

Connettendo il futuro  
Consapevolezza e Strategie del rischio cyber per le PMI

16.11.2023 | SAVE THE DATE

In collaborazione con  
VOLTA vianova kaspersky  
Cubbit aipsi ThinkQUANTUM

aipsi  
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

CERBEYRA  
your safe digital future  
Centro Studi Cyber Defense



## *I principali dati emersi dal Rapporto OAD 2023 di AIPSI sugli attacchi e le misure di sicurezza digitali in Italia in tempi di cyber warfare*

**Marco R. A. Bozzetti** (Presidente AIPSI, Founder e CEO Malabo srl)

**OAD**  
Osservatorio  
Attacchi Digitali  
in Italia

**aipsi**  
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

**Rapporto 2023 OAD**  
a cura di Marco R. A. Bozzetti  
con la collaborazione della Polizia Postale e delle Comunicazioni

Sponsor Gold  
QNTESI

Indagine AIPSI realizzata da  
malabo  
CCP ADVISORY



# L'indagine OAD/OAI dal 2007 ad oggi



- **16 anni consecutivi di indagini**
  - basate su questionari online anonimi
  - libero accesso al questionario per tutti i referenti di un sistema informativo operante in Italia
- **Per tutti i settori merceologici + Pubbliche Amministrazioni Centrali e Locali**
- **12 Rapporti pubblicati**
- Un sito ad hoc: [www.oadweb.it](http://www.oadweb.it)

# L'indagine online di AIPSI per OAD 2023

- Questionario online **assolutamente anonimo** basato sull'applicazione Limesurvey nel dominio oadweb.it
- **Questionario ridotto e semplificato** in modo da ridurre il tempo necessario a compilarlo, mantenendo significativi i contenuti e garantendo una continuità con le principali informazioni raccolte nelle precedenti indagini.
  - Si focalizza, con domande dettagliate, sugli **attacchi agli ambienti ed applicativi web nel 2022**
  - Per tutte le altre tipologie di attacco solo una domanda, ed una sulle tecniche di attacco **nel 2022**
  - **Opzionali** le domande sulla **misure** tecniche ed organizzative di sicurezza digitale in essere
- Software Limesurvey programmato per il salto in automatico delle sotto-domande in caso di risposta negativa alla domanda primaria
- Questionario online da fine gennaio a fine agosto 2023
- 326 totale risposte raccolte ed elaborate
  - Di questi il 42,2% ha risposto alle **domande opzionali sulle misure di sicurezza**

## Tipologie e tecniche di attacco in OAD

- **Tipologie di attacco digitale**
  - *Che cosa si attacca* → *obiettivo attacco*
    - *Dal singolo dispositivo fisico alle reti e alle applicazioni*
    - *Considerate 13 tipologie*
- **Tecniche di attacco digitale**
  - *In che modo e con quali tecniche si attacca*
    - *Considerate 7 famiglie di tecniche*

# Tipologie attacchi digitali in OAD 2023

1. Distruzione e/o compromissione FISICA di dispositivi ICT FISSI o di loro parti
2. FURTO dispositivi FISSI ICT o di loro parti
3. FURTO di dispositivi ICT mobili di proprietà dell'azienda/ente e in uso presso i suoi dipendenti/collaboratori
4. FURTO INFORMAZIONI da singoli specifici sistemi FISSI ICT (PC, server, storage system, etc.) del Sistema Informativo, anche terziarizzati/in cloud
5. FURTO INFORMAZIONI relative all'azienda/ente da sistemi MOBILI (palmari, smartpone, 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. *Nel corso dell'intero 2022 il Sistema Informativo ha subito attacchi digitali la cui tipologia non è stata individuata*

# Famiglie di tecniche di attacco considerate in OAD 2023

- **Attacco fisico:** per distruggere dispositivi ICT, ad esempio come atto vandalico o di terrorismo, include anche il furto di dispositivi ICT o di loro parti (ad esempio l'hard disk)
- Raccolta informazioni (**social engineering**): con le quali si possono compiere attacchi, quali ad esempio tecniche di social engineering, phishing, pharming, hoax, scannerizzazioni e ricerche in Internet, ecc.
- **Script e programmi maligni** quali ransomware, spyware, adware, ecc.
- **Agenti autonomi:** programmi maligni che si replicano e diffondono autonomamente, come virus e worm
- **Toolkit:** programmi in grado di scoprire e sfruttare vulnerabilità (rootkit, metaexploit, ecc.)
- **Strumenti distribuiti controllati centralmente** (da un Command Control) quali botnet
- **Utilizzo di due o più delle precedenti tecniche** (tipicamente, ad esempio, negli APT, Advanced Persistent Threat)

# Rapporto 2023 OAD e come scaricarlo



- 168 pagine A4, 133 immagini e grafici
  - 8 Capitoli (128 pagine A4)
  - 8 Allegati (40 pagine A4)
  - Nel Capitolo 8 i dati dalla Polizia Postale e delle Telecomunicazioni
  - Executive Summary in italiano e in inglese

6

Per scaricare il Rapporto 2023 OAD: <https://www.oadweb.it/>

- *Dopo aver fatto il login → occorre registrarsi al sito*

# I patrocinatori di OAD 2023 ed il loro ruolo nell'indagine



# Indice del Rapporto OAD 2023

Il quadro generale

Attacchi rilevati da OAD 2023

Misure sicurezza da OAD 2023

**Sommario**

1. Sintesi direzionale.....	5
1bis. Executive Summary.....	9
2. L'indagine OAD.....	13
3. Il quadro generale degli attacchi digitali intenzionali.....	16
3.1 I principali attacchi digitali a livello mondiale nel 2022.....	20
3.1.1 Esempi di significativi di attacchi a livello mondiale nel 2022.....	22
3.2 I principali attacchi digitali in Italia nel 2022.....	25
3.3 Le vulnerabilità causa degli attacchi.....	26
3.3.1 Le vulnerabilità tecniche.....	26
3.3.2 Le vulnerabilità delle persone.....	29
3.3.3 Le vulnerabilità organizzative.....	30
3.2 Gli attaccanti e le loro motivazioni.....	31
3.3 Le contromisure per la sicurezza digitale e la loro evoluzione.....	32
3.4.1 La terziarizzazione della sicurezza digitale.....	34
3.5 Il quadro di riferimento italiano per la sicurezza digitale.....	35
3.5.1 Aziende e PA in Italia.....	35
3.5.2 La spesa in sicurezza digitale in Italia nel 2022.....	36
3.5.3 Il PNRR ed il suo impatto nella trasformazione digitale del Paese.....	37
3.5.4 Le istituzioni per la sicurezza digitale.....	39
4. Gli attacchi digitali in Italia dall'indagine OAD 2023.....	42
4.1 Tipologie e tecniche di attacco emerse dall'indagine OAD 2023.....	44
4.2 Gli attacchi digitali alle applicazioni ed agli ambienti web in Italia dall'indagine OAD 2023.....	47
5. Tipologia attacchi digitali e tecniche di attacco più temute nel prossimo futuro.....	56
6. Il campione delle aziende/enti rispondenti e dei loro sistemi informativi emerso dall'indagine OAD 2023.....	59
6.1 Tipologia, ruolo e principali caratteristiche dei sistemi informativi delle aziende/enti rispondenti.....	59
6.2 L'Azienda/Ente rispondente.....	65
6.3 Ruolo della persona rispondente.....	70
7. Le misure di sicurezza digitale nei sistemi informativi delle aziende/enti rispondenti.....	72
7.1 Le misure organizzative per la sicurezza digitale in essere nelle aziende/enti rispondenti.....	73
7.1.1 La struttura organizzativa per la sicurezza digitale ed il ruolo di CISO nelle aziende/enti rispondenti.....	74
7.1.2 Policy e procedure organizzative per la sicurezza digitale.....	76
7.1.3 Analisi dei rischi digitali e dei possibili impatti.....	80
7.1.4 Auditing sulla sicurezza digitale.....	84

Rapporto OAD 2023

3

7.1.5 Certificazioni estese alle individuali sulla sicurezza digitale.....	86
7.2 Le misure tecniche di sicurezza digitale.....	88
7.2.1 Architetture per la sicurezza digitale.....	88
7.2.2 Misure tecniche di sicurezza fisica e perimetrale.....	91
7.2.3 Identificazione, autenticazione e autorizzazione degli utenti.....	95
7.2.4 Misure tecniche di sicurezza delle reti dei sistemi informativi.....	98
7.2.5 Misure di sicurezza delle applicazioni nei sistemi informativi.....	100
7.2.6 Misure tecniche di sicurezza digitale per la protezione dei dati.....	104
7.2.7 Misure e strumenti per la gestione ed il controllo della sicurezza digitale dei sistemi informativi.....	109
8. Contributo statistico della Polizia Postale e delle Comunicazioni all'indagine OAD 2023.....	120
PREMESSA.....	124
CENTRO NAZIONALE ANTICRIMINE INFORMATICO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE (C.N.A.I.P.I.C.) – COMPUTER CRIME – REATI CONTRO LA PERSONA ATTRAVERSO SOCIAL E RETE INTERNET.....	126
CENTRO NAZIONALE PER IL CONTRASTO DELLA PEDOPORNOGRAFIA ON-LINE (C.N.C.P.O.).....	126
IL COMMISSARIATO DI P.S. ONLINE.....	126
PREVENZIONE CYBERTERRORISMO.....	127
LE FRODI INFORMATICHE.....	127
LE TRUFFE ONLINE.....	127
REATI CONTRO LA PERSONA.....	128
Allegato A - Aspetti metodologici indagine OAD 2023.....	130
A.1 L'indagine OAD 2023.....	132
A.2 La tassonomia degli attacchi digitali per OAD 2023.....	133
A.2.1 Le classi di tecniche di attacco considerate (come si attacca).....	133
A.3 La macro valutazione qualitativa del livello di sicurezza digitale del sistema informatico oggetto delle risposte al questionario.....	136
ALLEGATO B - Glossario dei principali acronimi e termini tecnici.....	137
ALLEGATO C - Profilo SPONSOR GOLD.....	150
Qintesi.....	151
ALLEGATO D - Profilo Patrocinatori.....	154
ALLEGATO E - Riferimenti e fonti.....	159
E.1 Dall'OCI all'OAI e a OAD: un po' di storia.....	160
E.2 Le principali fonti sugli attacchi e sulle vulnerabilità.....	161
ALLEGATO F - AIPSI.....	162
ALLEGATO G - Profilo dell'autore Marco R. A. Bozzetti.....	165
ALLEGATO H - MALABO Srl.....	167

