soluzione in uso nelle piccolissime organizzazioni.

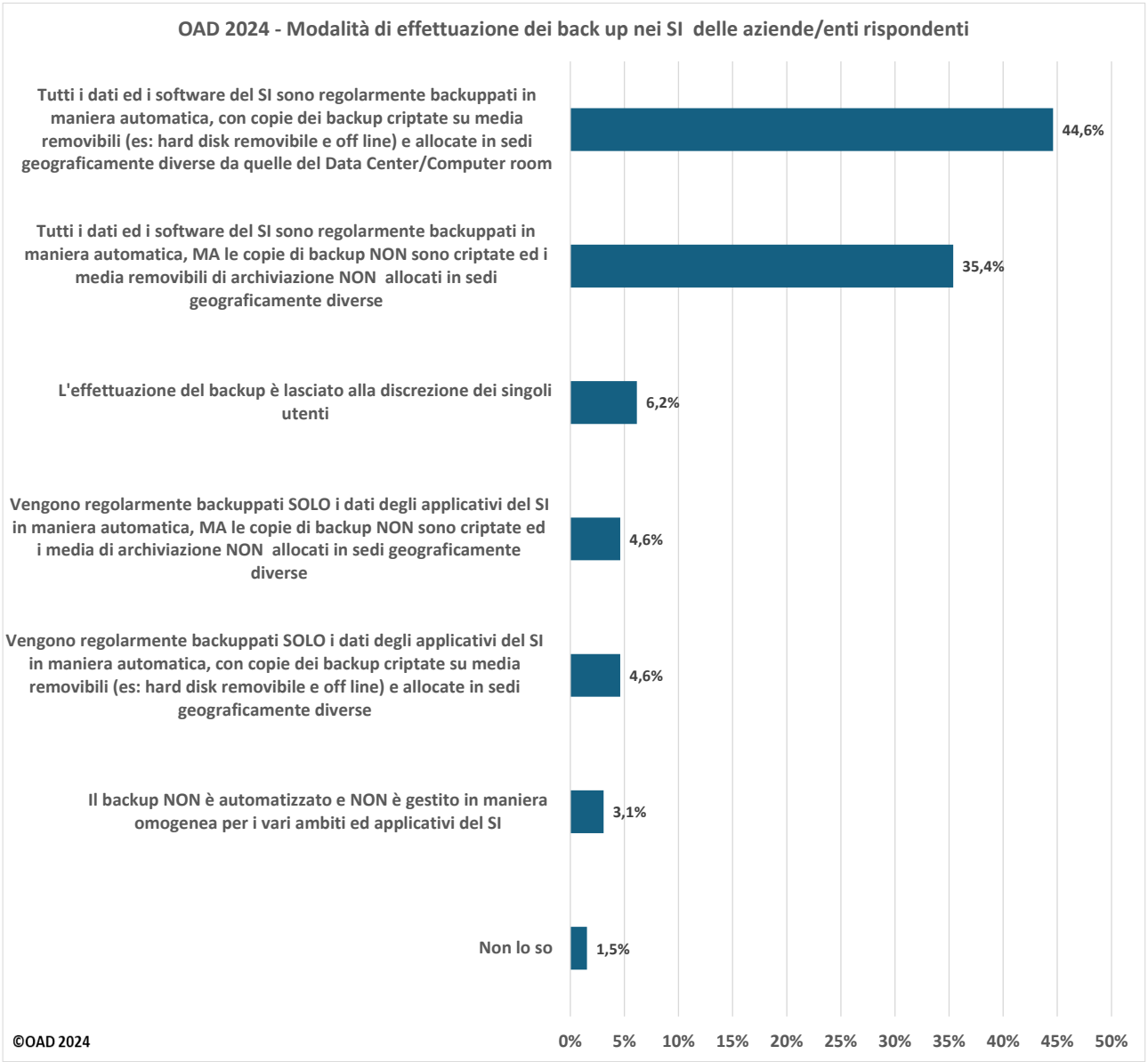


Fig. 7.2.6-6

Per una effettiva disponibilità dei dati del sistema informativo non solo occorre effettuare frequenti, periodici e sistematici backup, ma anche saper **ripristinare** i sistemi ICT, in caso di loro malfunzionamento o blocco o rottura, **tramite i dati di backup**.

La fig. 7.2.6-7 mostra che il **75,4%** delle aziende/enti rispondenti ha definito, ufficializzato ed utilizza **procedure per come ripristinare i vari sistemi dai dati dei backup**, ma di questi solo il **35,4%** *periodicamente le verifica e prova con test*, rendendosi quindi in grado di usarle correttamente e tempestivamente in caso di bisogno. Il **20%** non ha o non utilizza procedure di ripristino.
Questa percentuale, non trascurabile, è dovuta, a giudizio dell'autore, al numero elevato di piccole e piccolissime organizzazioni che hanno partecipato all'indagine OAD.

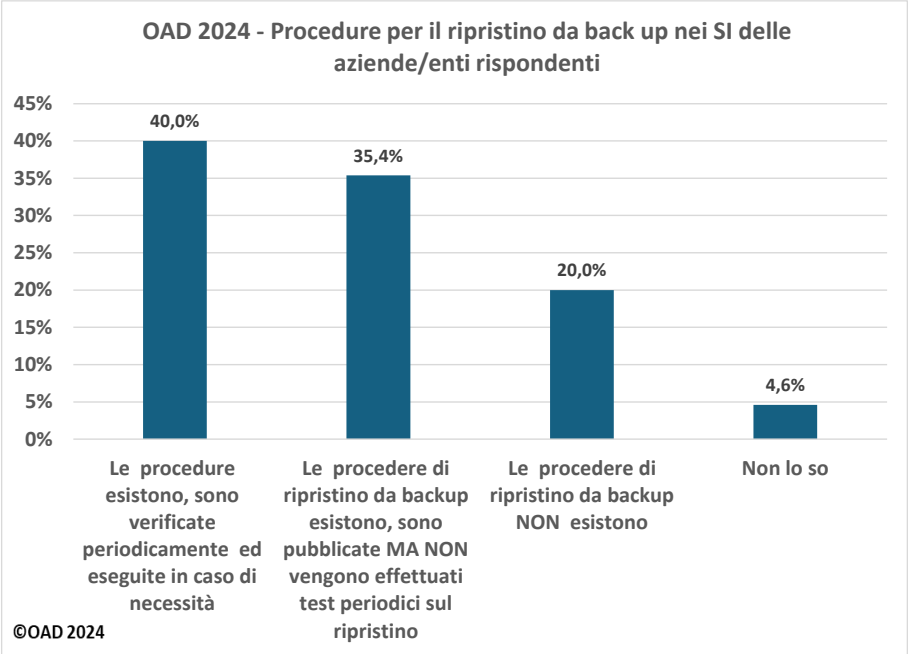


Fig. 7.2.6-7

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

Le misure e gli strumenti per la gestione della sicurezza digitale di un sistema informativo (SI) nel suo complesso sono un insieme di strumenti tecnici ed organizzativi, ed alcuni possono essere considerati anche come misure e strumenti specifici di contrasto. L'autore ha preferito evidenziare in un paragrafo a sé stante gli strumenti di solito usati per la gestione operativa della sicurezza digitale, che in molti casi è integrata con la gestione del SI e dei suoi componenti (reti, parte terziarizzate, etc.).

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 SI, includono i sistemi di directory di tutte le risorse digitali e delle loro configurazioni e licenze (ICT Asset Management), i sistemi di monitoraggio e controllo delle funzionalità e delle prestazioni dei sistemi ICT, i sistemi di raccolta, correlazione e gestione di tutti gli eventi (SIEM) rilevati dai sistemi ICT, ed in particolare i sistemi per la raccolta e la gestione dei log dei sistemi ICT e degli utenti (che sono sovente inclusi nei sistemi SIEM), i sistemi SOAR (Security Orchestration, Automation

and Response), che consentono di automatizzare e di velocizzare la gestione della sicurezza digitale, in particolare degli incidenti/attacchi digitali, i sistemi SASE (Secure Access Service Edge), i sistemi di analisi comportamentali di utenti e risorse ICT.
Oltre a queste misure e strumenti, che per lo più operano in maniera continua e in tempo reale, sono considerati alcuni strumenti e metodiche 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 SI, negli ultimi due anni sta ri-emergendo l'Intelligenza Artificiale, che include i sistemi esperti ed il machine learning.

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

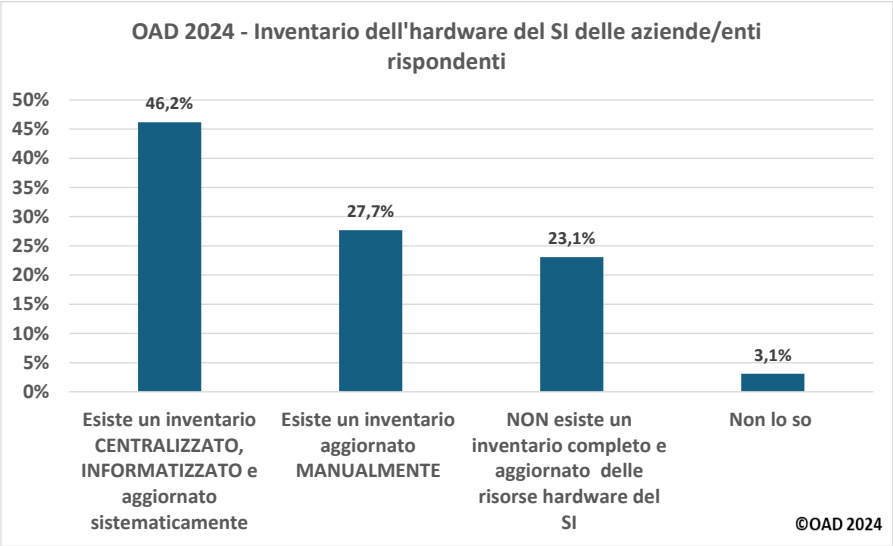


Fig. 7.2.7-1

La fig. 7.2.7-1 mostra la situazione per **l'inventario delle risorse hardware** del SI dell'azienda/ente rispondente. il **23,1%** non ha un inventario delle risorse hardware, mentre il **73,8%** ha un inventario, ma realizzato in differenti maniere: il **27,7%** di questi realizza una raccolta manuale delle informazioni sull'hardware esistente in fogli elettronici o in altri tipi di documenti; il **46,2%** ha un inventario centralizzato, aggiornato automaticamente con appositi software.

Le **licenze per l'hardware del SI**, necessarie in particolare per la sua manutenzione, dovrebbero essere associate all'inventario, per una loro più efficace gestione. La fig. 7.2.7-2 mostra la situazione emersa dall'indagine, limitata ai SI che dispongono di un inventario dell'hardware: per essi tale associazione esiste per il **56,3%** dei casi, ma di questi solo il **37,5%** riguarda tutte le risorse hardware, e nel **43,8%** dei casi tale associazione non esiste.

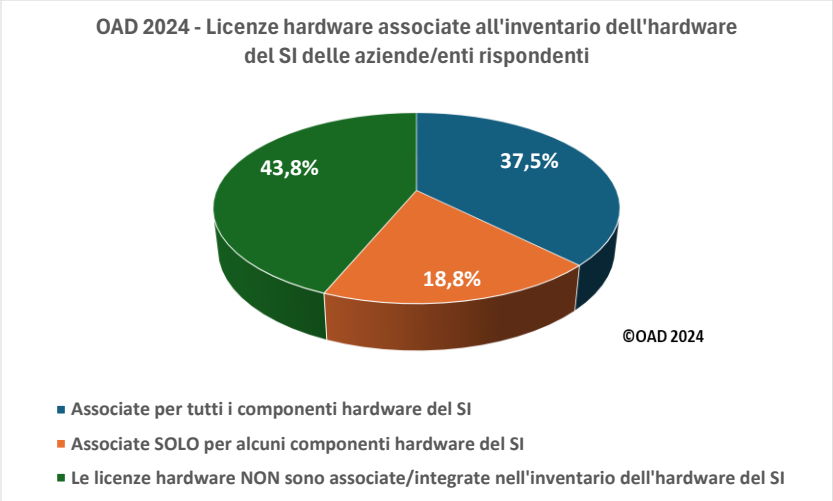


Fig. 7.2.7-2

Per quanto riguarda l'**inventario del software** del sistema informativo, sia di base sia applicativo, la fig. 7.2.7-3 evidenzia che il **30,8%** delle aziende/enti rispondenti non ha un inventario del software, il **66,2%** ha un inventario, ma realizzato in differenti maniere: il **26,2%** realizza una raccolta manuale delle informazioni sul software esistente in fogli elettronici o in altri tipi di documenti, probabilmente gestito e conservato nelle diverse sedi periferiche dove si trovano i dispositivi ICT; il **40%** ha un inventario centralizzato, aggiornato automaticamente con appositi software.

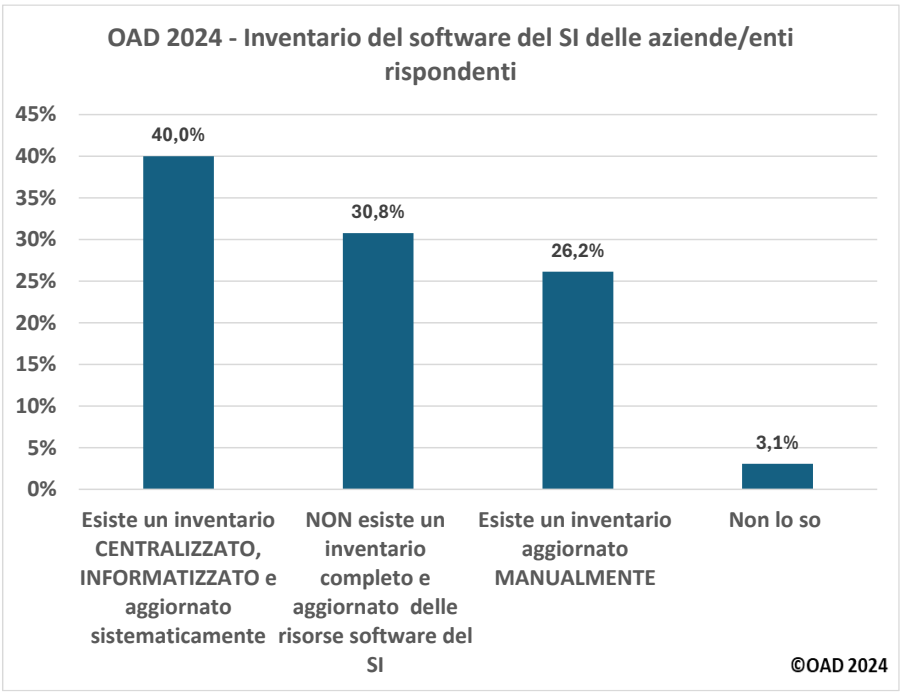


Fig. 7.2.7-3

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 inventario del software. La fig. 7.2.7-4 mostra la situazione emersa: il **53,5%** 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 **27,9%** l'ha per tutti i software inventariati, mentre il **16,3%** ha correlato le licenze solo per alcuni software.

Gli inventari dell'hardware e del software dovrebbero poi essere tra loro correlati ed integrati, per poter saper su quale hardware sono in funzione determinati programmi. La situazione su tale integrazione, limitata alle sole aziende/enti che hanno dichiarato, nelle precedenti risposte, di avere inventari dell'hardware e del software, è mostrata in fig. 7.2.7-5: il **73,8%** ha i due inventari dell'hardware e del software correlati/integrati tra loro.

Dalle risposte sugli inventari hardware e software e l'eventuale loro associazione/integrazione con le relative licenze emerge che:

- La situazione, come trend, è nettamente migliorata rispetto alle indagini OAD degli anni precedenti; questo sicuramente grazie alla crescente disponibilità (e conoscenza) di sistemi software, anche open source e gratuiti, che automatizzano l'assessment delle risorse ICT;
- l'hardware è più inventariato rispetto al software, almeno per i SI dei rispondenti; questo è anche dovuto ad una relativa maggior complessità nella realizzazione (e gestione) di un inventario di un medesimo software che opera su diversi hardware: si pensi ad esempio ai sistemi operativi, alle applicazioni sui PC, e così via;
- che alcune alte percentuali "negative", quali ad esempio quelle per l'associazione solo parziale o totalmente assente delle licenze ai relativi inventari, sono dovute alla larga percentuale di piccole e piccolissime organizzazioni tra i rispondenti, per le quali, avendo pochi sistemi ICT, il problema della loro gestione è assai semplice.