Rapporto OAD 2023

4

Misure sicurezza da OAD 2023



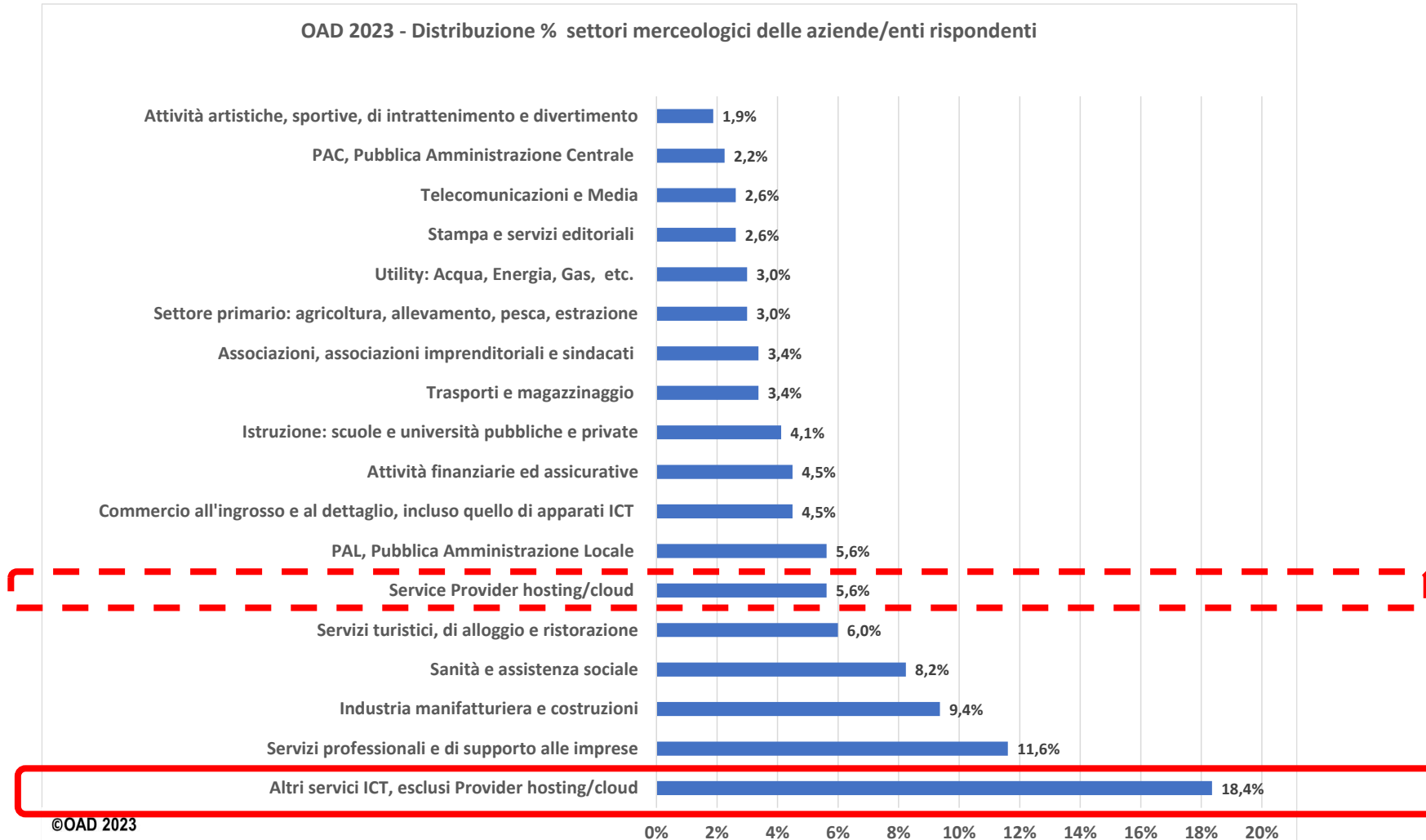
8

Allegati

# Dall'indagine OAD 2023

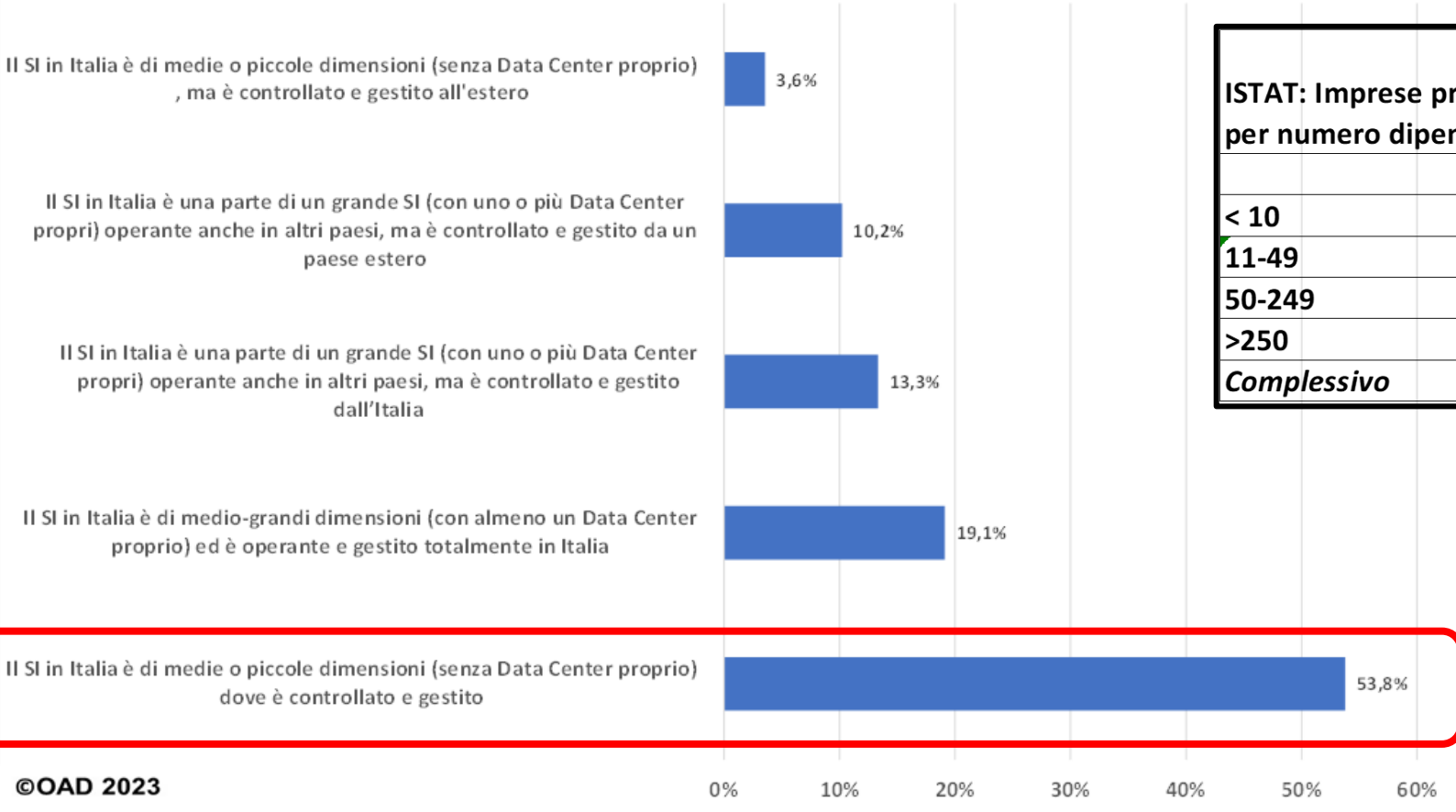


# Settore merceologico delle aziende/enti rispondenti



# I Sistemi Informativi (SI) dei rispondenti

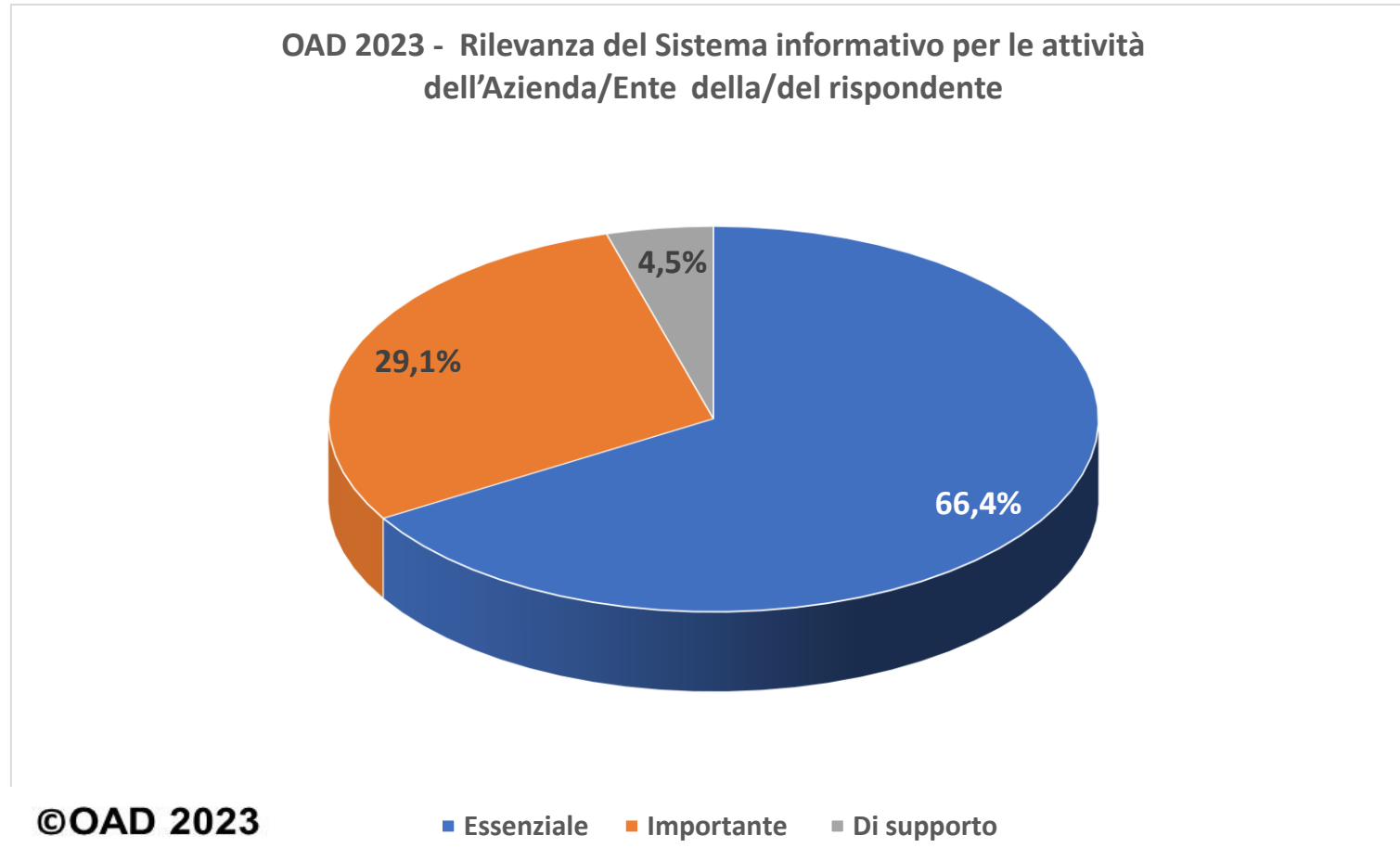
OAD 2023 - Macro tipologia del Sistema informativo (SI) nell'area Italianadell'azienda/ente rispondente



ISTAT: Imprese private per numero dipendenti	ISTAT Numero imprese	% sul totale ISTAT
< 10	4.149.572	<b>94,80%</b>
11-49	199.340	<b>4,55%</b>
50-249	24.288	<b>0,55%</b>
>250	4.179	<b>0,10%</b>