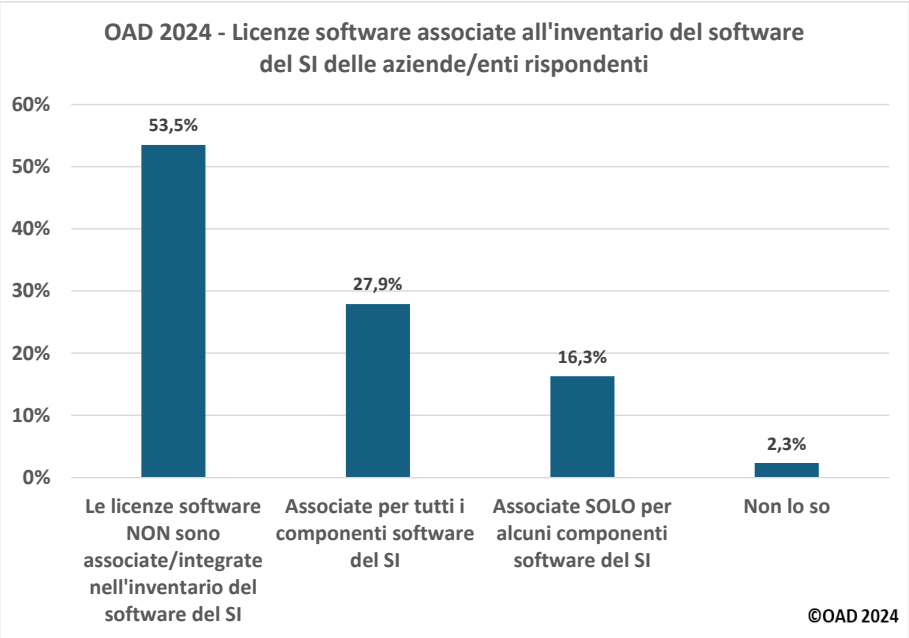


Fig. 7.2.7-4

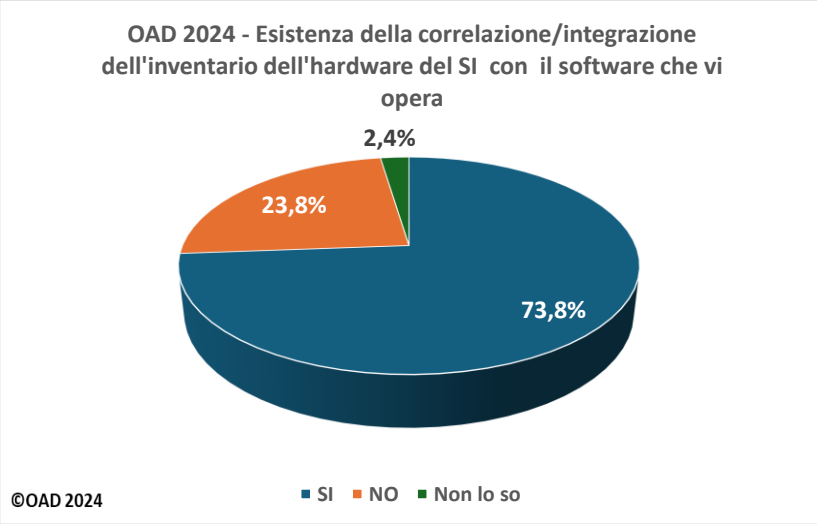


Fig. 7.2.7-5

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 SI; 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 2024 si è cercato di semplificare e ridurre le domande su questo ampio e complesso argomento, e la fig. 7.2.7-6 mostra i risultati emersi. A parte chi non ha saputo rispondere a questa domanda, solo il **20%** dei SI delle aziende/enti rispondenti non ha in funzione alcun sistema di controllo e monitoraggio della sicurezza digitale.
Tutti gli altri SI hanno sistema di controllo e monitoraggio per la sicurezza digitale: le due tipologie più diffuse e che rientrano in questa percentuale sono con il **35,4%** sistemi centralizzati, integrati con quelli di controllo e monitoraggio dell'intero SI e gestiti on premise, soluzione tipica per sistemi informativi di grandi dimensioni, e con il **18,5%** il controllo non centralizzato ma di ogni singolo sistema ICT in locale, soluzione diffusa nei sistemi informativi di piccole e piccolissime dimensioni. Il **16,8%** ha terziarizzato la gestione operativa della sicurezza digitale, e sono quindi di Terze Parti i sistemi di controllo e monitoraggio, e da questi ultimi gestiti.

Un altro aspetto importante per la gestione della sicurezza digitale è il settaggio e la configurazione corretta delle funzionalità di sicurezza nei sistemi ICT, in particolare per tutte le opzioni inerenti la sicurezza, che troppo spesso non vengono correttamente settate.

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 2024. Nel **47,7%** dei SI delle aziende/enti rispondenti le configurazioni inerenti la sicurezza digitale sono sistematicamente aggiornate, manualmente o in maniera automatica, ma per il **23,1%**, non sono definite metodiche/procedure per correttamente configurare le opzioni di sicurezza all'installazione o successivamente. Per un altro **23,1%** il settaggio/configurazione è effettuato alla sola prima installazione.

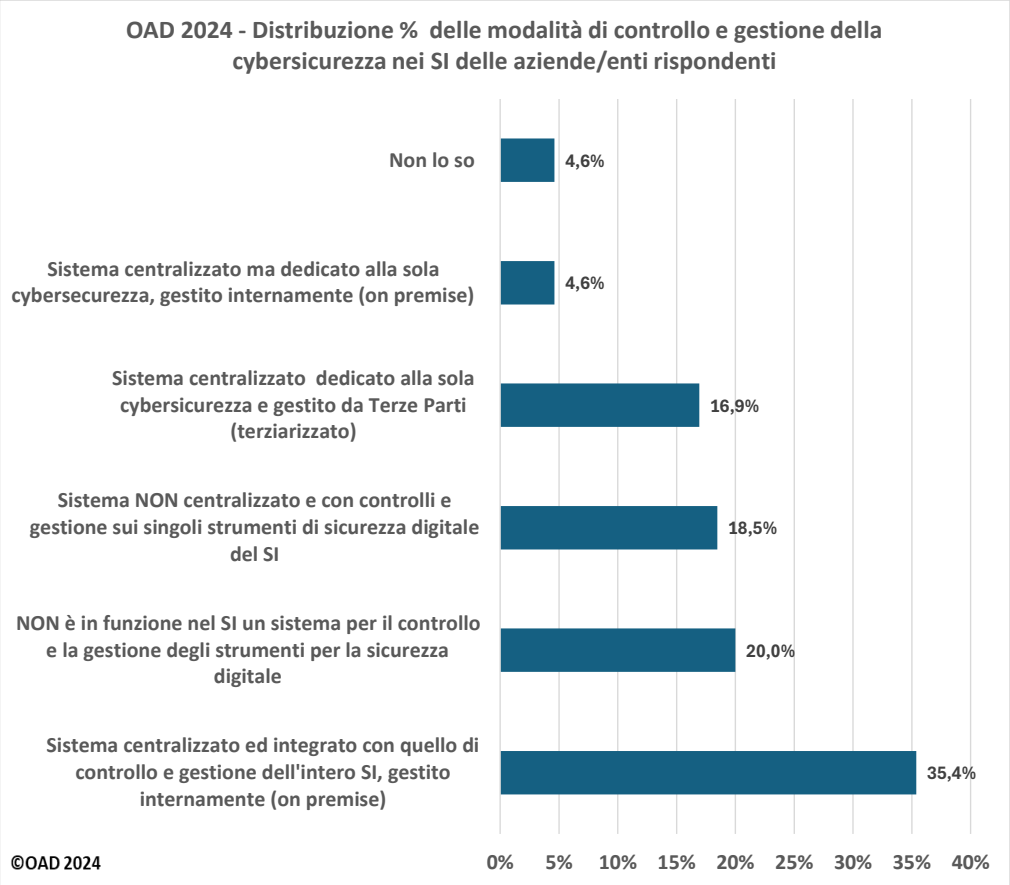


Fig. 7.2.7-6

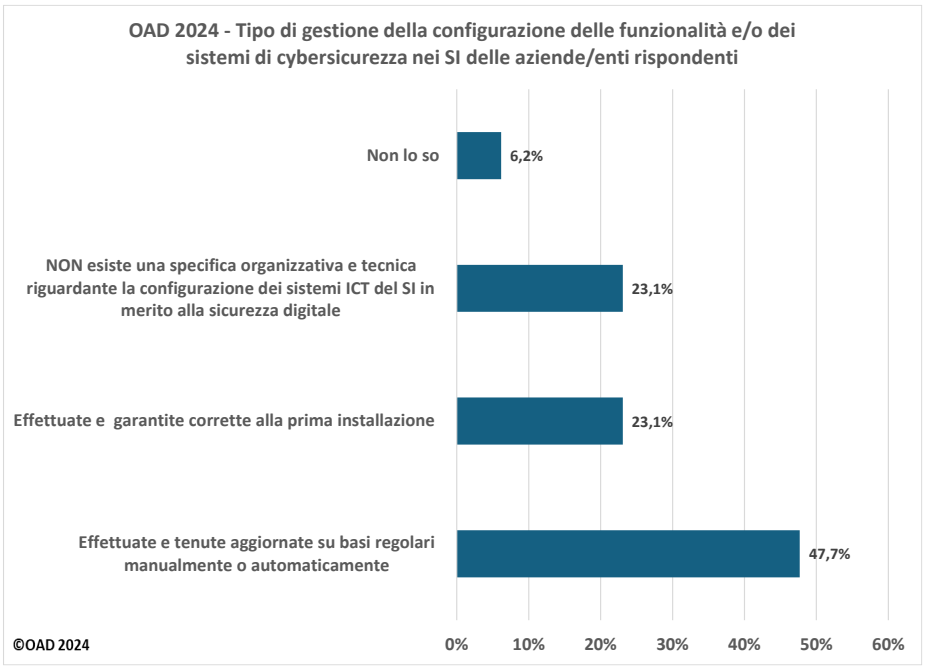


Fig. 7.2.7-7

Altro aspetto fondamentale nella gestione della sicurezza digitale di un SI è il **sistematico e tempestivo aggiornamento di ogni software in produzione**, da quello di base a quello applicativo. Come più volte evidenziato nei capitoli precedenti, la larga diffusione di ransomware in Italia è causata soprattutto dal non aggiornamento del software, e quindi dalla correzione/eliminazione di vulnerabilità che i ransomware (e più in generale i malware) sfruttano per attaccare il SI.

La fig. 7.2.7-8 mostra che il **64,6%** delle aziende/enti rispondenti **effettua sistematicamente e centralmente l'aggiornamento dei software** in produzione ad ogni aggiornamento segnalato dal fornitore. Il **18,5%** lo fa **solo per alcuni software** ed il **10,8%** lo fa effettuare dagli stessi utenti: questa è la situazione tipica delle piccole e piccolissime realtà.

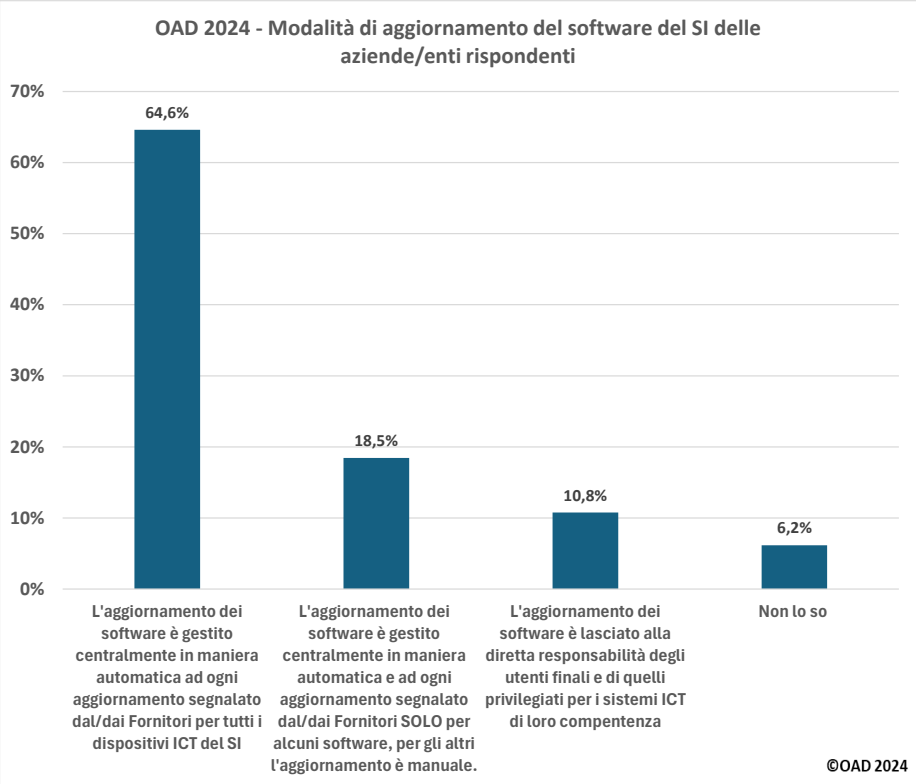


Fig. 7.2.7-8

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 nel questionario OAD una misura organizzativa, e l'indagine 2024 riporta i dati rilevati in §7.1.3.
L'analisi delle vulnerabilità ed i pentest sono invece considerate **misure tecniche**, ivi inclusa l'analisi delle vulnerabilità organizzative e degli utenti.

Come mostrato nella fig. 7.2.7-9, solo il **16,9%** delle aziende/enti rispondenti **non effettua** l'analisi delle vulnerabilità. E' un dato sostanzialmente positivo, relativo prevalentemente alle piccole e piccolissime organizzazioni rispondenti, controbilanciato da un ampio **49,2%**, poco meno della metà del totale, che effettua l'analisi delle vulnerabilità in maniera sistematica e periodica, e da un **29,2**% 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. Invece il **78,5%** delle aziende/enti rispondenti effettua l'analisi delle vulnerabilità (soprattutto di quelle tecniche), che è il primo basilare passo per una corretta implementazione delle misure di sicurezza idonee per il proprio specifico SI.

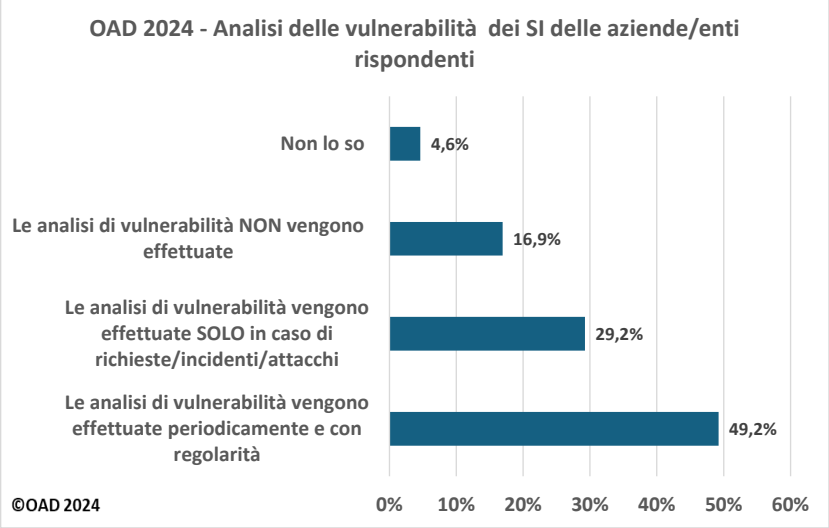


Fig. 7.2.7-9

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.

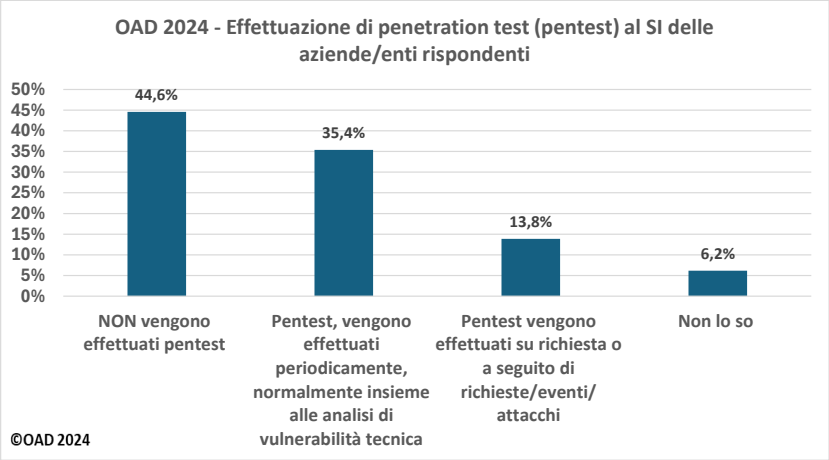


Fig. 7.2.7-10

La fig. 7.2.7-10 mostra che il **49,2%** delle aziende/enti rispondenti **effettua pentest**, e di questi il **35,4%** li effettua periodicamente e con regolarità, il resto li effettua solo quando richiesto, ad esempio per contribuire ad una certificazione aziendale, dopo l'installazione di un nuovo strumento di sicurezza digitale, etc. . Il **44,6% non li effettua**, ed anche questo dato è congruente con le numerose piccole realtà rispondenti, i cui piccoli SI

non richiedono, e soprattutto non effettuano, normalmente test di penetrazione per verificare la solidità delle misure di sicurezza in essere.

La raccolta e la gestione dei log è un'altra misura utile nella gestione operativa del sistema informativo e della sua sicurezza.
Il questionario OAD 2024 ha richiesto solo se viene effettuata la raccolta e la gestione dei log degli utenti, sia quelli privilegiati sia quelli finali.

La fig. 7.2.7-11 riassume le risposte raccolte: a parte un **16,2%** che non raccoglie ed analizza i log, **tutti gli altri lo fanno**, seppure con varie modalità. Il **32,4%** raccoglie e gestisce i log di tutti gli utenti, mentre il **17,6%** lo fa solo per gli utenti privilegiati, così come è obbligatorio per gli amministratori di sistema dal provvedimento del Garante italiano della privacy del 27/11/2008.
Interessante notare che nessuna delle aziende/enti rispondenti dichiara di archiviare solo i log degli utenti privilegiati, ma senza poi gestirli.

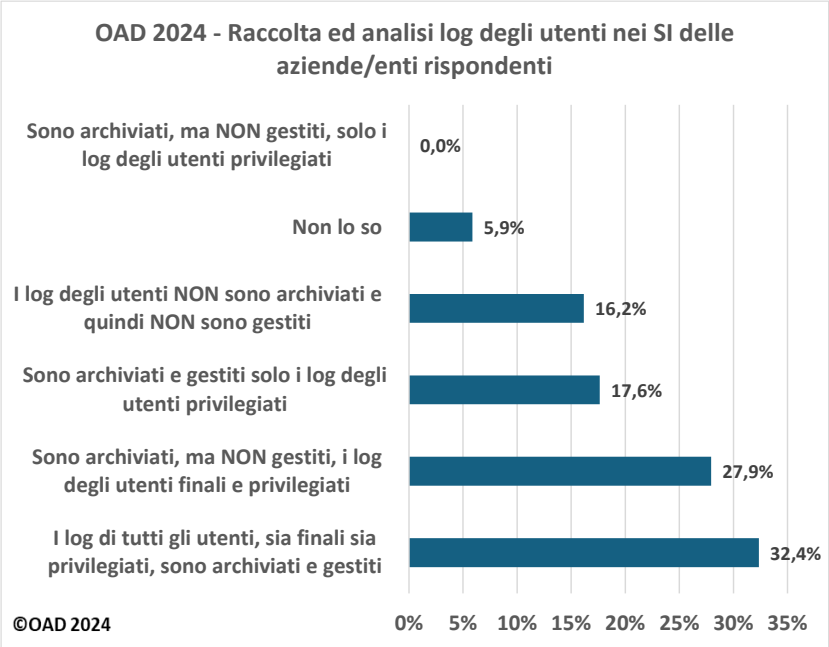


Fig. 7.2.7-11

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.

La figura 7.2.7-12 mostra che **un SOC è usato** dal **31,2%** delle aziende/enti rispondenti, e di queste il **20,3%** usa un **SOC fornito da Terze Parti**.
Un SOC è tipico di grande organizzazioni e di grandi fornitori di networking/cloud/hosting, ed il **10,9%** di un **SOC on premise** è ragionevole nel contesto di rispondenti emerso con l'indagine 2024.

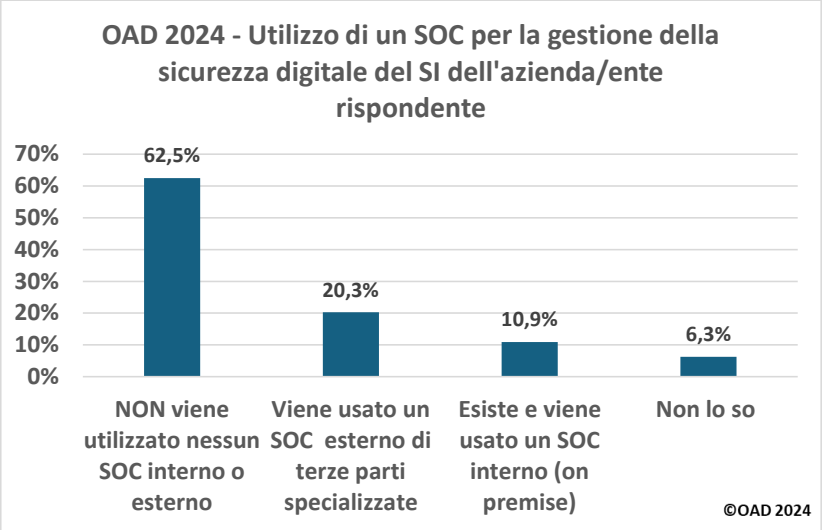


Fig. 7.2.7-12

Nell'ambito della gestione della sicurezza digitale un aspetto importante è la definizione di un **Piano di Disaster Recovery (DR) del SI**, che consenta all'azienda/ente, in caso di "disastro", di poter ripristinare in tempi brevi almeno le principali risorse ICT e poter garantire così la (minima) **continuità operativa** dei processi e delle attività che non possono e che non dovrebbero fermarsi nemmeno in caso di disastro.
Per questo motivo il Piano DR fa parte (o 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 alternative per attivare il DR in siti diversi da quello in cui si è avuto il "disastro" significa aver attivato, e quindi pagare, tali risorse ICT sostitutive rispetto a quelle "disastrate" del SI.
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 SI.
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. 7.2.7-13 evidenzia che il **75%** dei sistemi informativi delle aziende/enti rispondenti ha un Piano di DR, e di questi il **54,7%** l'ha attuato considerando solo le parti del SI fondamentali per garantire la continuità operativa minima per le sue attività/business.

La percentuale emersa è veramente alta, considerando la composizione delle aziende/enti emerse dal sondaggio. Questo da un lato dipende che i rispondenti appartengono, come più volte sottolineato, alla fascia medio-alta in termini di livello di sicurezza digitale, dall'altro che la diffusione di attacchi digitali sempre più "cattivi" ed impattanti l'attività ed il business sta portando imprese di ogni dimensione e settore merceologico a munirsi di adeguati strumenti non solo di prevenzione e difesa, ma anche di resilienza.

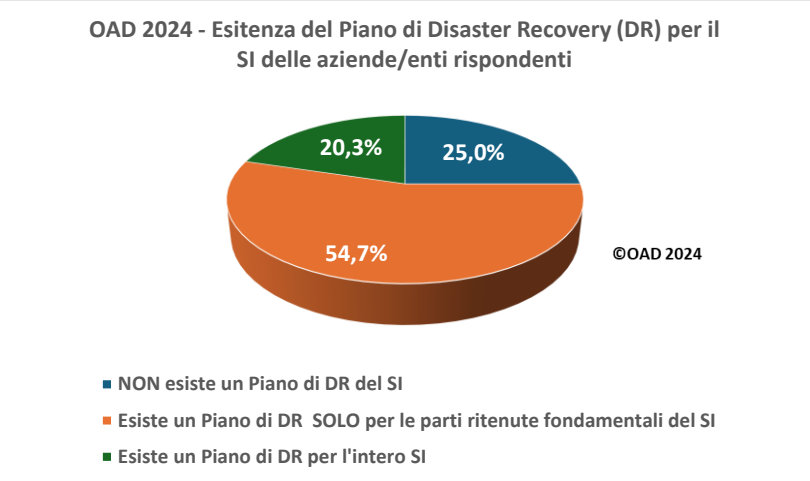


Fig. 7.2.7-13

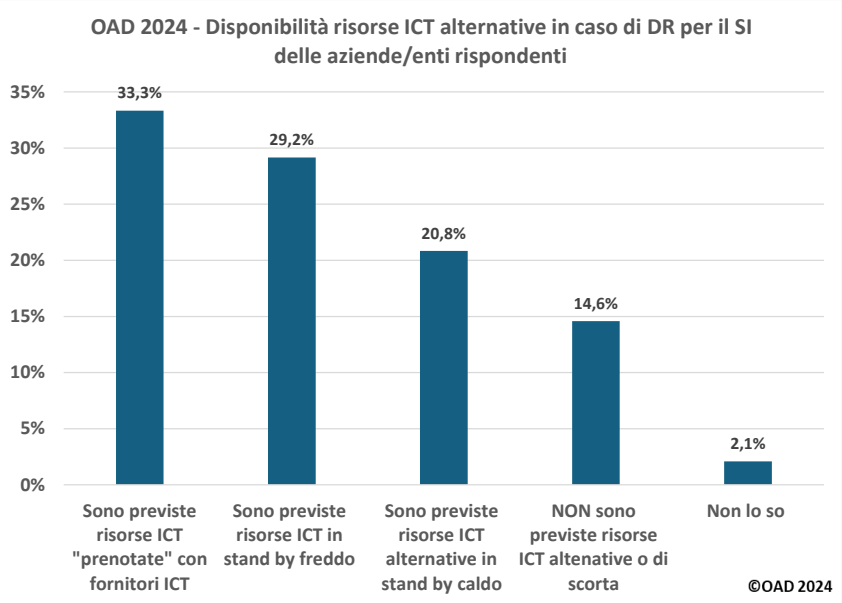


Fig. 7.2.7-14

Tale tendenza è confermata da quanto emerge dalla fig. 7.2.7-14, che mostra la disponibilità di risorse ICT ”alternative” da utilizzare in caso di DR del SI.

La fig. 7.2.7-14, mostra che **l’83,3%** delle aziende/enti rispondenti (limitate a quelle che avevano dichiarato di avere un Piano di DR come evidenziato nella 7.2.7-13) 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: prima il COVID poi le guerre in atto, con tutti gli attacchi digitali ad esse correlate, hanno sicuramente fatto comprendere anche alle piccole organizzazioni l’importanza della resilienza. Il **33,3%** delle organizzazioni rispondenti dichiara di aver prenotato risorse ICT alternative con i fornitori, tipicamente ora in ambito cloud. A scendere, ma con percentuali significative, il disporre di soluzioni in stand by freddo e caldo, ossia di avere

risorse ICT di scorta ma non attive, oppure disponibilità di risorse ICT in tempo reale e probabilmente in replica su risorse remote in una architettura ad alta affidabilità. Il **14,6%** delle aziende/enti rispondenti, pur avendo un piano di DR, non ha previsto alcuna risorsa ICT alternativa da utilizzare; hanno di fatto un DR solo sulla carta, di fatto difficilmente attuabile in breve tempo nel momento di un disastro.

La gestione efficace di una gravissima emergenza come il recovery di un sistema informativo richiede non solo la disponibilità di risorse alternative, come sopra discusso, ma anche una struttura e procedure organizzative che mettano in atto il piano di DR. OAD fa riferimento a tale struttura con il termine **ERT, Emergency Response Team**, e in §7.1.2 le figure 7.1.2-4 e 5 mostrano quale è la situazione in merito tra le aziende/enti rispondenti.

Aver definito un ERT e le relative procedure da seguire in caso di disastro non basta. Occorre che le persone dell'ERT, sulla base del Piano di DR, effettuino periodicamente delle **esercitazioni** (normalmente a tavolino, chiamate **DTE, Desk Top Exercise**), ad esempio su base semestrale, o annuale, così da verificare la corretta impostazione delle procedure organizzative e la preparazione del personale da coinvolgere in un DR.
In un DTE vengono simulati diversi possibili casi di disastri (considerando quanto analizzato nell'ultima analisi dei rischi ICT effettuata) e provate le procedure previste nel piano, attivando le persone da e le risorse ICT da coinvolgere.
Senza periodiche sperimentazioni e senza l'allocazione delle idonee risorse ICT alternative, un piano di DR ben difficilmente potrà essere attivato in caso di disastro nei tempi necessari ed a costi ragionevoli.

La fig. 7.2.7-15 mostra che solo il **23,1%** delle organizzazioni rispondenti che hanno un Piano di DR **non effettuano simulazioni e prove**. Tutte le altre le effettuano, ma in modalità e tempi diversi, come evidenziato nella figura. Hanno una percentuale uguale, il **30,8%,** l'effettuazione periodica di simulazioni **sull'intero SI** o **solo su alcune sue parti**, quelle più importanti e che supportano le attività primarie che non possono essere totalmente bloccate.

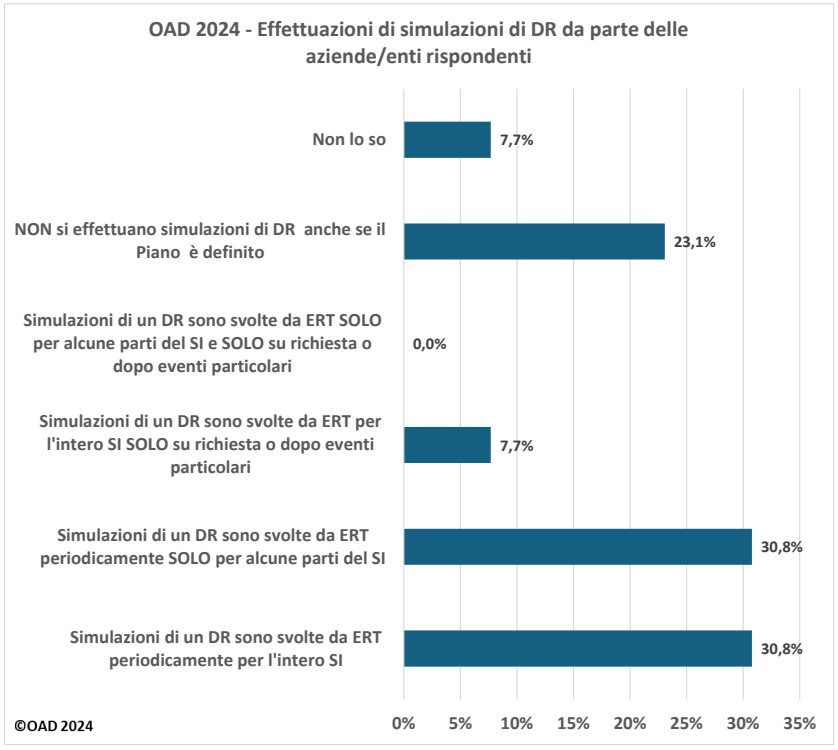


Fig. 7.2.7-15

7.3 Le misure di sicurezza per gli ambienti OT

Si è voluto dedicare questo paragrafo specifico sulle misure di cybersicurezza negli ambienti OT delle aziende/rispondenti, avendo effettuato un'analisi verticale sugli attacchi ai sistemi OT, riportata in §4.3.

Negli anni passati OAD aveva considerato gli attacchi a quelli che oggi si chiamano sistemi OT, prevalentemente quelli sui sistemi di automazione e di controllo dei processi industriali, e aveva posto specifiche domande anche sulle misure di sicurezza in atto per questi sistemi. Nelle ultime edizioni di OAD queste domande erano state eliminate per semplificare e rendere più veloce la compilazione del questionario online.
Si sono di nuove introdotte domande sulle misure di sicurezza per i sistemi OT in questa edizione 2024, ma lasciandole opzionali, e ovviamente "riservate" a chi aveva dichiarato di avere e gestire sistemi OT.

Le aziende/enti rispondenti che hanno e gestiscono sistemi OT sono il **37% del totale** (fig. 4.3-3) ed il **13%** tra quelle che hanno deciso di rispondere alle domande opzionali sulle misure di sicurezza.
Nonostante la percentuale di chi ha risposto sul totale di rispondenti sia relativamente bassa, le risposte emerse sono interessanti e riportate e commentate nel seguito di questo paragrafo.

Le domande nel questionario OAD 2024 per i sistemi OT seguono la medesima logica adottata per le domande sugli ambiti web , pur semplificandole e riducendo il loro numero.

La fig. 7.3-1 indica che la maggior parte dei sistemi OT, il **52,2%** operano sulle **stesse rete locali** ove operano gli altri sistemi ICT del SI, ed il **39,1%** utilizza invece **reti locali dedicate.** Questo ultimo approccio migliora intrinsecamente il livello di sicurezza dei sistemi OT, che a livello di networking sono isolati rispetto alle gli altri sistemi informatici, quali server, storage, PC, etc.

La fig. 7.3-2 mostra che la stragrande maggioranza dei sistemi OT delle aziende/enti rispondenti, il **78,3%** ha controlli e monitoraggi effettuabili sia in locale che da remoto, e il **13%** solo in locale; **nessun** sistema OT, tra quelli dei rispondenti, ha controlli solo da remoto.