<b>Complessivo</b>	<b>4.377.379</b>	<b>100%</b>

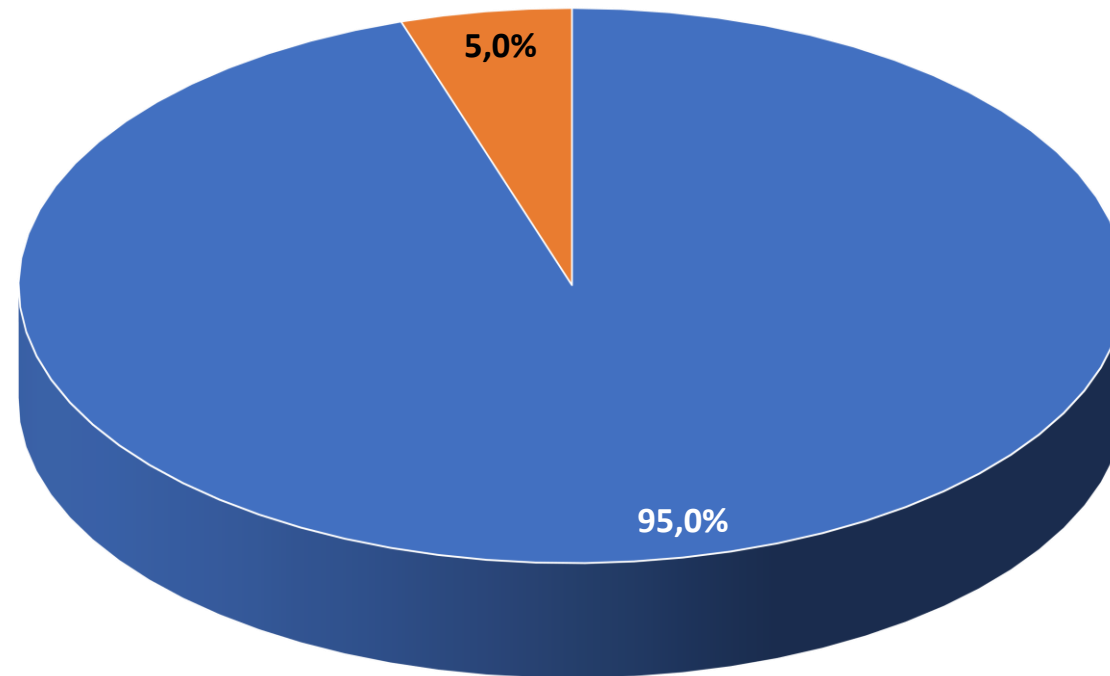
CLASSI DI DIPENDENTI	Istituzioni per numero dipendenti	%
da 0 a 9	6.383	47,6
da 10 a 49	4.595	34,3
da 50 a 249	1.751	13,1
da 250 a 999	362	2,7
da 1,000 a 24,999	306	2,3
25,000 e oltre	9	0,1
<b>Totale</b>	<b>13.406</b>	<b>100,0</b>

# Importanza del SI per l'azienda/ente rispondente



# SI aziende/enti rispondenti: ibridi = on premise + multi-cloud

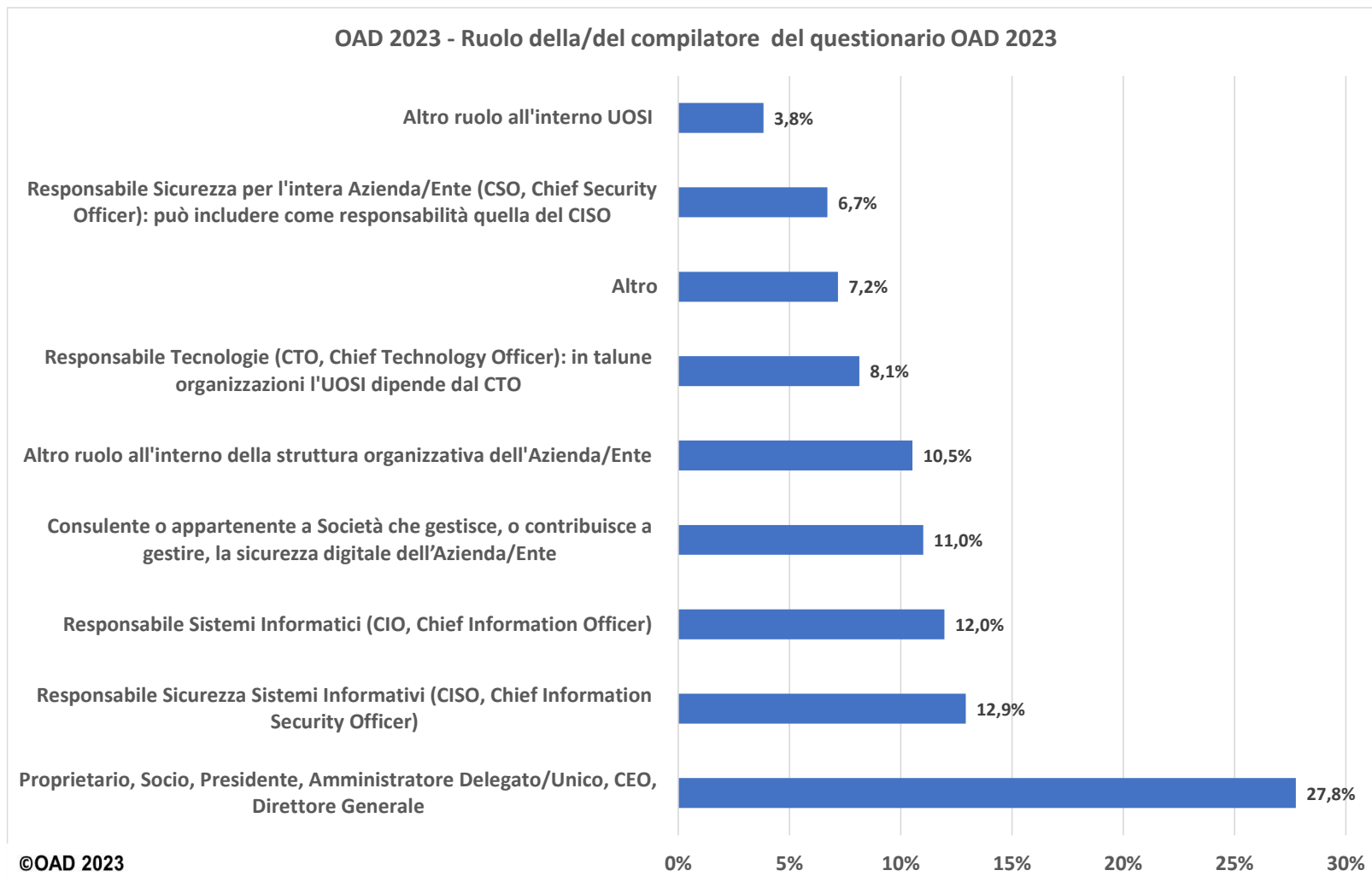
OAD 2023 - Utilizzo di sistemi/servizi terziarizzati nel Sistema Informativo oggetto delle  
risposte al questionario