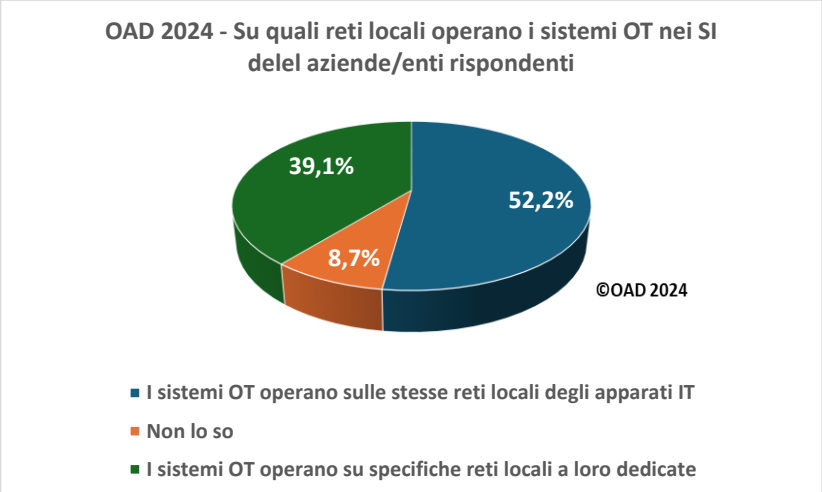


Fig. 7.3-1

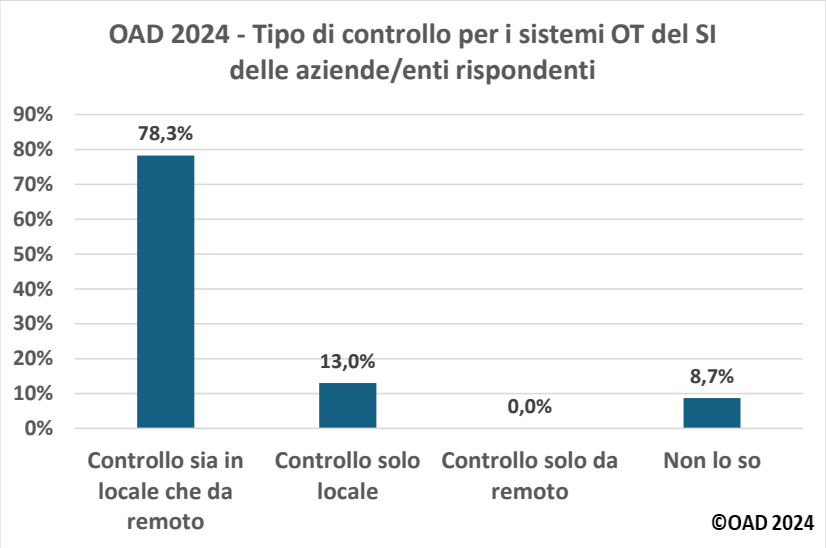


Fig. 7.3-2

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

La fig. 7.3-3 conferma tale tendenza anche nel campione di rispondenti emerso con OAD 2024: il **62,7%** dei sistemi OT delle aziende/enti rispondenti è collegato ed interoperante con il SI.

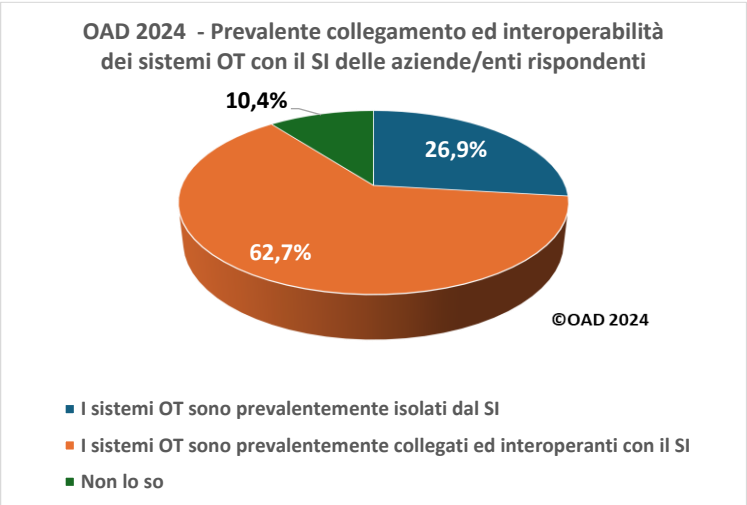


Fig. 7.3-3

Il livello di affidabilità e disponibilità di un sistema ICT, in caso di suo malfunzionamento, è dato anche dalla sua configurazione in replica in tempo "quasi" reale oppure dalla disponibilità di una sua copia "di scorta" che possa facilmente e tempestivamente sostituire il dispositivo malfunzionante.
Queste logiche di repliche on line e di pezzi di scorta dipendono fortemente dal tipo di sistema OT, in termini di dimensione, costo, complessità. Si possono avere repliche on line o pezzi di scorta per sistemi relativamente piccoli, non per grandi dispositivi come quelli medici per TAC.

La fig. 7.3-4 fornisce una indicazione di massima: il **52,2%** dei sistemi OT considerati **non è in replica e non ha scorte** di alcun tipo. Il **21,7% ha parti di scorta** ed il **17,4**% ha sistemi **in replica**: di questi la **metà in replica per tutti i sistemi OT**, **l'altra metà** è in replica **solo per quelli più critici**.

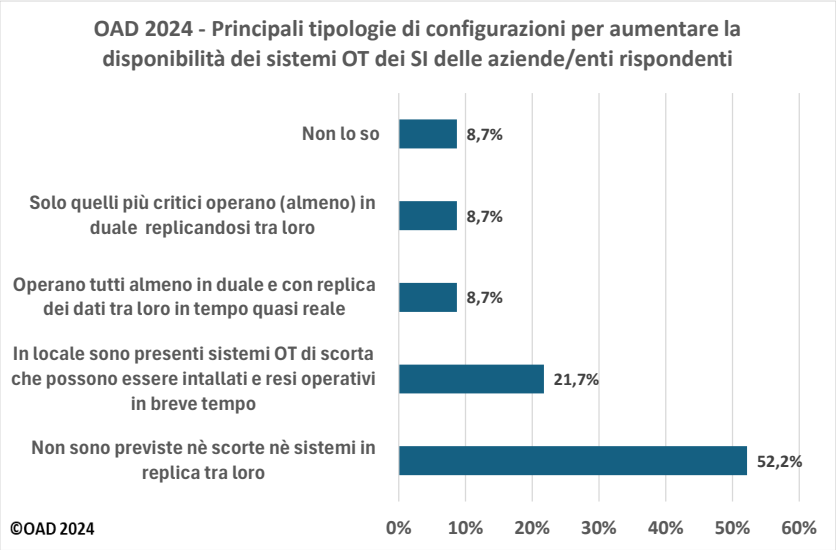


Fig. 7.3-4

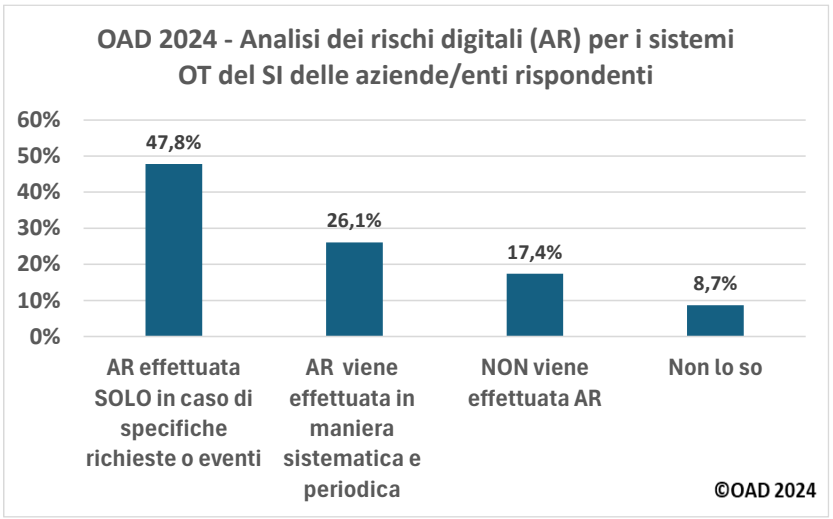


Fig. 7.3-5

Considerando l'ampio e assai diversificato insieme dei possibili sistemi OT nei più diversi ambiti di applicazione, e la loro frequente connessione ed interoperabilità con alcune applicazioni "centrali" del SI (si veda fig. 4.3-6), è importante effettuare una analisi dei rischi ICT (AR) sui sistemi OT e sui loro eventuali impatti anche sul SI.

La fig. 7.3-5 evidenzia che solo per il **26,1%** dei sistemi OT delle/dei rispondenti l'AR è effettuata sistematicamente e periodicamente, mentre per **quasi la metà** è effettuata solo a seguito di specifiche richieste. Risulta positivo il fatto che solo per il **17,4%** l'AR dei sistemi OT non è effettuata.

Come già evidenziato nei paragrafi precedenti, la rilevazione e la gestione degli incidenti ICT è basilare per poter garantire un idoneo livello di sicurezza digitale. Gli incidenti digitali, nel cui ambito sono inclusi gli attacchi, occorrono ovviamente anche in ambito OT, e come già evidenziato in §4.3, possono anche coinvolgere persone, non solo sistemi ICT, con possibili seri problemi nel connubio security-safety. La gestione di ogni incidente o attacco digitale richiede soprattutto chiare ed efficaci procedure organizzative, perché sia chiaro chi deve fare che cosa e come.

La fig. 7.3-6 mostra che per più della metà dei rispondenti, il **56,5%**, nel caso di incidenti in ambito OT **si usano le stesse procedure in uso per gli altri ambiti del SI**. Solo per **l'8,7%** sono definite e seguite **specifiche procedure**, e per il **26,1%** delle aziende/enti rispondenti **non esistono procedure** cui far riferimento per gestire gli incidenti digitali.
Questa %, a giudizio dell'autore, è molto alta, ed è, purtroppo, un indice di come siano sottostimati gli aspetti organizzativi della sicurezza digitale.

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

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

La fig. 7.3-7 mostra che il **56,5%** delle aziende/enti rispondenti **segue questi standard** soprattutto per i dispositivi OT più recenti e moderni, mentre un più esiguo **8,7%** ne fa riferimento per tutti i sistemi OT che utilizza e che dovrà acquisire.

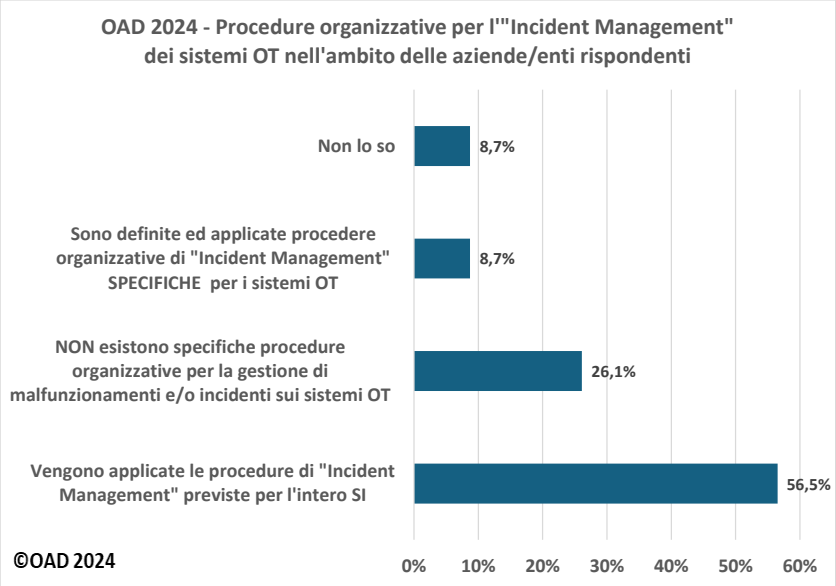


Fig. 7.3-6

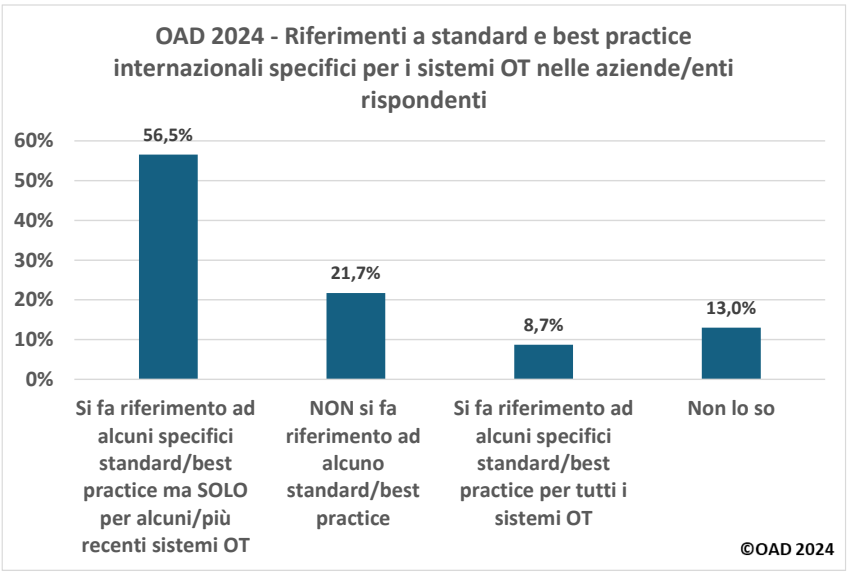


Fig. 7.3-7

Cap 8 Contributo della Polizia Postale e per la Sicurezza Cibernetica

Il Rapporto OAD 2024 riporta in questo capitolo l'intero contributo della Polizia Postale e per la Sicurezza Cibernetica, mantenendo quanto più possibile il formato grafico con cui è stato fornito.

L'autore ed AIPSI ringraziano vivamente gli autori di questo contributo, l'Ispettore **Gaetano Martucci** e dell'Assistente **Luigi Ummaro**, oltre al **Direttore** della Polizia Postale e per la Sicurezza Cibernetica **Ivano Gabrielli.**

La Polizia Postale e per la Sicurezza Cibernetica, per brevità indicata come Polizia Postale, da anni collabora con AIPSI per le indagini 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 e al cyber terrorismo.

Per quanto riguarda i dati sulla protezione delle infrastrutture critiche, la Polizia Postale ha una propria struttura, il **C.N.A.I.P.I.C., Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche**[71], incaricata in via esclusiva della prevenzione e della repressione dei crimini informatici che hanno come obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale.

Nella fig. 8-1 sono messe a confronto le informazioni ricevute da OAD negli anni dalla Polizia Postale per la protezione delle infrastrutture critiche, quindi dal C.N.A.I.P.I.C.
Gli attacchi rilevati, gli allarmi diramati, le indagini avviate e le persone denunciate/indagate (prime quattro righe della tabella in figura) sono diminuite nel 2023 rispetto a quelle del 2022, ma rimando dello stesso ordine di grandezza.
Soprattutto gli attacchi rilevati hanno avuto una diminuzione, **-8,25%** tra 2023 e 2022, ma sempre **con valori molto alti** rispetto agli anni dal 2021 in giù.

Tale tendenza conferma quanto rilevato dall'indagine online di OAD 2024, si veda in particolare fig. 4-2.
Ma sembra essere in contrasto con il dato dell'ACN, che nel citato Rapporto ACN 2023 al Parlamento evidenzia un aumento degli attacchi nel 2023 rispetto al 2022 del 140% (si veda §3.3 e fig. 3.3-3).
Questa differenza è dovuta al fatto che i bacini di riferimento sono diversi, anche se simili. I dati forniti da ACN fanno riferimento a quanto rilevato dalle segnalazioni alla sua struttura CSIRT Italia, mentre quelli della Polizia Postale fanno riferimento alle rilevazioni del C.N.A.I.P.I.C.
Come già indicato in precedenza, a giudizio dell'autore, questa differenza è dovuta ai bacini numericamente diversi di chi segnala gli attacchi digitali allo CSIRT di ACN rispetto al C.N.A.I.P.I.C. della Polizia Postale: il bacino di aziende/enti cui fa riferimento CSIRT è al momento più piccolo rispetto a quello del C.N.A.I.P.I.C.

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 2023 sono nell'ordine delle centinaia di migliaia, aumentati rispetto al 2022; e per il 1° semestre 2024 il numero è già molto alto, e potrebbe per la fine del 2024 ulteriormente superare quello del 2023.

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

Protezione strutture critiche/essenziali	1 gen - 30 giugno 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Attacchi rilevati (*)	5.903 **	12.101 **	13.099	282	509	1181	459	1.032	844
Alert diramati	31.033	77.012	113.420	24.824	83.416	82.484	80.777	31.524	6.721
Indagini avviate (***)	36	96	110	34	103	155	74	72	70
Persone denunciate/indagate (*)	101 **	224 **	334	n.d.	105	117	14	1.316	1.226
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	23	79	77	17	69	79	108	83	85
Indagini avviate su attacchi rilevati	0,61%	0,79%	0,84%	12,06%	20,24%	13,12%	16,12%	6,98%	8,29%
Persone indagate su attacchi rilevati	1,71%	1,85%	2,55%	n.d.	20,63%	9,91%	3,05%	127,52%	145,26%

* Per il 2023-24: Target: Infrastrutture Critiche (I.C.), Operatori Servizi Essenziali (OSE), Pubbliche Amministrazioni Locali (PAL), Aziende, Privati
** Per il 2023-24: Dati aggregati C.N.A.I.P.I.C. e Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.).
*** Per il 2023-24 dal C.N.A.I.P.I.C.

Fig. 8-1 (Fonte: elaborazione OAD su dati storici della Polizia Postale)

Cyber Terrorismo	1 gen - 30 giugno 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018
Spazi web monitorati	138.267	182.209	175.572	11.962	37.081	36.377	36.000

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

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.

OAD
Osservatorio
Attacchi Digitali
in Italia

Ministero dell'Interno

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

POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

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

ANNO
2023
e
Primo Semestre 2024

(fonte dati: mattinale Polizia Postale e delle Comunicazioni)

Dati aggiornati al 30 giugno 2024

Roma, 12 luglio 2024

Rilevazione statistica a cura di:
Ispettore della Polizia di Stato Gaetano Martucci
Assistente della Polizia di Stato Luigi Ummaro

PREMESSA

Viviamo in un'epoca in cui la lotta per il dominio cibernetico è sempre più serrata e globale. Di conseguenza, la sicurezza e la protezione delle società moderne dipendono in gran parte dalla prevenzione e dal contrasto della criminalità informatica. In Italia, la Polizia Postale e per la Sicurezza Cibernetica svolge un ruolo fondamentale nella sicurezza cibernetica, sia attraverso l'opera del Servizio centrale che delle sue articolazioni territoriali, che comprendono 18 Centri Operativi per la Sicurezza Cibernetica nei principali capoluoghi di regione e 82 Sezioni Operative per la Sicurezza Cibernetica nelle più importanti province italiane.

La prevenzione e il contrasto dei crimini informatici sono diventati ancora più vitali alla luce degli attuali conflitti russo-ucraini e in Medio Oriente, che hanno innescato una vera e propria guerra senza confini sul fronte cibernetico. Inoltre, l'Italia ha recentemente approvato il DDL Cybersicurezza, una legge che mira a rafforzare la cybersicurezza nazionale e a prevenire e reprimere i reati informatici. Questo rappresenta un ulteriore passo significativo nel fornire alle autorità competenti strumenti normativi all'avanguardia per la protezione delle infrastrutture critiche e delle informazioni sensibili del Paese.

La Polizia Postale, organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazioni, svolge un ruolo essenziale nella prevenzione e nel contrasto degli attacchi cibernetici che minacciano le infrastrutture critiche nazionali. Questi attacchi, spesso orchestrati da gruppi criminali transnazionali o da attori statali ostili, mirano a destabilizzare servizi essenziali come la sanità pubblica, l'energia, le telecomunicazioni e i trasporti. Tali minacce non solo compromettono la continuità operativa di questi servizi, ma mettono anche a rischio la sicurezza e il benessere della popolazione. Attraverso un costante monitoraggio e interventi tempestivi, il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), incardinato all'interno del Servizio Polizia Postale, lavora per proteggere il Paese da queste insidie, contribuendo, in sinergia con altre entità come il Comando per le Operazioni in Rete, il Sistema di Informazione per la Sicurezza della Repubblica e l'Agenzia per la Cybersicurezza Nazionale, alla resilienza delle infrastrutture e a garantire l'ordine e la sicurezza pubblica a favore di tutti i cittadini.
Con l'aumento delle transazioni online, i crimini economici e finanziari sono diventati una delle principali sfide del nostro tempo. Frodi informatiche, furto di dati personali sensibili di natura finanziaria attraverso tecniche di ingegneria sociale sempre più ingegnose e sofisticate, e truffe perpetrate con l'ausilio degli strumenti informatici, oggi rese più efficaci anche grazie a un uso distorto dell'intelligenza artificiale, rappresentano solo alcune delle minacce che i cittadini affrontano quotidianamente.
La Polizia di Stato lavora instancabilmente per identificare e neutralizzare queste minacce, proteggendo i risparmi e le finanze delle persone. Attraverso un costante monitoraggio delle attività sospette e l'adozione di tecnologie avanzate, è in grado di intervenire tempestivamente, garantendo un ambiente digitale più sicuro per tutti.
Fondamentale è il ruolo del Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO) nella lotta contro lo sfruttamento sessuale dei minori su internet. In questi ultimi anni, il CNCPO ha intensificato ulteriormente i suoi sforzi per affrontare le sfide crescenti legate allo sfruttamento sessuale dei minori online, implementando nuove strategie e collaborazioni internazionali, con un focus particolare sulla condivisione di informazioni e risorse con altre agenzie di contrasto alla criminalità informatica. Questo ha permesso di migliorare l'efficacia delle operazioni e di ampliare la portata delle indagini.
Nonostante i successi ottenuti, il CNCPO continua a fronteggiare numerose e sempre nuove sfide. La rapida evoluzione tecnologica e l'uso crescente di piattaforme di comunicazione criptate rendono sempre più difficile

individuare e perseguire i responsabili di crimini pedopornografici. Tuttavia, il Centro rimane impegnato a sviluppare nuove tecnologie e metodologie investigative per affrontare queste minacce.
Importante è l'impegno profuso nelle attività di sensibilizzazione e prevenzione, basata prevalentemente sulla collaborazione con le scuole, genitori e comunità per educare i giovani sui pericoli della rete e promuovere comportamenti sicuri online. Promuove campagne di sensibilizzazione, come "Una vita da social," per educare i cittadini sui rischi e le migliori pratiche per proteggersi online.
La Polizia di Stato e il Ministero dell'Istruzione realizzano questa iniziativa nell'ambito del progetto "Generazioni Connesse." Durante il tour, che conta oltre 70 tappe sul territorio nazionale, si affrontano temi legati ai social network e al cyberbullismo. Medesimi contenuti volti alla sensibilizzazione e all'informazione vengono veicolati dalla specialità della Polizia di Stato attraverso il sito www.commissariatodips.it.

L'attività di prevenzione e repressione dei reati contro la persona perpetrati attraverso o con l'ausilio delle tecnologie della comunicazione e dell'informazione ha confermato che la donna rimane il soggetto più odiato e colpito nel web: in aumento il *cyber stalking*, le molestie e la diffusione di immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate (*Revenge Porn*).

Nell'ambito della prevenzione e del contrasto alla diffusione di contenuti terroristici online e, in particolare, dei fenomeni di radicalizzazione sul web, la Polizia Postale effettua costantemente il monitoraggio del web e svolge attività investigative, sia d'iniziativa che su specifica segnalazione (anche grazie a quelle che giungono dai cittadini tramite il portale del Commissariato di P.S. Online), al fine di individuare i contenuti illeciti presenti all'interno degli spazi e dei servizi di comunicazione online di ogni genere.
Il target operativo di tale settore, dunque, si concretizza nella prevenzione e repressione dei reati che utilizzano la dimensione virtuale per fini terroristici, minando l'ordine e la sicurezza pubblica per ragioni riconducibili sia a forme di fondamentalismo religioso, sia a forme di estremismo politico ideologico, anche in contesti internazionali.

Ogni giorno, le donne e gli uomini della Polizia Postale affrontano sfide complesse e in continua evoluzione. La rapidità con cui le tecnologie si sviluppano richiede un costante aggiornamento delle competenze e delle strategie di intervento. La formazione continua è essenziale per mantenere un alto livello di efficacia nella prevenzione e nel contrasto dei crimini informatici. La formazione del personale è quindi una priorità imprescindibile. Oltre ai corsi di specialità, i ruoli operativi della Polizia Postale partecipano a tre corsi di alto livello di recente istituzione: uno per l'OSINT (Open Source Intelligence) e Soc.M.Int. (Social Media Intelligence), uno per il contrasto all'abuso sessuale minorile online, e uno per operatore cyber per la protezione delle infrastrutture critiche. Questi corsi garantiscono che il personale sia sempre pronto e reattivo per affrontare le sfide più complesse e sofisticate.

Accanto alla formazione del personale si pone un'efficace attività di ricerca e innovazione tecnologica che sono pilastri fondamentali per le forze dell'ordine. L'intelligenza artificiale ad esempio, utilizzata anche dalla criminalità comune ed organizzata per perseguire i loro scopi delittuosi, sta emergendo sempre più come uno strumento indispensabile per le forze di polizia per analizzare grandi quantità di dati, identificare sospetti e prevedere potenziali minacce. I governi di tutto il mondo stanno investendo nella ricerca e sviluppo di queste tecnologie per migliorare le capacità operative e garantire una risposta tempestiva ed efficace alle minacce cibernetiche.

Il Servizio Polizia Postale e per la Sicurezza cibernetica è incardinato nella nuova Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica istituita con il Decreto del 7 febbraio 2024 del Ministro dell'Interno, di concerto con il Ministro dell'Economia e delle Finanze, che rappresenta un'importante evoluzione nel campo della sicurezza nazionale, progettata per coordinare e ottimizzare le operazioni di sicurezza anche cibernetica a livello nazionale, fornendo supporto tecnico e operativo alle unità territoriali.
Gli altri servizi che insieme al Servizio Polizia Postale formano la nuova direzione, sono:

- Il Servizio Affari Generali: Si occupa della gestione amministrativa e contabile, della pianificazione strategica e della gestione delle risorse umane e logistiche. Coordina le attività dei vari servizi della Direzione Centrale, garantendo un'azione unitaria e coerente.
- Il Servizio Polizia Scientifica: Responsabile delle attività di polizia scientifica, questo servizio si occupa della raccolta, analisi e conservazione delle prove scientifiche. Supporta le indagini con tecniche avanzate di analisi forense.
- Il Servizio per la Sicurezza Cibernetica del Ministero dell'Interno: Assicura la protezione delle reti e dei sistemi informatici del Ministero dell'Interno, garantendo la sicurezza delle comunicazioni e delle operazioni interne.

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

	1 gen – 31 dic 2023
Attacchi rilevati totali (*)	12.101 **
Alert diramati	77.012
Indagini avviate dal C.N.A.I.P.I.C.	96
Persone indagate (*)	224 **
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	79
Attacchi solo I.C. – OSE – PAL	***1.117***
Persone indagate solo I.C. – OSE – PAL	***112***

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

	Primo semestre 2024
Attacchi rilevati totali (*)	5.903 **
Alert diramati	31.033
Indagini avviate dal C.N.A.I.P.I.C.	36
Persone indagate (*)	101 **
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	23
Attacchi solo I.C. – OSE – PAL	***672***
Persone indagate solo I.C. – OSE – PAL	***37***

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

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

	1 gen – 31 dic 2023
Casi trattati pedopornografia e adescamento online	2.702
Persone indagate	1.239
Perquisizioni	927
Monitoraggi rete	28.355
Siti presenti in black list al 31/12/2023	2.739

	Primo Semestre 2024
Casi trattati pedopornografia e adescamento online	1.418
Persone indagate	619
Perquisizioni	532
Monitoraggi rete	15.170
Siti presenti in black list al 30/06/2024	2.759

IL COMMISSARIATO DI P.S. ONLINE

	1 gen – 31 dic 2023
Segnalazioni	84.293
Informazioni	21.075
Visite	2.646.422
Accessi	44.346.910
Alert Diramati	53
Interventi finalizzati alla prevenzione di intenti suicidari	204

	Primo Semestre 2024
Segnalazioni	44.513
Informazioni	11.843
Visite	1.359.185
Accessi	26.392.596
Alert Diramati	17
Interventi finalizzati alla prevenzione di intenti suicidari	139

PREVENZIONE CYBERTERRORISMO

• *Eversione Internazionale Estremismo religioso e politico* • *Eversione nazionale estrema destra, area antagonista, attività in circostanze di emergenza*	**1 gen – 31 dic 2023**
Spazi web monitorati	182.209
Spazi Virtuali con contenuti illeciti rilevati	2.037
Spazi oscurati per attiv. infoinvestigative	2.700

• *Eversione Internazionale Estremismo religioso e politico* • *Eversione nazionale estrema destra, area antagonista, attività in circostanze di emergenza*	**Primo Semestre 2024**
Spazi web monitorati	138.267
Spazi Virtuali con contenuti illeciti rilevati	947
Spazi oscurati per attiv. infoinvestigative	487

LE FRODI INFORMATICHE

	1 gen – 31 dic 2023
Casi trattati	10.755
Persone indagate	927
Somme sottratte	40.503.616

	Primo Semestre 2024
Casi trattati	4.557
Persone indagate	532
Somme sottratte	22.382.693

LE TRUFFE ONLINE

	1 gen – 31 dic 2023
Casi trattati	16.637
Persone indagate	3.610
Somme sottratte	139.536.457

	Primo Semestre 2024
Casi trattati	9.690
Persone indagate	1.761
Somme sottratte	98.555.935

REATI CONTRO LA PERSONA

	1 gen – 31 dic 2023
Casi trattati	9.538
Persone indagate	1.249

	Primo Semestre 2024
Casi trattati	4.884
Persone indagate	725

ALLEGATI

Allegato A Aspetti metodologici dell'indagine OAD 2024

L'indagine OAD 2024, come le precedenti, è indirizzata da un lato all'analisi totalmente anonima degli **attacchi digitali intenzionali** ai sistemi informativi (SI) delle aziende/enti rispondenti operanti in Italia (non agli incidenti ai SI causati da malfunzionamenti hardware e software, da errato/maldestro uso dei sistemi ICT da parte degli utenti e degli operatori, o da fenomeni accidentali esterni); dall'altro la rilevazione ed analisi, sempre in maniera anonima, delle principali caratteristiche dei SI dei rispondenti, e delle loro misure di sicurezza, sia tecnche che organizzative.
Sono considerati gli attacchi che sono stati effettivamente rilevati, e non è necessario che essi abbiano creato danni ed impatti negativi al SI attaccato, ovvero che l'attacco non abbia avuto il successo sperato dall'attaccante.
L'attacco contro un SI va a buon fine quando si intende violato, con una attività non autorizzata, almeno uno dei requisiti della sicurezza ICT, intesa come la "protezione dei requisiti di integrità, disponibilità e confidenzialità" delle informazioni trattate, ossia acquisite, comunicate, archiviate e processate.

OAD costituisce l'unica indagine indipendente online in Italia sugli attacchi digitali intenzionali ai sistemi informativi delle aziende e degli enti pubblici operanti in Italia. OAD non predefinisce uno specifico bacino di rispondenti, il medesimo negli anni, ma consente a chiunque, interessato e coinvolto nella gestione di un SI di una azienda/ente, un pieno e libero accesso al questionario online, in maniera totalmente anonima.
Grazie al numero di risposte raccolte e alla loro distribuzione tra aziende ed enti pubblici di varie dimensioni e appartenenti a diversi settori merceologici, l'indagine OAD cerca e puntualmente riesce a fotografare il fenomeno degli attacchi digitali intenzionali in Italia, riuscendo a coinvolgere nell'indagine anche le piccole e piccolissime realtà, che costituiscono in Italia la stragrande maggioranza (si veda §3.7.1 e §6.1) e che altre indagini nazionali ed internazionali ben difficilmente considerano.

Il questionario è rigorosamente **anonimo**: non viene richiesta alcuna informazione personale e/o identificativa del compilatore e della sua azienda/ente, non viene rilevato e tanto meno registrato il suo indirizzo IP, sulla banca dati delle risposte non viene specificata la data di compilazione.
Tutti i dati forniti vengono usati solo a fini di analisi complessiva e per la produzione di grafici e tabelle di sintesi.
Il livello di dettaglio sulle caratteristiche tecniche dei sistemi ICT non consente in alcun modo di poter risalire alla azienda/ente rispondente.
Per garantire un ulteriore livello di protezione ed evitare l'inoltro di più questionari compilati dalla stessa persona, il questionario, una volta completato e salvato, non può più essere modificato, e dallo stesso posto di lavoro non è più possibile compilare una seconda volta il questionario.
L'autore, AIPSI e Malabo garantiscono comunque la totale riservatezza sulle risposte raccolte.

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

Quando termina il periodo previsto per la compilazione del questionario, Malabo elabora ed analizza i dati raccolti tramite fogli elettronici, e sulla base di tali elaborazioni viene redatto il rapporto finale, che viene pubblicato sul sito di OAD e su quello AIPSI per poter essere scaricato gratuitamente da tutti gli interessati.
Come già indicato, il bacino dei rispondenti all'indagine non è predefinito e bilanciato statisticamente. L'indagine OAD non ha pertanto valore strettamente statistico, ma dato il numero e l'eterogeneità delle aziende/enti dei rispondenti, sia per settore merceologico sia per dimensione, è comunque significativa e sufficiente per fornire attendibili indicazioni sul fenomeno degli attacchi digitali in Italia e sulle loro tendenze.

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

Il calcolo statistico per la creazione dei grafici differisce a seconda che le risposte siano multiple (l'utente può selezionare più risposte per la stessa domanda) oppure no, e se la domanda, con relative risposte, è un dettaglio rispetto ad una precedente risposta.
Per le risposte multiple ad una data domanda, il denominatore nel calcolo della percentuale è dato dal numero di rispondenti complessivo per quella domanda o insieme di domande, non per la sommatoria delle risposte avute: la somma finale delle percentuali di ogni singola risposta può essere pertanto superiore o inferiore al 100%.
Per le risposte singole ad una data domanda, il denominatore nel calcolo della percentuale è dato dalla somma dei rispondenti: la somma finale delle percentuali di ogni singola risposta è e deve essere 100%.
In molti casi delle domande fanno riferimento ad una specifica risposta di una domanda precedente: per queste il valore al denominatore per il calcolo della percentuale è dato dal numero dei rispondenti che hanno selezionato la specifica risposta cui fa poi riferimento la successiva sotto domanda.
La correlazione tra i dati forniti da domande diverse dal questionario è effettuata tramite pivot del foglio elettronico contenente tutte i record delle risposte, e da questi fogli pivot vengono rielaborati i dati estratti e creati i relativi grafici.