©OAD 2023

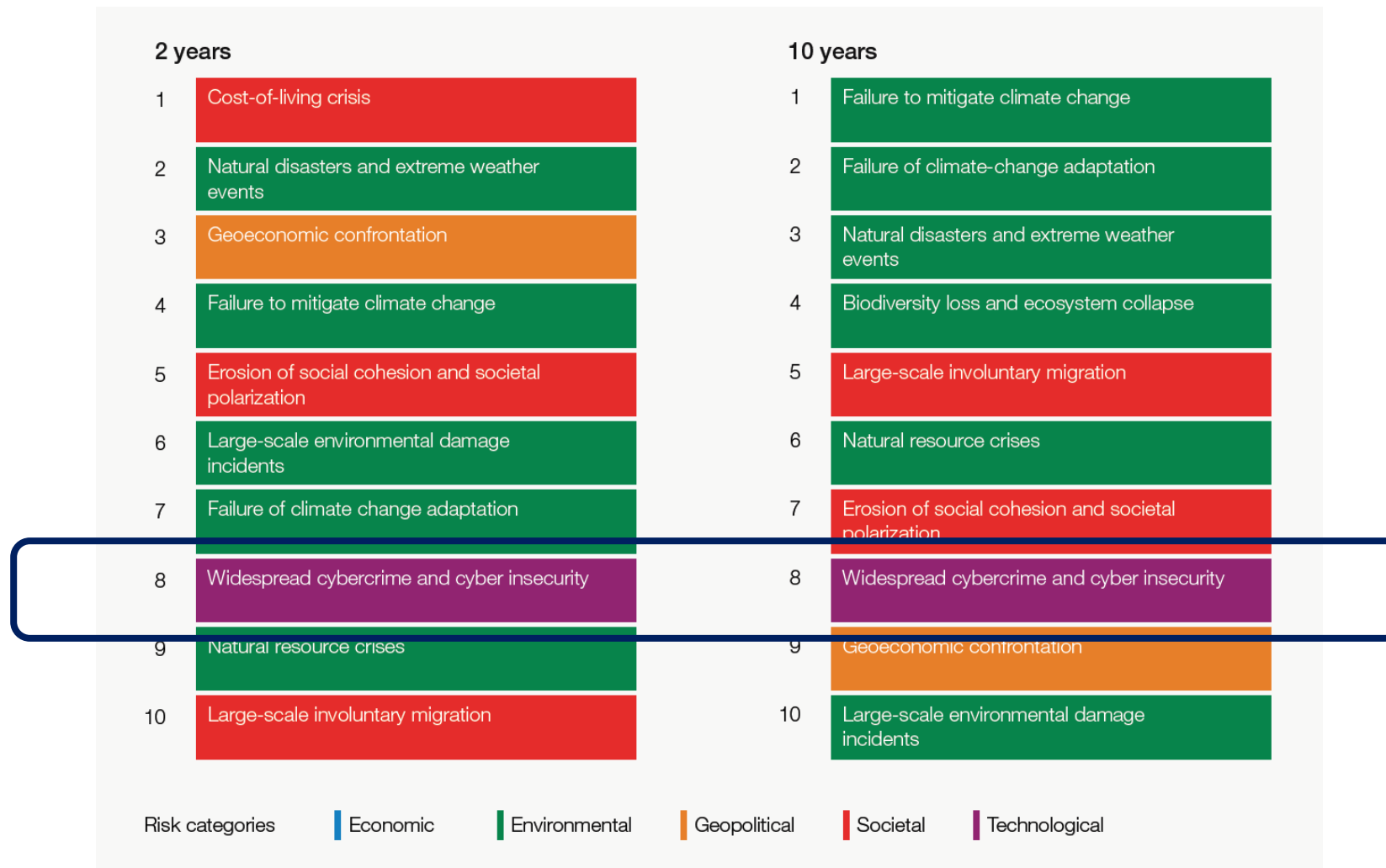
■ SI ■ NO

# Ruolo della/del rispondente al questionario OAD 2023



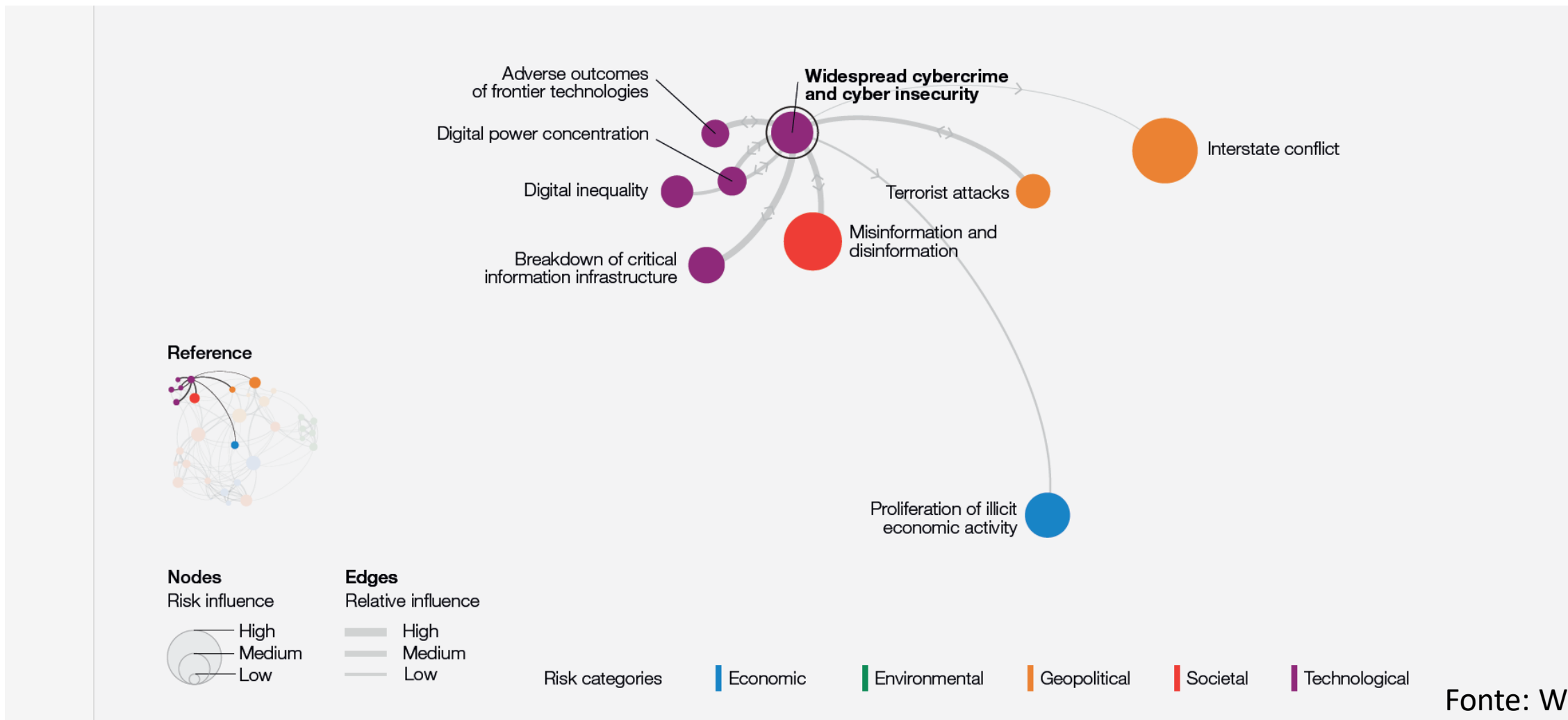


# I 10 principali rischi a 2 e 10 anni a livello mondiale



Fonte: WEF

# L'interconnessione dei rischi cyber



# I 10 principali rischi cyber al 2030 secondo Enisa

## TOP 10 EMERGING CYBER- SECURITY THREATS FOR 2030



**Rischi ibridi: rischi cyber sofisticati ed associati a rischi fisici o offline**

# Le vulnerabilità tecniche dei prodotti ICT dal CVE Mitre



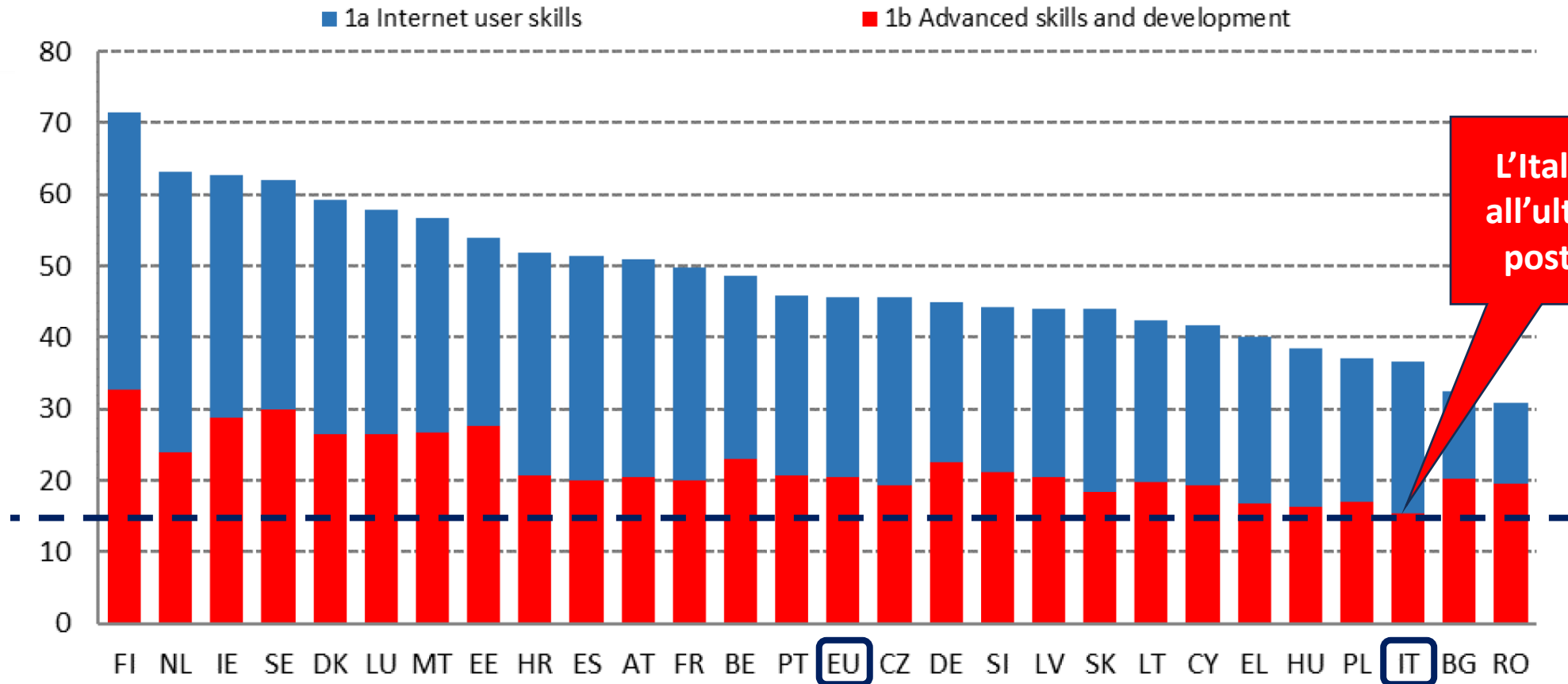
Gli attacchi digitali sono causati da vulnerabilità:

- Tecniche
- Personali
- Organizzative

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