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

A.1 L'indagine OAD 2024

L'indagine effettuata tramite un questionario on line via web ha posto due sole domande sugli attacchi digitali subiti nel 2023 dai Sistemi Informativi (SI) delle aziende/enti rispondenti, in modo da poter continuare l'analisi dei trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 ad oggi, ed ha approfondito gli attacchi digitali rilevati nel 2023 **alle applicazioni ed agli ambienti web** ed ai **sistemi OT, Operation Technology**.

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

Il **questionario online OAD 2024**, con risposte predefinite da selezionare, è strutturato con **109 domande raccolte in 8 sezioni**, molte delle quali opzionali e "saltabili" nel corso della compilazione. In alcune sezioni sono presenti delle sottosezioni per meglio articolare e contestualizzare le varie domande. Inoltre in alcune sezioni ci sono delle "domande" non visibili che effettuano calcoli sulle risposte selezionate per la valutazione del livello di sicurezza del SI oggetto delle risposte.
Le sezioni considerate nel questionario 2024:

- S1 - Brevi informazioni sulla Azienda/Ente della/del rispondente (7 domande)
- S2 - Attacchi digitali di ogni tipo al Sistema Informativo rilevati nell'intero 2023 (3 domande)
- S3 - Approfondimento attacchi ai siti e alle applicazioni web del Sistema Informativo (12 domande)
- S3B - Approfondimento sugli attacchi a sistemi ed apparati OT del Sistema Informativo (9 domande)
- S4 - Attacchi più temuti nel prossimo futuro (3 domande)
- S5 - Macro caratteristiche del Sistema Informativo cui la/il rispondente fa riferimento, sia per aziende Provider hosting/cloud che per le altre aziende/enti (11 domande)
- S6 - Misure tecniche in atto per la sicurezza digitale dell'intero Sistema Informativo (6 domande)
    - S6.1 - Misure fisiche di sicurezza digitale (5 domande)
    - S6.2 - Misure di Identificazione, Autenticazione e Autorizzazione (4 domande)

  - S6.3 - Misure per la sicurezza delle reti, locali e geografiche, incluse le connessioni ad Internet (4 domande)
  - S6.4 - Misure di sicurezza delle applicazioni del Sistema Informativo (4 domande)
  - S6.5 - Misure tecniche di sicurezza digitale per la protezione dei dati (6 domande)
  - S6.6 - Strumenti tecnici per il controllo e la gestione della sicurezza digitale del SI (10 domande)
  - S6.7 - La sicurezza nei sistemi OT in uso (10 domande)
- S7 - Misure organizzative di sicurezza digitale nell'Azienda/Ente della/del rispondente (18 domande)
- S8 - Ruolo della/del rispondente (1 domanda)
- S10 – Calcoli e presentazione della macro valutazione del livello di sicurezza del SI.

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

Gli approfondimenti sugli attacchi erano richiesti per due **indagini verticali**, la prima sugli ambienti, sulle applicazioni e sui siti web, la seconda sugli ambienti OT.
Per l'indagine verticale sul web, si è fatto anche riferimento alle 10 top vulnerabilità in ambito web e ai 10 top rischi delle API web individuate da OWASP e approfondite in §4.2.
Per entrambe le indagini verticali sugli attacchi digitali agli ambienti web e a quelli OT sono state poste le domande che nelle precedenti versioni del questionario OAD erano riportate per qualsiasi 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 2024

L'edizione 2024 ha aggiunto alle 13 tipologie di attacco delle precedenti edizioni una nuova tipologia che fa riferimento agli attacchi alla supply chain, ed ha anche aggiunto o migliorato alcune definizioni e risposte preimpostate.
Le 14 tipologie di attacco considerate sono le seguenti, e fanno riferimento, a grandi linee, a che cosa si attacca:

1. Distruzione e/o compromissione FISICA di dispositivi ICT FISSI o di loro parti
2. FURTO dispositivi FISSI ICT o di loro parti
3. FURTO di dispositivi ICT mobili di proprietà dell'azienda/ente e in uso presso i suoi dipendenti/collaboratori

4. FURTO INFORMAZIONI da singoli specifici sistemi FISSI ICT (PC, server, storage system, etc.) del Sistema Informativo, anche 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 cloud
10. MODIFICHE malevoli e/o non autorizzate alle INFORMAZIONI trattate dalle applicazioni del Sistema Informativo, anche quelle terziarizzate/in cloud
11. SATURAZIONE (DoS, DDoS) risorse digitali del Sistema Informativo, anche quelle terziarizzate/in cloud
12. Attacchi ai propri sistemi/servizi digitali in CLOUD o comunque TERZIARIZZATI presso Fornitori terzi
13. Attacchi a dispositivi dei sistemi OT, Operational Technology, ivi inclusi i sistemi IoT, i sistemi per l'automazione industriale ((SCADA, DCS, PLC, ..) e la robotica
14. Attacchi alla "supply chain" causati da vulnerabilità di fornitori e/o clienti interconnessi
15. Nel corso dell'intero 2023 il Sistema Informativo ha subito attacchi digitali la cui tipologia non è stata individuata.

Il quindicesimo punto consente una risposta a chi ha rilevato attacchi al proprio SI ma non è in grado di associarli ad una o più delle tipologie indicate.

La classificazione degli attacchi in OAD distingue il **che cosa** si attacca dal **come**. Spesso infatti, anche nei più autorevoli rapporti internazionali, la distinzione tra che cosa viene attaccato e quali tecniche si usano per effettuare tale attacco non sempre è chiara, anche perché talvolta il nome usato per individuare l'attacco rappresenta anche la tecnica di attacco. Si è cercato di distinguere il più chiaramente possibile il target dell'attacco, ossia che cosa si attacca, dalle tecniche usate (sovente una loro combinazione), queste ultime raggruppate in 7 voci, descritte nel prossimo paragrafo §A.2.1.

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

Facendo riferimento principalmente alle tassonomie sviluppate da CERT[72] e da Sandia[73], 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.

In ambito AIPSI si è discusso a lungo se aggiungere l'**Intelligenza Artificiale** (IA, o anche AI con l'acronimo inglese) tra le tecniche di attacco. Si è deciso per il no, dato che l'IA è un grande insieme di tecniche, alcune delle quali sono o potranno essere utilizzate per automatizzare e potenziare molte

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

delle “famiglie” di tecniche di attacco considerate, ma a sé stante: l’IA non è, almeno per ora, una famiglia di attacchi autonoma e diversa dalle sette fino ad ora considerate.

AIPSI e l’autore si riservano di ripensare per la prossima edizione di OAD questa decisone, tenendo conto delle evoluzioni e delle applicazioni che l’IA potrà nel contempo sviluppare nell’ambito degli attacchi alla sicurezza digitale.

A.2.1.1 Attacco

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. ***fisico***

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

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

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

A.2.1.2 Raccolta/diffusione malevola e non autorizzata di informazioni

Per attaccare un sistema ICT sono utili, in taluni casi indispensabili, informazioni sia dirette sulla sua posizione, sul suo funzionamento, sulla sua configurazione, sulle misure di sicurezza di cui dispone, sugli account degli utenti, sia indirette, come i nomi dei suoi utenti e dei suoi gestori, indirizzi fisici e digitali, numeri di telefono, contatti anche via rete con dipendenti potenzialmente infedeli o ingenui etc. Innumerevoli le tecniche per carpire, direttamente o indirettamente, le informazioni che servono per attuare un attacco digitale. Alcune sono “fisiche”, come la personale interazione con le persone che usano o gestiscono un dispositivo o le applicazioni del SI, come l’acquisizione di informazioni da carte e stampe nei cestini dei rifiuti, come la richiesta di informazioni in maniera subdola sia de visu sia per telefono (anche questo è social engineering). Altre tecniche per raccogliere informazioni sono informatiche ed includono, ad esempio, phishing, pharming, hoax, scam, data entry in server trappola, scannerizzazioni e ricerche in Internet, etc.
Si sta inoltre assistendo in maniera crescente alla diffusione, soprattutto via Internet, di informazioni false (le così dette fake news) e/o malevoli atte a far compiere all’inconsapevole destinatario operazioni di ausilio all’attuazione dell’attacco. I canali

A.2.1.3 Script e programmi maligni

Gli **script** sono semplici programmi software scritti in un linguaggio interpretato facile da utilizzare, senza interfaccia grafica, che svolgono funzioni molto specifiche ed accessorie, ed in grado di interfacciarsi con altri programmi più complessi per svolgere operazioni più sofisticate. Gli script sono sovente usati per

personalizzare la configurazione automatica di un sistema ICT, per rendere più dinamica una pagina web, per fornire comandi ad un sistema operativo (tipico dei così detti "script shell") e a data base, per personalizzare e rendere "smart" documenti Microsoft Office, Libre Office, o analoghi. Esempi di linguaggi di scripting includono Bash, AppleScript, JavaScript, Perl, Python, PHP, VBScript.
Programmi in script sono usati per attacchi digitali, e quelli più semplici richiedono un intervento umano per farli giungere sul sistema bersaglio (ad esempio l'apertura di un allegato in posta elettronica o lo sfruttamento di un buffer overflow presente in una applicazione); quelli più sofisticati sono in grado di attaccare senza bisogno di interventi di persone.
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 negli ambienti Microsoft Windows è prevalso un altro significato: uno strumento che nasconde la presenza di malware. Tipicamente il rootkit guadagna i diritti di amministratore usando vulnerabilità note o carpendo informazioni via social engineering, e poi modifica il sistema operativo in modo da nascondere la sua presenza e quella di altro malware che ad esempio può installare backdoor, keylogger o strumenti che bloccano o eludono i meccanismi di controllo delle licenze, di protezione delle copie e più in generale i meccanismi di sicurezza digitale.
Gli exploit sono attacchi ad una risorsa ICT basandosi sulle sue vulnerabilità ed il termine "meta exploit" indica strumenti software che facilitano l'individuazione di vulnerabilità e la verifica di come sfruttarle per attuare attacchi, anche con l'aiuto di basi di conoscenza contenenti centinaia di exploit.
Si noti che gli strumenti tipo "toolkit" 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, spesso indicato con 2C, 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 2024, è stata fornita, in tempo reale a chi completa la compilazione, una macro valutazione qualitativa del livello di sicurezza digitale del sistema informativo oggetto delle sue risposte, rispetto alle esigenze di sicurezza dell'azienda/ente per la quale si risponde.
La macro valutazione è stata realizzata assegnando degli opportuni "pesi" numerici a tutte le opzioni di risposta previste nel questionario, rispetto alle domande relative:

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

Nel procedere nella compilazione del questionario, il sistema LImeSurvey, opportunamente configurato e predisposto, somma i pesi delle risposte relative alle domande inerenti A, B ed S.
Calcola poi un Indice di Sicurezza Digitale numerico (IDS) dato dalla formula seguente:

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

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

ALLEGATO B Glossario

2C	Command & Control, indica un sistema centralizzato per coordinare e gestire bootnet e sferrare attacchi soprattutto di tipo DoS/DDoS.
Account	Insieme di informazioni di identificazione ed autenticazione di un utente di un sistema informativo. Tipicamente è costituito da un identificativo d'utente e da una password, ma può estendersi a certificati digitali, riconoscimenti biometrici e richiedere l'uso di token quali smart card, chiavette USB, ecc.
ACL	Access Control List: elenco di regole per il controllo degli accessi a risorse ICT.
ACN	Agenzia Cibernetica Nazionale
Active Directory	Sistema di directory della Microsoft, integrato nei sistemi operativi Windows dal 2000 in avanti. Utilizza SSO, LDAP, Kerberos, DNS, DHCP, etc.
Active X Control	File che contengono controlli e funzioni in Active X che “estendono” (eXtension) ed espletano specifiche funzionalità; facilitano lo sviluppo di software di un modulo software dell’ambiente Windows in maniera distribuita su Internet.
Address spoofing	Generazione di traffico (pacchetti IP) contenenti l’indicazione di un falso mittente (indirizzo sorgente IP).
Adware	Codice maligno che si installa automaticamente nel computer, come un virus o lo spyware, ma in genere si limita a visualizzare una serie di pubblicità mentre si è connessi a Internet. L'adware può rallentare sensibilmente il computer e nonostante costringa l'utente a chiudere tutte le finestre pop-up visualizzate, non rappresenta una vera minaccia per i dati, a meno che non nasconda un codice maligno.
AET	Advanced Elusion Techniques: tecniche avanzate di elusione degli strumenti di sicurezza in uso.
AI	Artificial Intelligence, che individua l’ampio campo delle tecniche e delle teorie di intelligenza artificiale.
AIPSI	Associazione Italiana Professionisti Sicurezza Informatica.
AISE	Agenzia Informazioni e Sicurezza Esterna.
AISI	Agenzia Informazioni e Sicurezza Interna.
API	Application Programming Interface
App	Neologismo ed abbreviazione di "application" (applicazione) per indicare, anche in italiano, le applicazioni operanti localmente sui sistemi mobili, tipicamente su smartphone.
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	O specifico, indicato sovente con il termine inglese targeted attack: attacco portato ad uno specifico sistema obiettivo, o a un gruppo similare di obiettivi, con tecniche sofisticate e specifiche per il sistema target. Viene incluso sovente tra gli ATP.
Attacco massivo	Attacco rivolto ad una grande massa di obiettivi simili, anche dell’ordine di milioni: può essere semplice e non sofisticato, ma nella massa qualche attacco va quasi sempre a buon fine. Tipici esempi i phishing ed i ransomware.
Audit	Per la sicurezza digitale, il risultato di un auditing.
Auditing	Per la sicurezza digitale, il processo documentato di revisione (ossia verifica, controllo e valutazione) della efficacia delle misure in essere e della loro gestione, oltre che della conformità di tali misure alle leggi vigenti e alle normative, anche interne, che devono essere seguite.
Backdoor	Interfaccia e/o meccanismo nascosto che permette di accedere ad un programma superando le normali procedure e barriere d’accesso.

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

CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, all'interno della Polizia Postale e per la Sicurezza Cibernetica.
COBIT	Control Objectives for Information and related Technology: consolidata best practice per il governo (governance) di un SI ed il suo audit.
Consumerizzazione	Si veda BYOD.
Container	Istanza di un ambito virtualizzato di applicazioni, che isola le risorse hardware e software in uso da ognuna di esse, pur sempre all'interno di un solo e unico sistema operativo.
COPASIR	Comitato parlamentare per la sicurezza della Repubblica: è l'organo di controllo parlamentare sulle agenzie italiane di intelligence.
COR	Comando Operazioni in Rete (Ministero Difesa).
CPS	Cyber-Physical System (in ambiti OT).
CRAMM	CCTA Risk Analysis and Management Method
Cryptojacking	Utilizzo di capacità elaborativa di un inconsapevole sistema ICT target da parte di un cybercriminale per creare criptovaluta.
CSIRT	Computer Security Incident Response Team, italiano, ora sotto ACN
Crowdturfing	Combinazione di "crowdsourcing" e "astroturfing", indica *un attacco basato su recensioni scorrette e false per danneggiare la reputazione di un prodotto o di una azienda/ente.*
CSaaS	Cyber Security as a Service
CSO	Chief Security Officer; responsabile della sicurezza dell'intera azienda/ente, prevalentemente per la sicurezza fisica di edifici e del personale. In alcune organizzazioni il CISO riporta a questa figura.
CSSLP	Certified Secure Software Lifecycle Professional.
CTO	Chief Technology Officer: è il direttore tecnico di più alto livello, tipicamente per aziende che producono prodotti e servizi ICT. In talune organizzazioni il CIO riporta a questa figura.
CTTA	Central Computer and Telecommunications Agency del Governo UK, ora chiamato Cabinet Office.
CVE	Common Vulnerabilities and Exposures: l'acronimo indica sia il programma di identificazione e classificazione delle vulnerabilità tecniche di ogni sistema e servizio ICT, sia l'elenco di record delle vulnerabilità identificate.
CVSS	Common Vulnerability Scoring System: metrica internazionale di valutazione della gravità di una vulnerabilità di un sistema ICT.
DAC	Discretionary Access Control.
Darknet	Rete virtuale privata nella quale gli utenti si connettono solamente con persone di cui si fidano.
Dark web	Siti web che si raggiungono via Internet ma attraverso specifici software, configurazioni e accessi autorizzativi, e non sono indicizzati, e quindi ritrovabili, dai motori di ricerca. Molti dark web contengono informazioni criminali, dalla pedopornografia a strumenti informatici di attacco e da account e identità digitali rubate che sono poste in vendita.
Data Breach	Letteralmente "violazione dei dati", spesso è usato come sinonimo di furto di dati. Tecnicamente è usato per indicare l'accesso a banche dati o a file system contenenti identità digitali ed informazioni personali.
Data Center	Centro Dati: si veda CED.
DB	Data Base: banca dati.
DBMS	Data Base Management System.
DCS	Distributed Control System (ambiti OT).
Deadlock	Condizione in cui due o più processi non sono più in grado di proseguire perché ciascuno aspetta il risultato di una operazione che dovrebbe essere eseguita dall'altro.
Deamon:	Software di base operante in back-ground in un ambiente multi-tasking.

Defacement o Defacing	In inglese significa deturpare, e nel gergo della sicurezza digitale indica un attacco ad un sito web per modificarlo o distruggerlo; spesso con tale attacco viene modificata solo la home-page a scopo dimostrativo.
DES	Data Encryption Standard
DoS/ DDoS	Denial of Service e Distributed Denial of Service: attacco per saturare sistemi e servizi ed impedire la loro disponibilità.
Dialer	Programma software che connette il sistema ad Internet, ad una rete o ad un computer remoto tramite linea telefonica (PSTN o ISDN); può essere utilizzato per attacchi e frodi.
DKIM	Domain Keys Identified Mail: in ambito DMARC, chiavi di crittografia asimmetrica per l'autenticazione di ogni messaggio di posta elettronica. Il messaggio viene firmato dal server e il destinatario controlla i messaggi con la chiave pubblica DKIM, che viene fornita nel DNS del dominio.
DMARC	Domain-based Message Authentication, Reporting, and Conformance: sistema standard di autenticazione dei messaggi di posta elettronica, che aiuta gli amministratori della posta a impedire che hacker e altri malintenzionati eseguano lo spoofing dell'organizzazione e del dominio
DNS	Domain Name System.
Docker	Software per la creazione di container
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.
Download	Azione di scaricare file, tipicamente via Internet
Drive-by Downloads	Attacchi digitali causati dallo scaricare (anche inconsapevolmente) codici maligni o programmi malevoli.
Drones, Droni	Si veda bots.
ECDL	European Computer Driving Licence, è il patentino europeo di conoscenza di vari aspetti dell'ICT soprattutto nell'ottica dell'utente finale. Ideato, realizzato e gestito da AICA, da più di venti anni, ha recentemente cambiato nome in ICDL
eCF	European Competence Framework: quadro europeo standardizzato sulle competenze digitali e sui ruoli ICT che espletano professionalmente tali competenze.
ECSF	European Cybersecurity Skills Framework, emanato a fine 2022 da ENISA: considera 10 ruoli per la sicurezza digitale, tra cui il CISO.
EDGE	Enhanced Data rates for GSM Evolution.
EDR	Endpoint Detection and Response.
eIDAS	electronic IDentification Authentication and Signature: fornisce la normativa di base a livello UE sull'identità digitale per i servizi fiduciari e l'identificazione elettronica degli Stati membri. Il precedente Regolamento UE n. 910/2014 è stato aggiornato e superato dal nuovo Regolamento UE n. 1183/2024.
ENISA	European Union Agency for Cybersecurity.
ETACS	Extended TACS.
FIRST	Forum of Incident Response and Security Teams, che attualmente ha incarico la gestione della metrica CVSS.
FTP	File Transfer Protocol: protocollo per il trasferimento di file.
Exploit	Attacco ad una risorsa ICT utilizzando sue vulnerabilità.
Extranet	Intranet accessibile anche da utenti esterni all'azienda/ente.

Ethical hacking	Attività di provare attacchi ai fini di scoprire bachi e vulnerabilità dei programmi, e porvi rimedio con opportune patch/fix.
EUCIP	European Certification of Informatics Professionals: ora sostituito da eCF.
Fix	correzione di un programma software, usato spesso come sinonimo di patch.
Flash threats	Tipi di virus in grado di diffondersi molto velocemente.
Flooding	Letteralmente significa "allagamento" ed è un termini associato a varie tecniche per attacchi DoS/DDoS.
Form	In informatica indica il campo generato da una applicazione visibile su una schermata, nel quale l'utente deve inserire dei caratteri per interagire con l'applicazione stessa; è l'elemento base per l'interfaccia tra utente e applicazione per l'inserimento dei dati (data entry).
FSD	Fornitori di Servizi Digitali, così come definiti da NIS.
FTPS	File Transfer Protocol Secure: per il trasferimento di file crittati
FW	FireWall generico, normalmente di rete.
FWA	FireWall Applicativo.
GDPR	General Data Protection Regulation: Regolamento 2016/679 UE per la protezione dei dati personali delle persone fisiche (privacy).
GPRS	General Packet Radio Service.
GSM	Global System for Mobile communications.
Hactivism	Termine derivato dalla combinazione di hack e di activism, indica un uso sovversivo dell'ICT per promuovere un'ideologia politica/religiosa e la sua agenda o un cambiamento sociale.
Hijacking	Tipico attacco in rete "dell'uomo in mezzo" tra due interlocutori, che si maschera per uno dei due e prende il controllo della comunicazione. In ambito web, questo termine è usato per indicare un attacco ove: le richieste di pagine a un web vengo dirottate su un web falso (via DNS), sono intercettati validi account di e-mail e poi attaccati questi ultimi (flooding).
Hoax	In italiano "bufala" o burla, indica la segnalazione di falsi virus; rientra tra le tecniche di social engineering.
Honeynet	Rete di honeypot.
Honeypot	Sistema "trappola" su Internet per farvi accedere con opportune esche possibili attaccanti e poterli individuare.
Hosting	Servizio che "ospita" risorse logiche ICT del Cliente su hardware del fornitore del servizio.
Housing	Concessione in locazione di uno spazio fisico, normalmente in un Data Center già attrezzato, ove riporre, funzionanti, le risorse ICT di proprietà del Cliente.
HSDPA	High Speed Downlink Packet Access.
HTTPS	HyperText Transfer Protocol Secure: protocollo sicuro per le transazioni crittate tra browser e sito web, e viceversa.
Hypervisor	Elemento di base di un sistema virtualizzato, che crea e gestisce sistemi virtuali.
IAA	Identificazione - Autenticazione – Autorizzazione: per il controllo degli accessi ai sistemi ICT.
IaaS	Infrastructure as a Service.
IAM	Identity & Access Management.
ICDL	International Certification of Digital Literacy. Nuovo nome dato alle precedenti certificazioni ECDL di AICA, portate a livello europeo ed internazionale e che rappresentano lo standard riconosciuto per la computer literacy.
ICS	Industrial Control System (in ambienti OT)
IDS	Intrusion Detection System.
Information Leakage	Diffusione-dispersione non autorizzata di informazioni.
Info stealer (anche infostealer)	Malware progettati per carpire informazioni, tipicamente quelle di un utente mentre effettua un login

Intranet	Rete e server operanti in http/https ed accessibili solo ad utenti interni ad una data azienda/ente.
IoT	Internet of Things (Internet delle Cose): componenti/sistemi intelligenti ed interoperanti su Internet, tipici di ambienti OT.
IIoT	Industrial IoT.
IPS	Intrusion Prevention System
ISACA	Information Systems Audit and Control Association.
ISSA	Information Systems Security Association: AIPSI è il suo capitolo italiano
ISTAT	Istituto Nazionale di Statistica
ITIL	Information Technology Infrastructure Library: consolidata best practice per la gestione operativa (management) di un SI.
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.
KEV	Known Exploited Vulnerabilities, catalogo basato su CVE e gestito dalla agenzia statunitense CISA
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	Codice indirizzo assegnato in modo univoco ad ogni scheda di rete.
MAC	Media Access Control: sub strato del livello datalink del modello ISO/OSI.
MAC flooding	Tecnica di attacco tipo DoS/DDoS ad un dispositivo con indirizzo MAC per saturarlo e bloccarne il corretto funzionamento.
Malicious insider	Attaccante interno all'organizzazione cui viene portato l'attacco.
Malvertising	Contrazione di "malicious advertisements": pubblicità malevola, con pagine web che nascondono un codice maligno o altre tecniche di attacco, come il dirottamento su siti web mascherati e fraudolenti.
Malware	Termine generico che indica qualsiasi tipo di programma software di attacco.
MaaS	Malware as a Service: fornitura in cloud di malware (a pagamento).
MEHARI	MEthod for Harmonized Analysis of RIsk
MFA	Multi-Factor Authentication: autenticazione con più fattore, ad esempio con certificati, token diversi e identificazioni biometriche
Microservizi	Approccio allo sviluppo ed all'organizzazione dell'architettura dei software, evoluzione dell'architettura SOA e dell'object orientation. I microservizi sono moduli software autonomi, specializzati, indipendenti di piccole dimensioni che comunicano tra loro tramite API ben definite. Le architetture dei microservizi permettono di scalare e sviluppare le applicazioni in modo rapido e semplice.
Mirroring	termine inglese per indicare la replica e la sincronizzazione di dati su due o più dischi.

MSS	Managed Security Service.
MSSP	Managed Security Service Provider: fornitore di servizi per la sicurezza digitale.
NAC	Network Access Control: termine usato con più significati, che complessivamente indica un approccio architetturale ed un insieme di soluzioni per unificare e potenziare le misure di sicurezza a livello del punto di accesso dell'utente al sistema informativo.
NCS	Nucleo per la cybersicurezza ora operante in ambito ACN.
NFT	Non Fungible Token: è un gettone non riproducibile nell'ambito di una blockchain. Gli NFT sono associati a beni virtuali, da un documento a un'opera d'arte, e come tali hanno un mercato mondiale.
NIS	Network and Information Security: direttiva UE 2016/1148, recepita in Italia con il D. Lgs. n. 65 del 18/5/2018, che definisce le misure di sicurezza digitale necessarie a livello di ogni paese membro per le infrastrutture ICT critiche, chiamate anche "servizi essenziali".
NIS2	Aggiornamento ed ampliamento della NIS con direttiva UE , recepita in Italia da
NIST	National Institute of Standards and Technology
NSTPFT	Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza contrastare le frodi telematiche ed informatiche, nonché tutelare la privacy.
NVD	National Vulnerability Database statunitense, gestito da NIST
OASIS	Consorzio di aziende ICT no profit che fornisce norme implementative per alcuni standard, tra i quali la SOA e la sua sicurezza (SALM SPML, XACML).
OLE	Object Linking and Embedding.
OPC	OLE for Process Control (ambito OT).
OPS	Open Platform Communications. Standard de facto per la comunicazione tra sistemi OT
OPS UA	Open Platform Communications Unified Architecture.
OSA	Open Security Architecture.
OT	Operational Technology.
OTP	One Time Password: logica e/o dispositivo che genera password da usarsi una sola volta per sessione/transazione.
Outsourcer	Fornitore di servizi digitali terziarizzati.
OWASP	Open Web Application Security Project
PaaS	Platform as a Service.
PAC	Pubblica Amministrazione Centrale.
PAC	Programmable Automation Controller (ambiti OT)
PAL	Pubblica Amministrazione Locale.
PAM	Privileged Access Management.
Payload	"Carico utile" di informazioni all'interno di un programma, di un protocollo, ecc.; tipicamente è il codice maligno da attivare sul sistema attaccato dopo esservi penetrati.
PEC	Posta Elettronica Certificata.
Pharming	Attacco digitale per carpire informazioni riservate di un utente basato sulla manipolazione dei server DNS o dei registri del sistema operativo del PC dell'utente.
Phishing	Attacco digitale di social engineering per carpire informazioni riservate di un utente, basato sull'invio di un falso messaggio in posta elettronica che fa riferimento ad un ente primario, che richiede di collegarsi ad un server (trappola) per controllo ed aggiornamento dei dati.
PID	Proportional-Integral-Derivative (in ambito OT)
Ping of death	Invio di pacchetti di ping di grandi dimensioni (ICMP echo request), che blocca la pila di protocolli TCP/IP: è un tipo di attacco DoS/DDoS.
PLC	Programmable Logic Controller (ambiti OT).
PMI	Piccole e Medie Imprese: sotto i 250 dipendenti.
PNRR	Piano Nazionale di Ripresa e di Resilienza.

Port scanner	Programma software che esplora una fascia di indirizzi IP sulla rete per verificare quali porte, a livello superiore, sono accessibili e quali vulnerabilità eventualmente presentano. È uno strumento di controllo della sicurezza, ma è anche uno strumento propedeutico ad un attacco.
Provisioning	Attività grazie alle quale vengono fornite le opportune risorse ICT e la loro configurazione, in particolare i diritti d'accesso, ad utenti di un SI
PUP	Potentially Unwanted Programs: programma che l'utente consente di installare sui suoi sistemi ma che, a sua insaputa, contengono codici maligni o modificano il livello di sicurezza del sistema. Tipici esempi: adware, dialer, sniffer, port scanner.
QR	Quick Response: è un codice a barre bidimensionale, ossia a matrice, che è impiegato per memorizzare informazioni generalmente destinate a essere lette tramite uno smartphone.
Race condition	Termine che indica le situazioni derivanti da condivisione di una risorsa comune, ad esempio un file o un dato, ed in cui il risultato viene a dipendere dall'ordine in cui vengono effettuate le operazioni.
Ransomware	Codice maligno che restringe e/o blocca i diritti d'accesso e tramite il quale viene chiesto un riscatto (ransom) per far funzionare correttamente il sistema.
RBAC	Request Based Access Control.
RBAC	Role Based Access Control.
RFID	Radio-Frequency Identification: tecnologia per l'identificazione e/o memorizzazione automatica di informazioni inerenti oggetti, animali o persone, basata su un tag intelligente identificativo dell'entità oggetto dell'identificazione ed un dispositivo in grado di riconoscere l'entità se in sua prossimità, scambiando in radio frequenza delle informazioni.
Ricatto	L'attacco digitale perpetrato viene poi usato per ricattare l'attaccato perché paghi per non subirne di altri, magari più perniciosi. Il malware ransomware ha come tipica motivazione il ricatto, che è un tipo della più generale frode informatica.
Ritorsione	L'attacco digitale è stato portato come "vendetta" verso torti subiti, o come tali ritenuti: tipico il caso di un dipendente cui è stata negata una sua richiesta, o di ex dipendente licenziato. L'attaccante intende "colpire" con un attacco digitale l'Azienda/Ente che ritiene "colpevole" dei (presunti) torti subiti.
Robot	Un sistema in grado di svolgere, più o meno indipendentemente, un lavoro al posto dell'uomo
Robotica	La disciplina dell'ingegneria che studia e sviluppa metodi che permettano a un robot di eseguire dei compiti specifici riproducendo in modo automatico il lavoro umano.
Rogueware	Falso antivirus che a sua volta è un codice maligno che infetta il sistema.
Rootkit	Programma software di attacco che consente di prendere il completo controllo di un sistema, alla radice come indica il termine.
RPU	Remote Processor Unit (in ambiti OT).
SaaS	Software as a Service.
SALM	Security Assertion Markup Language.
SASE	Secure Access Service Edge.
SCADA	Supervisory Control And Data Acquisition: sistema informatico distribuito per il controllo ed il monitoraggio di processi, ed in parte per la loro automazione, in ambiti OT.
Scam	Tentativo di truffa via posta elettronica. A fronte di un millantato forte guadagno o forte vincita ad una lotteria, si chiede di versare un anticipo o pagare una tassa.
Scammer	Chi effettua uno scam.
SCAP	Security Content Automation Protocol.
SCC	Security Command Centre.
Scareware	Software d'attacco che finge di prevenire falsi allarmi, e diffonde notizie su falsi malware o attacchi.

Scraping	Letteralmente significa “raschiando”, è il termine usato per indicare l’attività di ricerca e raccolta, in maniera automatica, di determinate informazioni dai sistemi connessi in Internet.
SD-WAN	Software Defined WAN (Wide Area Network)
SGSI	Sistema Gestione Sicurezza Informatica.
SIEM	Security Information and Event Management: sistemi e servizi per la gestione in tempo reale di informazioni ed allarmi generati dalle risorse ICT di un sistema informativo, inclusi i log.
Sinkhole	metodo per reindirizzare specifico traffico Internet per motivi di sicurezza, tipicamente per analizzarlo, per individuare attività anomale o per sventare attacchi. Può essere realizzato tramite darknet o honeynet.
Sistema Informatico	Insieme dei sistemi e dei servizi ICT, dalle reti ai server ed agli applicativi, anche terziarizzati e in cloud, organizzato in una specifica architettura e che una azienda/ente usa a supporto delle proprie attività. Il sistema informatico può includere anche i dispositivi d’utente fissi e mobili (PC, smartphone, tablet, etc.), i sistemi di automazione e controllo industriale (DCS, PLC, robot, ecc.) ed i dispositivi IoT. Il termine indica quindi l’insieme dei sistemi ICT che lo costituiscono
Sistema Informativo	Indica il Sistema Informatico con tutte le informazioni che vi sono trattate.
Sniffing-snooping	Tecniche mirate a leggere il contenuto (pay load) dei pacchetti in rete, sia LAN che WAN.
Slack	Servizio di messaggistica per le aziende che collega le persone alle informazioni di cui hanno bisogno, creando e gestendo gruppi di lavoro.
Smart city	Città “intelligente” largamente dotata di infrastrutture e soluzioni ICT sia per i suoi abitanti e per interagire con loro, sia per migliorare il controllo del territorio, della sua sicurezza, dell’ambiente, della viabilità, ecc.
Smart grid	Grid è la rete elettrica di distribuzione di energia, che affiancata da una rete informatica che la gestisce diviene “smart”.
Smishing	Attacco di social engineering per carpire informazioni riservate di un utente, basato sull’invio di SMS. E’ l’analogo del phishing con la posta elettronica.
SMS	Short Message Service.
Smurf	Tipo di attacco per la saturazione di una risorsa, avendo una banda trasmissiva limitata. Si usano tipicamente pacchetti ICMP Echo Request in broadcast, che fanno generare a loro volta ICMP Echo Replay.
SOA	Service Oriented Architetture.
SOAR	Security Orchestration, Automation and Response: sistemi di automazione ed integrazione dei vari strumenti e processi di sicurezza digitale.
SOC	Security Operation Centre
Social Engineering	Ingegneria sociale: con questo termine vengono considerate tutte le modalità di carpire informazioni, quali l’user-id e la password, per accedere illegalmente ad una risorsa informatica.
Spamming	Invio di posta elettronica “indesiderata” all’utente.
SPF	Sender Policy Framework: in DMARC, un record di testo DNS nel dominio considerato, che indica ai servizi di posta e ai ricevitori di ricevere l'e-mail dall'IP del server fornito nel record SPF.
SPID	Sistema Pubblico di Identità Digitale: è attualmente obbligatorio per accedere on line ai servizi digitali delle Pubbliche Amministrazioni.
SPML	Service Provisioning Markup Language.
Spoofing	Attacco digitale che falsifica l'indirizzo nell'intestazione Da: di un messaggio email. Un messaggio contraffatto mediante lo spoofing sembra provenire dall'organizzazione o dal dominio la cui identità è stata rubata.