Fonte: CVE

# DESI 2022: competenze ICT di base e avanzate



20

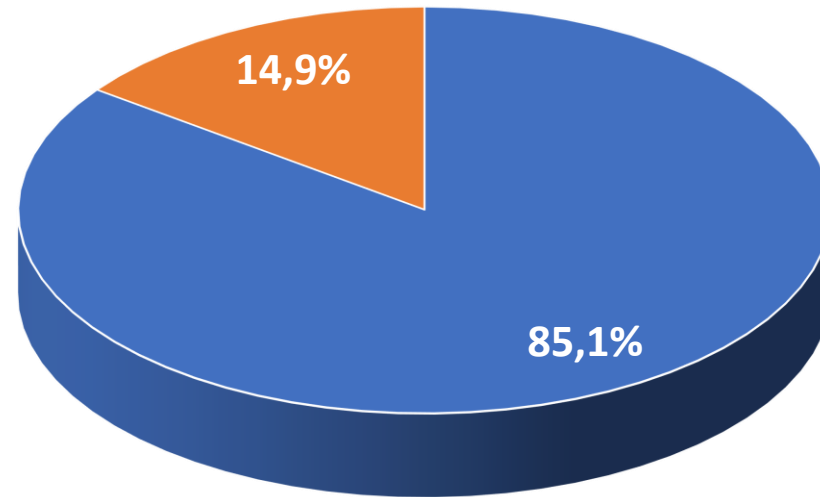
L'Italia è all'ultimo posto!!

# Situazione a livello mondiale attacchi digitali

- **Forte incremento nel 2022 anche a causa**
  - Il prolungarsi della pandemia Covid
  - Crescita tensioni geopolitiche
  - Invasione Ucraina
  - *Trend confermato anche per l'Italia dall'indagine OAD*
- **Tale trend continua nel 2023 e oltre**
  - Attacco terroristico Hamas 7/10/2023 e risposta israeliana
  - Ulteriore crescita tensioni geopolitiche

# OAD 2023: gli attacchi digitali rilevati dai rispondenti

OAD 2023 - % Sistemi Informativi delle/dei rispondenti  
che nel 2022 hanno o non rilevato attacchi digitali