Spyware	Codice maligno che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete, etc.) senza il suo consenso, utilizzandole poi per trarne profitto, solitamente attraverso l'invio di pubblicità mirata.
SQL	Structured Query Language: linguaggio per interazione con un DB relazionale.
SQL injection	Tecnica di inserimento di codice in un programma che sfrutta delle vulnerabilità sul database con interfaccia SQL che viene usata dall'applicazione.
SSCP	Systems Security Certified Practitioner.
SSO	Single Sign On: autenticazione unica per avere accesso a diversi sistemi e programmi.
Stealth	Registrazione invisibile.
Stuxnet	Uno dei primi e più noti attacchi ATP, portato ai sistemi di controllo delle centrifughe delle centrali nucleari iraniane.
SYN Flooding	Invio di un gran numero di pacchetti SYN a un sistema per intasarlo (DoS/DDoS).
TA	Targeted Attacks: attacchi mirati, talvolta persistenti, effettuati con più strumenti anche contemporaneamente; rientrano in questa categoria APT e Watering Hole.
TACS	Total Access Communication System.
Telegram	Servizio di messaggistica istantanea e di broadcasting criptato e gratuito.
TLC	Telecomunicazioni.
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.oadweb.it.
Utente finale	Utente di un sistema d'utente e/o di una o più applicazioni con i diritti di accesso relativi al suo ruolo, ma non di tipo privilegiato.
Utente privilegiato	Utenti con diritti d'accesso privilegiati: includono operatori, manutentori ed amministratori di sistema di un sistema informativo, che hanno i più elevati diritti per poter accedere e gestire le risorse ICT del sistema informatico sulle quali debbono operare. Rientrano in questa categoria anche gli sviluppatori di software. Gli attuali trend di forte terziarizzazione di queste funzioni portano a personale esterno dei fornitori dell'azienda/ente cliente tali diritti, con la necessità di maggiori controlli su di loro per assicurarsi l'adeguate livello di sicurezza digitale.
Vishing	Attacco di social engineering per carpire informazioni riservate di un utente, basato su chiamate telefoniche. E' l'analogo del phishing con la posta elettronica.
VoIP	Voice over IP.
VPN	Virtual Private Network: rete virtuale creata tramite Internet per realizzare una rete "privata" e sicura per i soli utenti abilitati.
XACML	eXstensible Access Control Markup Language.
XSS	Cross - site scripting: una vulnerabilità di un sito web che consente di inserire a livello "client" dei codici maligni via "script", ad esempio JavaScript, ed HTML per modificare le pagine web che l'utente vede.
Watering Hole	Famiglia di attacchi che rientrano nella categoria dei Targeted Attack. Il termine, traducibile in" attacco alla pozza d'acqua", fa riferimento agli agguati di animali carnivori alle prede

	che si dissetano in una pozza d'acqua. La metafora è usata per attacchi mirati a siti web specialistici, ad esempio di finanza, di politica, di strategie, ecc., cui una persona o un'azienda target accede periodicamente.
Wiper	Malware distruttivo che manipola e/o cancella il driver di un hard disk, eliminando tutti i dati archiviati e non consentendo più il suo utilizzo.
Worm	Tipo di virus che non necessita di un file eseguibile per attivarsi e diffondersi, dato che modifica il sistema operativo del sistema attaccato in modo da essere eseguito automaticamente e tentare di replicarsi sfruttando per lo più Internet.
Zero-day attack	Attacchi basati su vulnerabilità ancora non note e/o a cui non è ancora stato trovato rimedio.
Zombies, zombi	Si veda bots.

ALLEGATO C Profili SPONSOR SILVER

OAD
Osservatorio
Attacchi Digitali
in Italia

Gruppo Qintesi

www.qintesi.com

Il Gruppo Qintesi – con un organico di oltre 400 dipendenti – è una *Tech-Company* che eroga servizi di *management consulting* e *system integration*. Contribuisce ad accrescere il valore e migliorare la competitività dei clienti supportandoli nei processi di digitalizzazione ed innovazione, attraverso una *value proposition* basata su soluzioni applicative SAP, Google e Kyriba, 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" ed 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)
UNI/PdR 125:2022 per la "Parità di genere", ottenuta nel 2023, che attesta l'impegno di Qintesi nel supportare l'empowerment femminile all'interno dei percorsi di crescita aziendale, lo sviluppo di una leadership equa ed il contrasto di stereotipi, divari, penalizzazioni e disparità a tutti i livelli.

Qintesi ha anche ottenuto importanti riconoscimenti, quali:

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

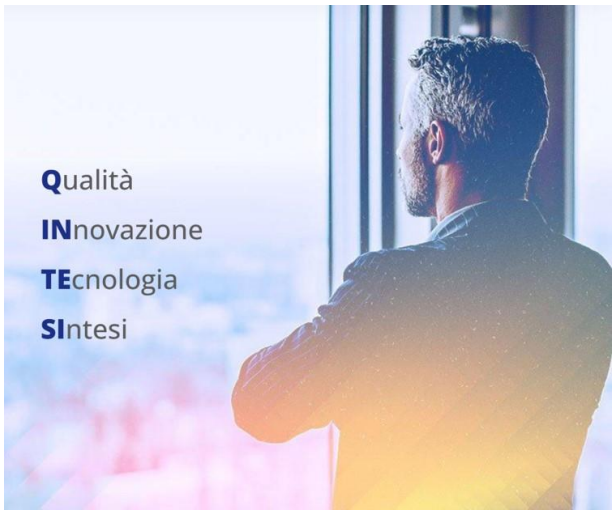
Qintesi è **Google Cloud Partner** e ha realizzato alcuni tra i primi progetti a livello europeo di migrazione a SAP S/4HANA su piattaforma Google Cloud Platform; è attiva, inoltre, in importanti progetti di digital transformation basati sulla piattaforma Google.

Qintesi ha inoltre avviato una partnership con **Kyriba**, società leader mondiale nelle soluzioni di tesoreria e finanza in cloud.

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' ICDL (ex ECDL) e l'eCF (UNI EN 16234-1:2016): per quest'ultimo è accreditata in Italia 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/

ANIPA

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

https://www.anipa.it/

Anitec-Assinform

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

https://www.anitec-assinform.it/

ANORC

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

https://anorc.eu/

ASSI-Bologna

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

www.assi-bo.it

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.ased.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 del Digitale e dell'Innovazione di Torino

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

http://www.clubdi.org/

Club Dirigenti Tecnologie dell'Informazione di Roma

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

https://www.cdti.org/

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

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

Club per le Tecnologie dell'Informazione di Milano

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT 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 di varie Associazioni (i cui soci possono essere solo persone fisiche) della tecnologia dell'informazione, molti dei quali operanti a livello regionale. Si propone come "nodo" attivo del Sistema-Paese per lo sviluppo del settore delle tecnologie dell'informazione e della comunicazione, e per aiutare le Associazioni socie nella crescita della professionalità e delle competenze dei loro 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 in diversi settori dell'ICT. Aderisce a FIDAInform.

http://www.inforav.it/

SESAMO

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

http://www.sesamoamministratori.it/

Allegato E Principali fonti e riferimenti

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

- FTI: "Osservatorio sulla criminalità informatica – Rapporto 1997", Franco Angeli.
- M. R. A. Bozzetti, P. Pozzi (a cura di): "Cyberwar o sicurezza? Secondo Osservatorio Criminalità ICT", 2000, Franco Angeli.
- M. R. A. Bozzetti, R. Massotti, P. Pozzi (a cura di): "Crimine virtuale, minaccia reale", 2004, Franco Angeli
- M. R. A. Bozzetti, F. Zambon: "Sicurezza Digitale – una guida per governare un sistema informatico sicuro", Giugno 2013, Soiel International, ISBN 9788890890109
- I vari Rapporti annuali OAI e OAD: https://www.oadweb.it/it/main-it/rapporti-e-relativi-convegni.html
- Marco R. A. Bozzetti: "Attacchi digitali e misure di sicurezza: l'indagine OAD di AIPSI", SecSolution Magazine n.34, p. 75-78, Agosto 2024: https://www.secsolution.com/notizia.asp?id=18956&c=0
- Marco R. A. Bozzetti: "Come evolvono gli attacchi cyber in Italia: le indagini OAD di AIPSI", Agenda Digitale 360, 1 Agosto 2024: https://www.agendadigitale.eu/sicurezza/evoluzione-degli-attacchi-digitali-in-italia-lanalisi-delle-indagini-oad-di-aipsi/

E.2 Le principali fonti sugli attacchi e sulle vulnerabilità

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

- ACN, Agenzia Cybersicurezza Nazionale: https://www.acn.gov.it/
- AGID, Agenzia per l'Italia Digitale: https://www.agid.gov.it/
- CISA, Cybersecurity Infrastructure Security Agency, (), è l'Agenzia statunitense per la sicurezza informatica e delle infrastrutture (analoga all'ACN italiana): https://www.cisa.gov/
- CSIRT, Computer Security Incident Response Team – Italia: https://csirt.gov.it/
- CVE, Common Vulnerabilities and Exposures, è un elenco aggiornato di tutte le vulnerabilità note pubblicamente, identificate da un numero univoco: https://cve.mitre.org/
- Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri: https://innovazione.gov.it/
- ENISA, European Union Agency for Network and Information Security: http://www.enisa.europa.eu/
- First, Forum for Incident Response and Security Team, fornisce aggiornate informazioni su attacchi e vulnerabilità, classificandole in base al CVSS, Common Vulnerability Scoring System: http://www.first.org/
- Internet Crime Complaint Center (IC3) è una partnership tra FBI (Federal Bureau of Investigation), il National White Collar Crime Center (NW3C) e il Bureau of Justice Assistance (BJA), e fornisce, oltre alla possibilità di denunciare negli US attacchi digitali, informazioni sugli attacchi stessi e sui trend in atto per i crimini digitali: https://www.ic3.gov/
- NVD, National Vulnerability Database, è l'archivio statunitense di informazioni sulla vulnerabilità standardizzate e gestibili in maniera automatizzata con il protocollo SPAC: https://nvd.nist.gov/
- OECD, Organisation for Economic Co-operation and Development, produce rapporti sui rischi e gli attacchi digitali che impattano sull'economia delle nazioni in Europa: http://www.oecd.org/sti/ieconomy/security.htm

- OWASP, Open Web Application Security Project, progetto open source per la sicurezza delle applicazioni web, fornisce vari rapporti e linee guida sul tema, tra cui, periodicamente, le "top ten", le vulnerabilità ed i rischi più critici per le applicazioni web: https://www.owasp.org/
- SANS Institute fornisce sistematicamente segnalazioni su vari tipi di attacchi e di vulnerabilità, oltre all'aggiornato elenco 20 prioritari controlli di sicurezza per le norme Federali US FISMA: www.sans.org
- Sistema di informazione per la sicurezza della Repubblica Italiana, insieme di organi e autorità che hanno il compito di assicurare le attività di informazione per la sicurezza, allo scopo di salvaguardare la Repubblica da ogni pericolo e minaccia proveniente sia dall'interno sia dall'esterno del Paese, inclusa la sicurezza digitale: http://www.sicurezzanazionale.gov.it/
- WASC, Web Application Security Consortium, effettua vari progetti indipendenti sulla sicurezza digitale per le applicazioni web, e fornisce il WASC Threat Classification Online, simile a OSWAP: http://www.webappsec.org/,
- World Economic Forum, realizza un annuale rapporto sui rischi globali, che includono anche i rischi ICT e le cyberwar: https://www.weforum.org/reports/global-risks-report-2023/

Allegato F AIPSI

AIPSI, Associazione Italiana Professionisti della Sicurezza Informatica (https://www.aipsi.org/), capitolo italiano di **ISSA**, la più grande organizzazione mondiale no-profit dedicata alla sicurezza informatica (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 principale obiettivo di AIPSI 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.
Gli elementi che caratterizzano AIPSI includono l'etica professionale dei soci, la sua terzietà rispetto a qualsiasi fornitore ed ente, la qualità ed il livello professionale sempre ricercato per le proprie iniziative, l' internazionalità che consente di avere contatti e di coinvolgere esperti dei vari Capitoli di ISSA a livello mondiale.
Da inizio 2024 AIPSI prevede 3 tipologie di socio: il Socio AIPSI-ISSA, con la fee annua di US $ 160,00, il Socio solo AIPSI, con la fee annua di € 50,00, il Socio GIOVANE (con il primo anno gratuito ed i successi fino a 26 anni compiuti con la fee annua di € 25,00. Queste tre tipologie di socio possono usufruire dei diversi servizi erogati da ISSA e da AIPSI come dettagliato nella tabella a fianco.

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

Oltre a qualificati webinar, iniziative ed eventi, alcuni aperti al pubblico altri riservati ai soli Soci, tra i quali corsi di formazione e certificazioni professionali con significativi sconti, AIPSI ha attivato un importante servizio di mentorship di indirizzamento e crescita professionale gratuito per tutti i Soci, dettagliato in https://www.aipsi.org/aree-tematiche/sig-riservati-ai-soci/crescita-e-percorsi-professionali/mentorship-aipsi.html

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 libere associazioni di professionisti nell'ambito digitale (https://fidainform.it/).

Essere Socio di AIPSI significa entrare in una comunità e in un ecosistema di interessati, appassionati e di professionisti della sicurezza digitale, tema interdisciplinare e non solo tecnico, che opera per la diffusione della cultura della sicurezza digitale e per la crescita professionale.

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

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

Allegato G Malabo srl

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

Che cosa Malabo può offrire::

- 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 Informativo, 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, assessment delle competenze ICT;
  - 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 il cliente in modo che l'ICT crei un effettivo e misurabile **valore** per il suo business e per le sue attività.

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

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

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

Allegato H Il profilo dell'autore Marco R. A. Bozzetti

Marco Rodolfo Alessandro Bozzetti

Ingegnere elettronico laureato al Politecnico di Milano, 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 sia lato 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 CIO 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 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, 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, insieme alle principali Fiere nazionali dell'ICT in Europa, EITO, European Information Technology Observatory, l'indagine annuale europea sul mercato ICT e sui suoi trend tecnologici. 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 un valore per il business effettivamente misurabile.
I suoi principali campi di intervento includono il governo e la gestione di un sistema informativo (ITIL, COBIT, ISO e NIST standard), la sicurezza digitale, l'analisi e gestione dei rischi ICT e dei loro impatti (BIA), il progetto e l'implementazione della "Business Continuity" e del Piano di Disaster Recovery, il disegno di architetture ICT, la razionalizzazione, la definizione ed il supporto di strategie ICT, l'assessment delle competenze e dei ruoli ICT, l'analisi del valore per l'ICT, la trasformazione digitale e l'innovazione tramite l'ICT, la riorganizzazione di strutture e processi ICT, il supporto per la compliance alle varie normative italiane ed europee.
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 universitari. 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, e tutti gli argomenti elencati negli interventi consulenziali di cui sopra. In tutti i corsi inserisce 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 (https://www.aipsi.org/), Capitolo Italiano della mondiale ISSA (https://www.issa.org/), nel Consiglio Direttivo e Tesoriere di FIDAInform (www.fidainform.it), socio e revisore dei conti del ClubTI di Milano (https://www.clubtimilano.net/), socio AICA (https://www.aicanet.it/)**.**
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 ad oggi 340 pubblicazioni, e tra queste più di 50 tra libri e rapporti anche internazionali. Gli argomenti includono l'evoluzione tecnologica dell'ICT e del suo mercato, la sicurezza digitale, le normative europee ed italiane, la trasformazione digitale, gli scenari e gli impatti dell'ICT, le competenze digitali.

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
Ai fini della legge sulla privacy, si autorizza l'uso e la circolazione del presente curriculum vitae.

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

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

OAD Osservatorio Attacchi Digitali in Italia

aipsi ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

ASSOCIAZIONI PATROCINANTI OAD 2024