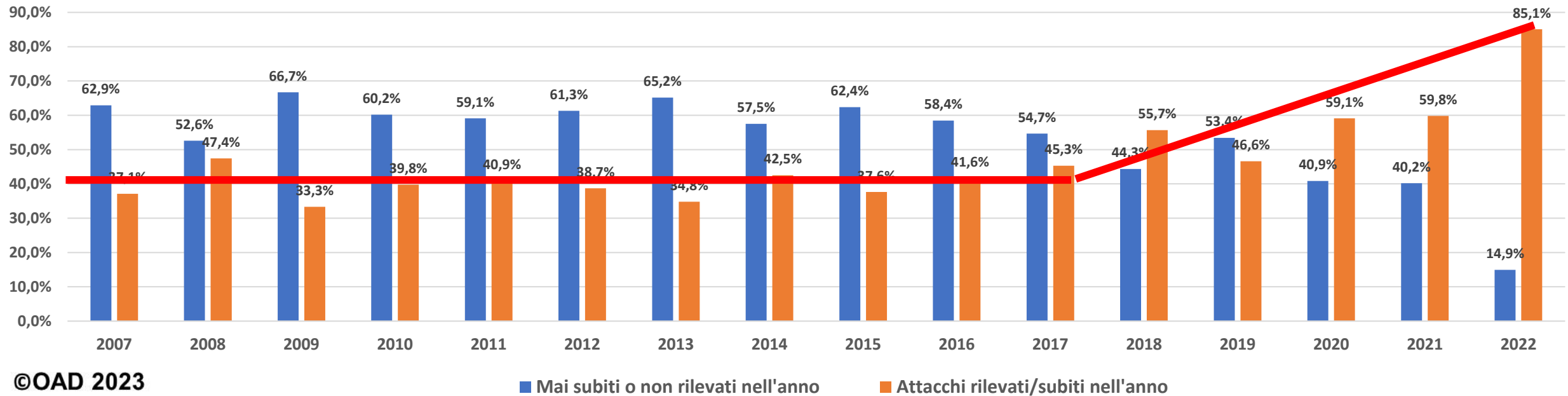
©OAD 2023

■ Rilevato attacchi

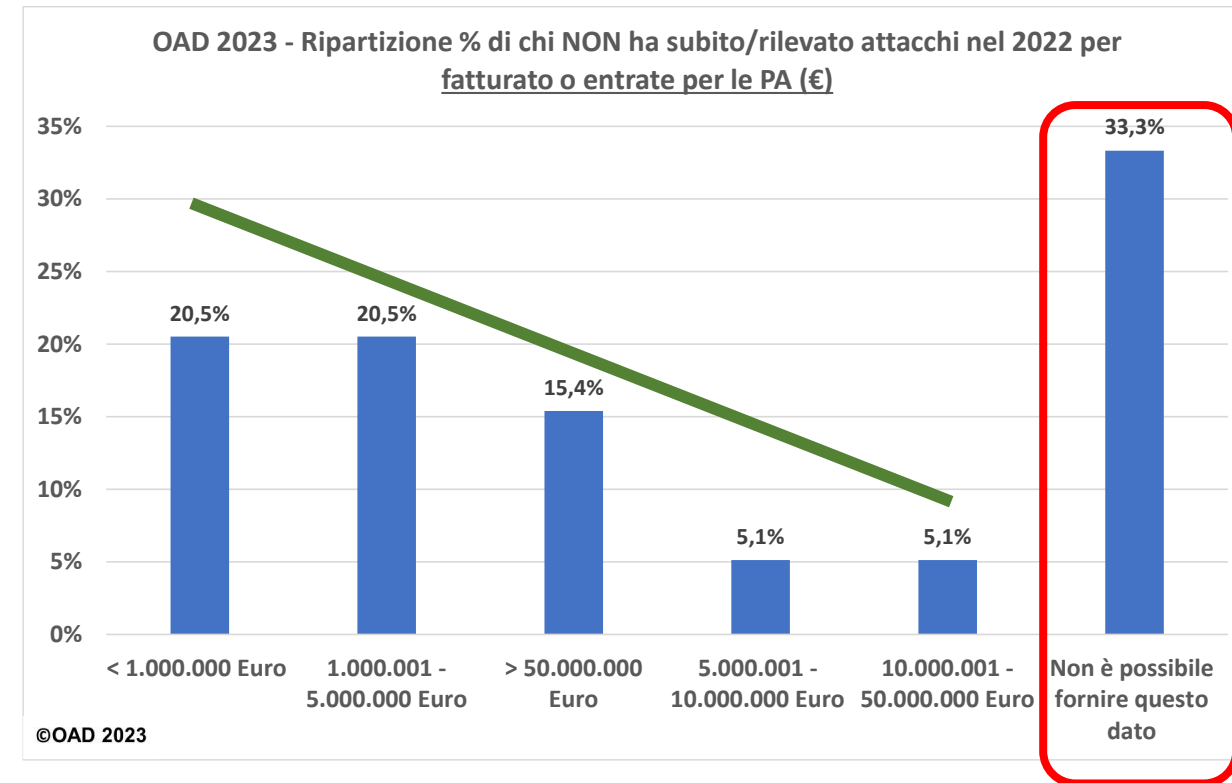
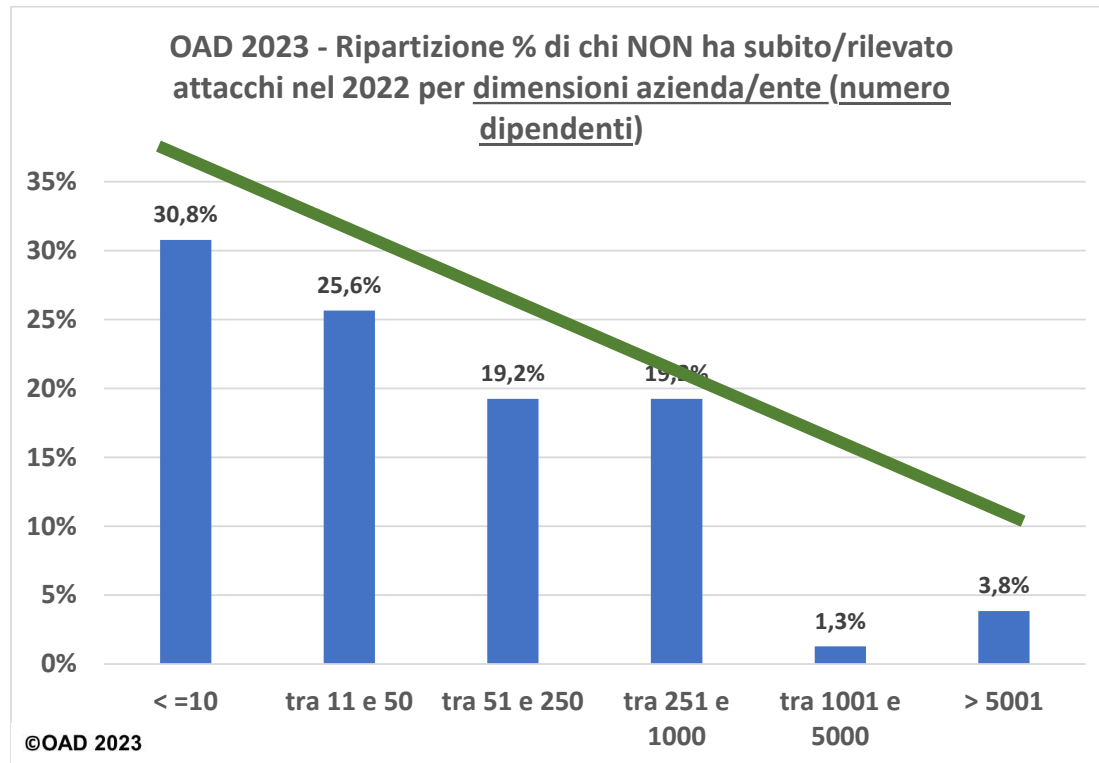
■ Non rilevato attacchi

# Forte aumento attacchi digitali intenzionali come trend dai rispondenti indagini OAD 2007-2022

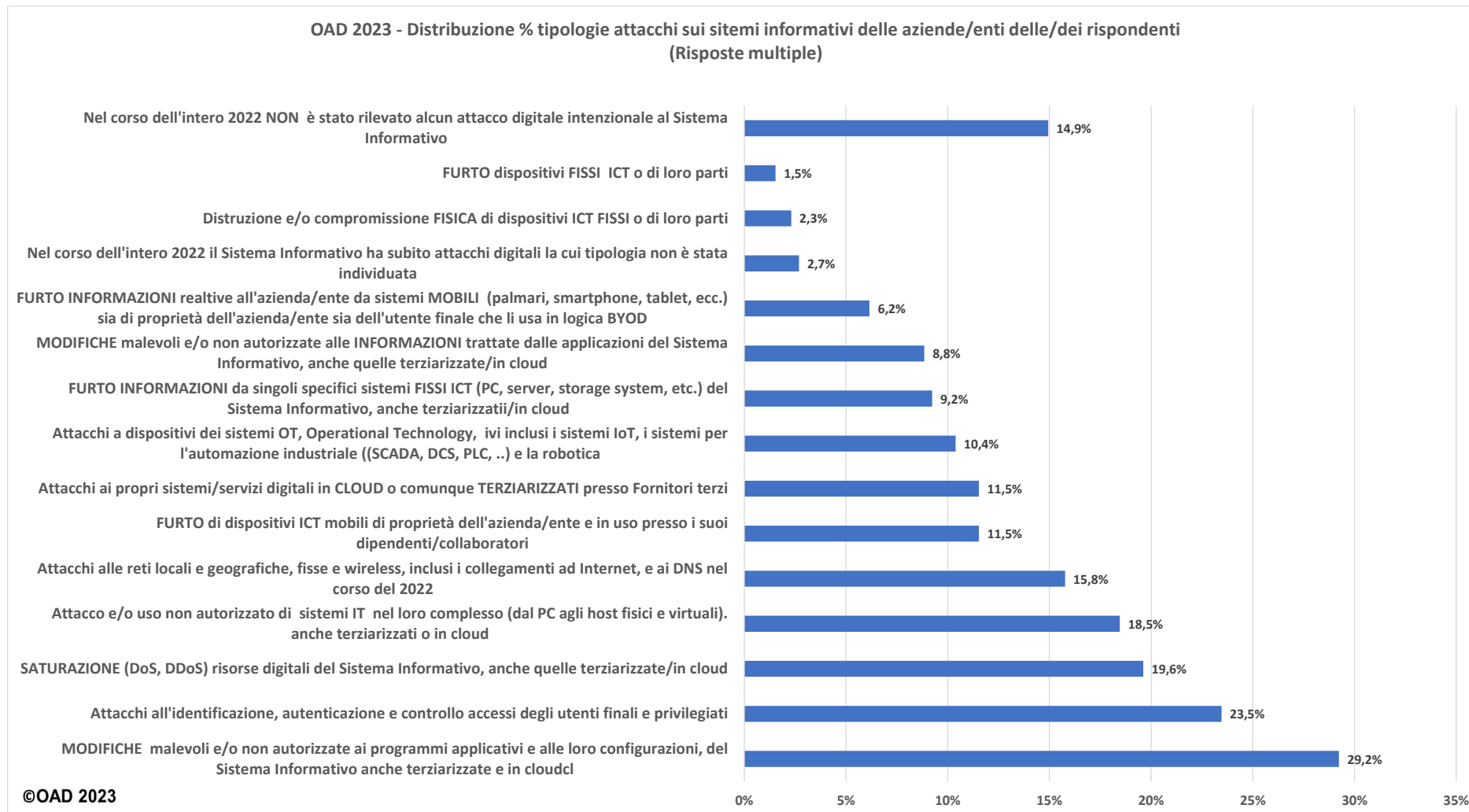
OAD 2023 - Confronto attacchi digitali rilevati o non nelle varie indagini OAD dal 2007 al 2022  
(NB: il confronto tra i vari anni non ha validità statistica ma di trend)



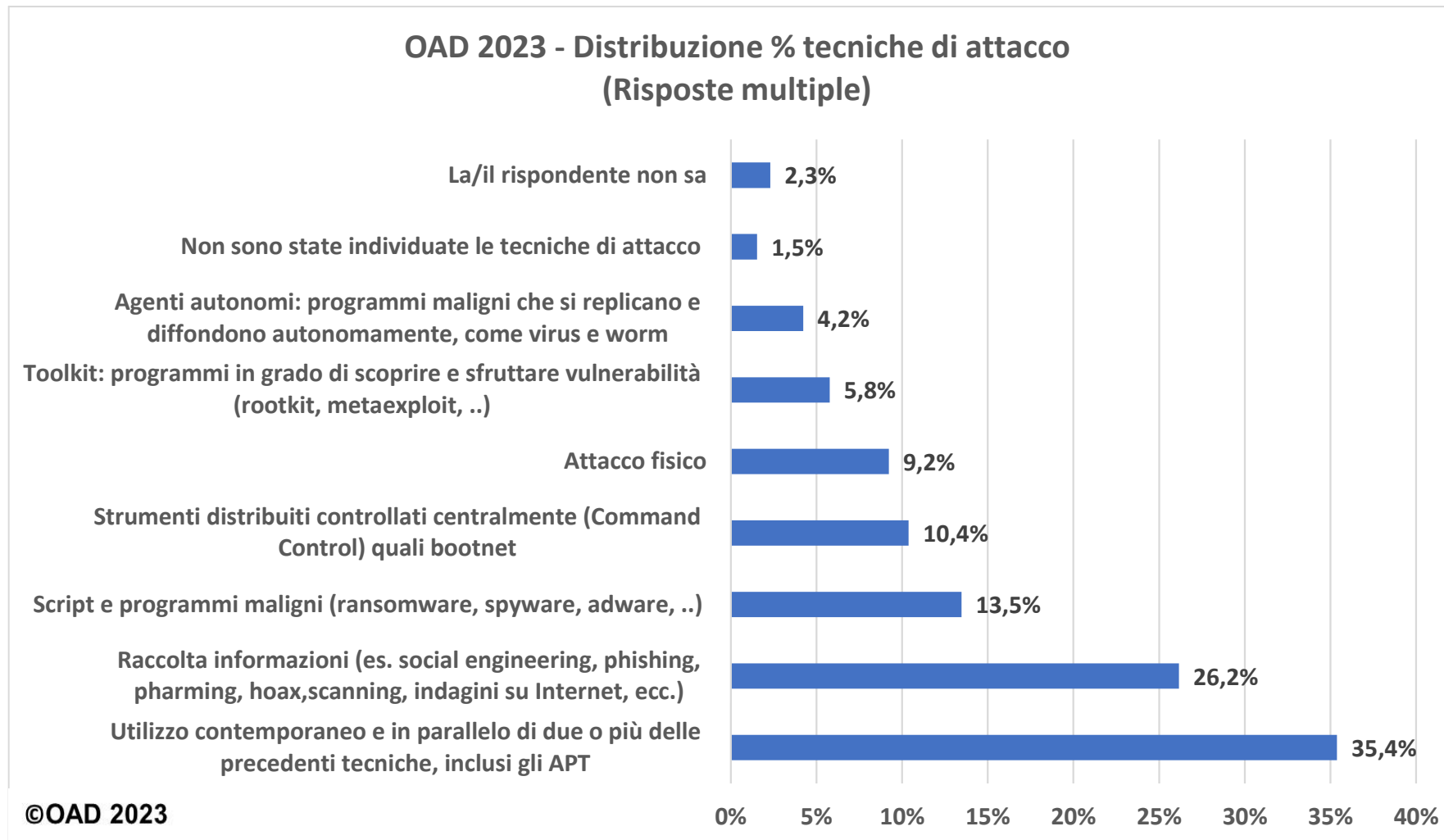
# Attacchi digitali prevalenti alle organizzazioni più grandi e più ricche



# Distribuzione % tipologia attacchi digitali



# Distribuzione % tecniche di attacco digitale

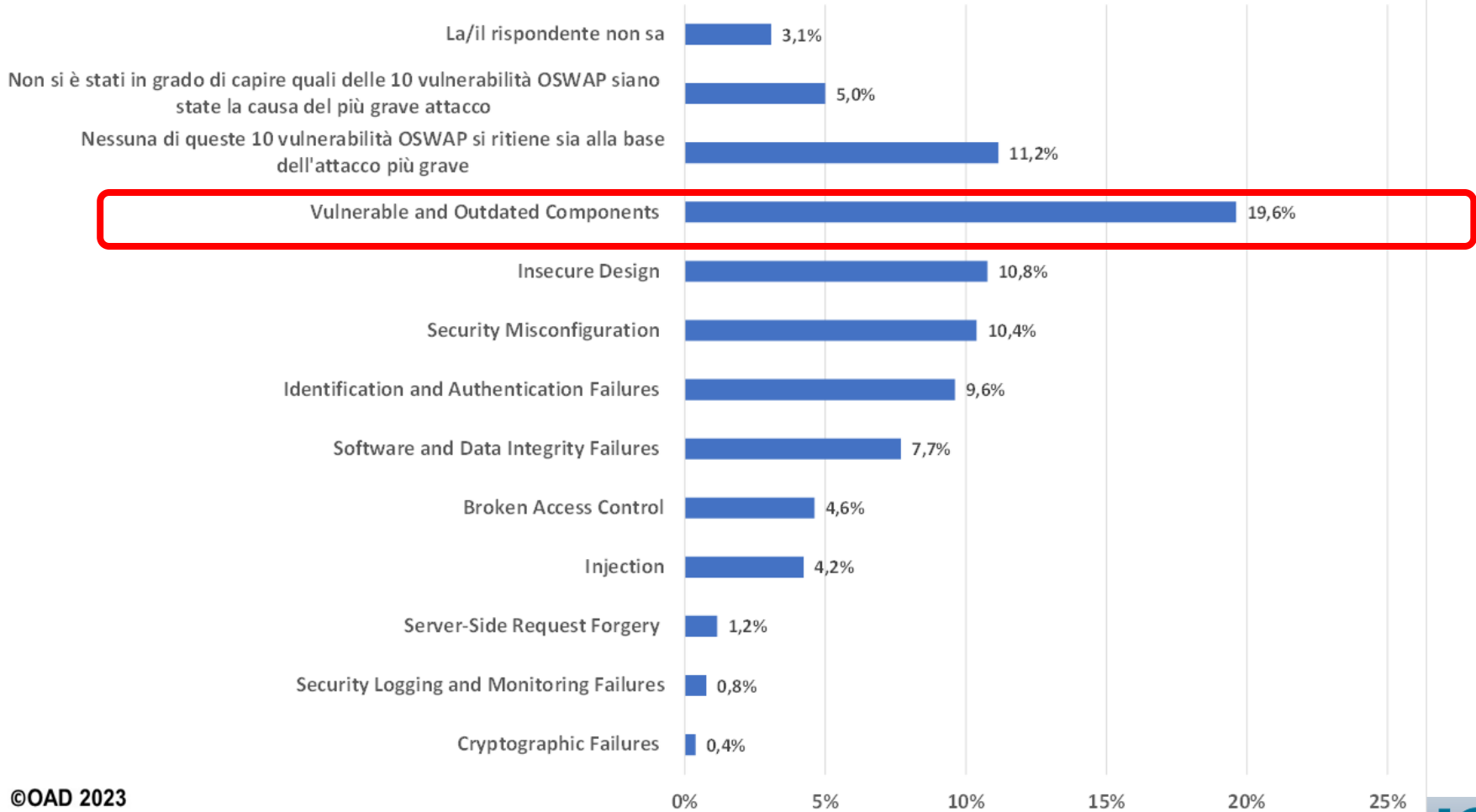


# Le top 10 vulnerabilità OSWAP nel 2022

<i>Nome vulnerabilità</i>	<i>Breve spiegazione</i>
<b>Broken Access Control</b>	Per superare in maniera non autorizzata, e quindi illegale, il controllo dell'accesso alle applicazioni e ai dati da queste trattate.
<b>Cryptographic Failures</b>	Errori/caduta/superamento delle tecniche crittografiche
<b>Injection</b>	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
<b>Insecure Design</b>	Progettazione non sicura
<b>Security Misconfiguration</b>	Cattiva o incompleta configurazione dei sistemi e degli strumenti di sicurezza
<b>Vulnerable and Outdated Components</b>	Componenti non aggiornati e quindi vulnerabili
<b>Identification and Authentication Failures</b>	Errori/caduta/superamento delle misure di identificazione ed autenticazione
<b>Software and Data Integrity Failures</b>	errori e malfunzionamenti del software e dell'integrità dei dati trattati.
<b>Security Logging and Monitoring Failures</b>	Errori, malfunzionamento e caduta degli strumenti di monitoraggio e di logging
<b>Server-Side Request Forgery</b>	Falsificazione di richieste lato server

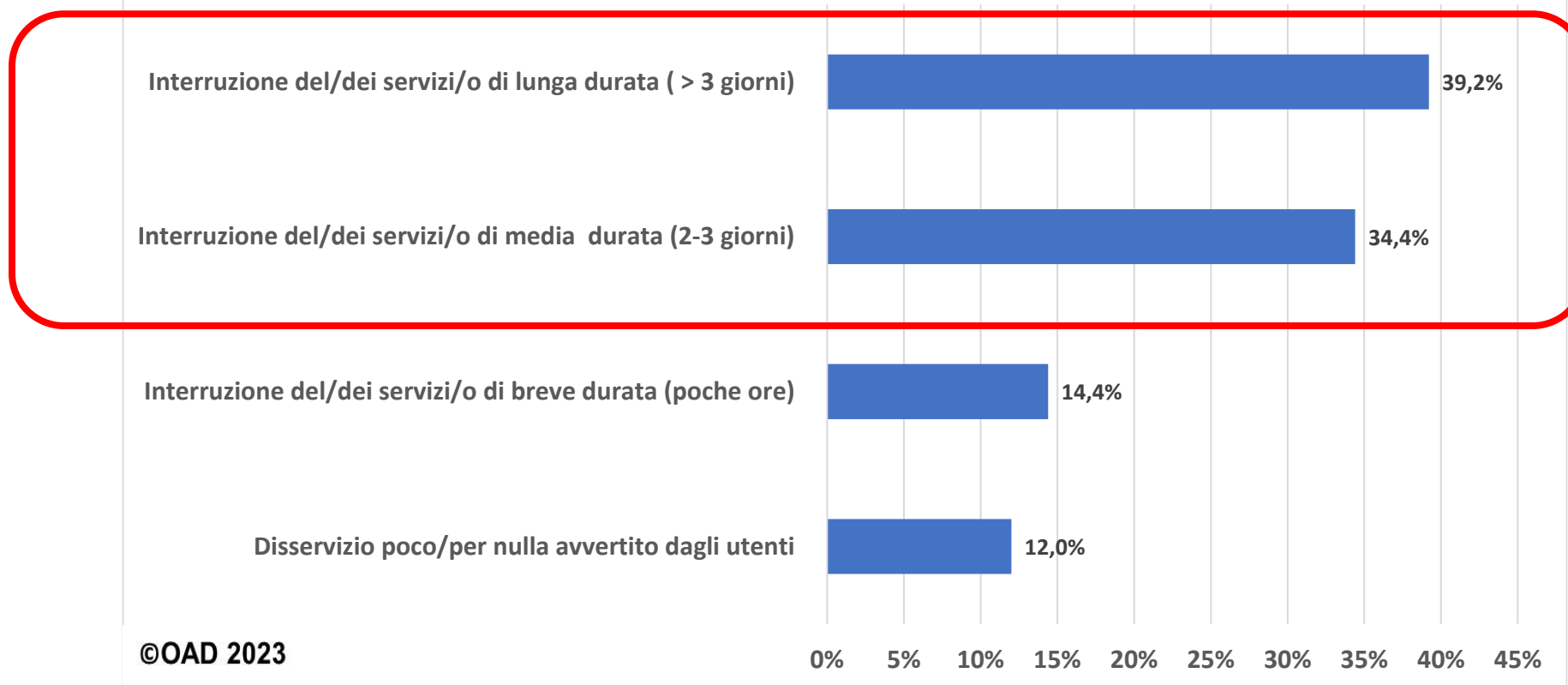
# Attacchi agli ambienti web causati dalle top 10 vulnerabilità

OAD 2023 - Distribuzione % delle probabili 10 principali vulnerabilità OWSAP per l'attacco più grave (Risposte multiple)

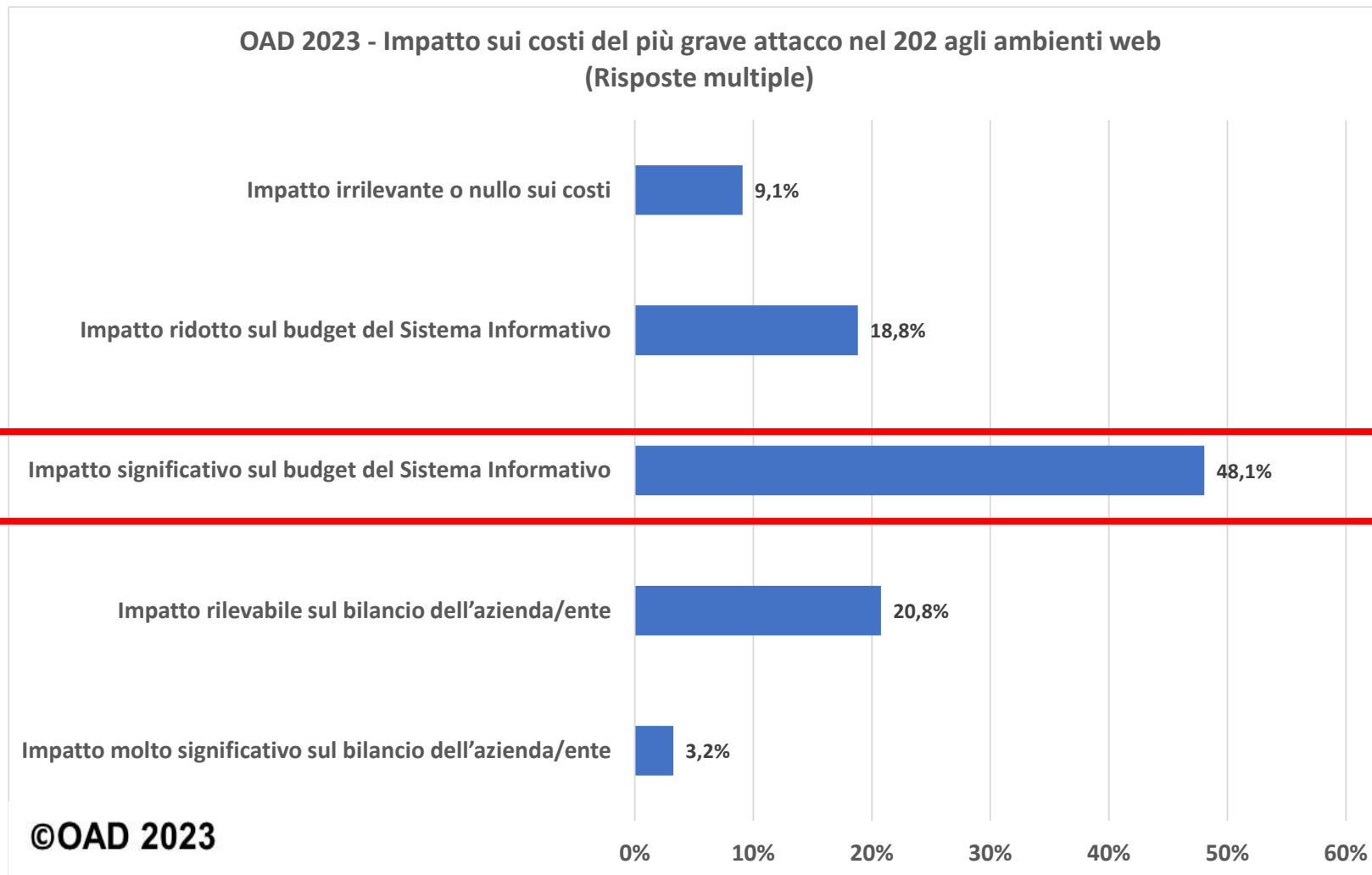


# Impatti tecnici dall'attacco più grave ai web nel 2022

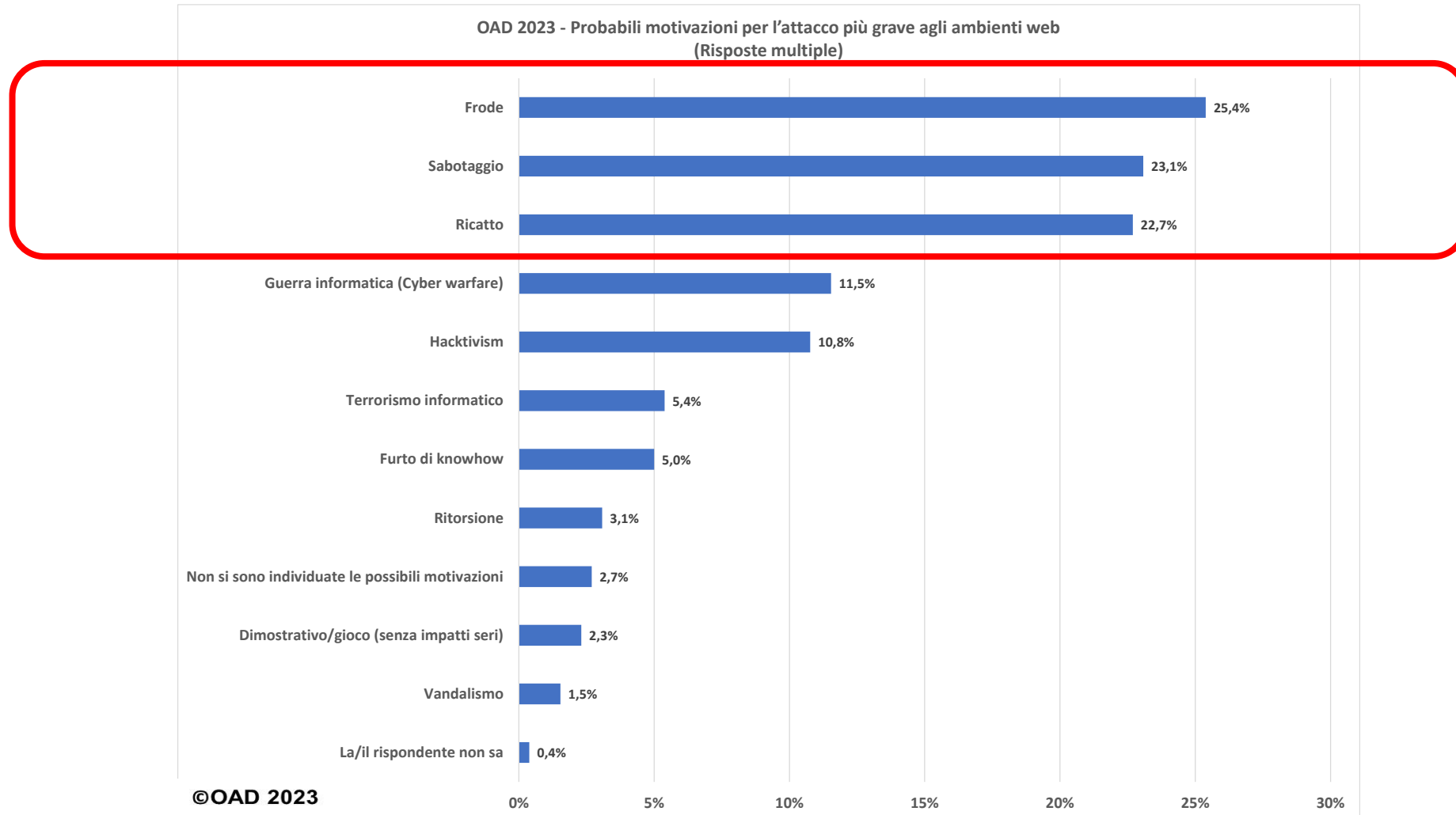
OAD 2023 - Impatto sull'erogazione dei servizi dall'attacco più grave agli ambienti web rilevato nel 2022



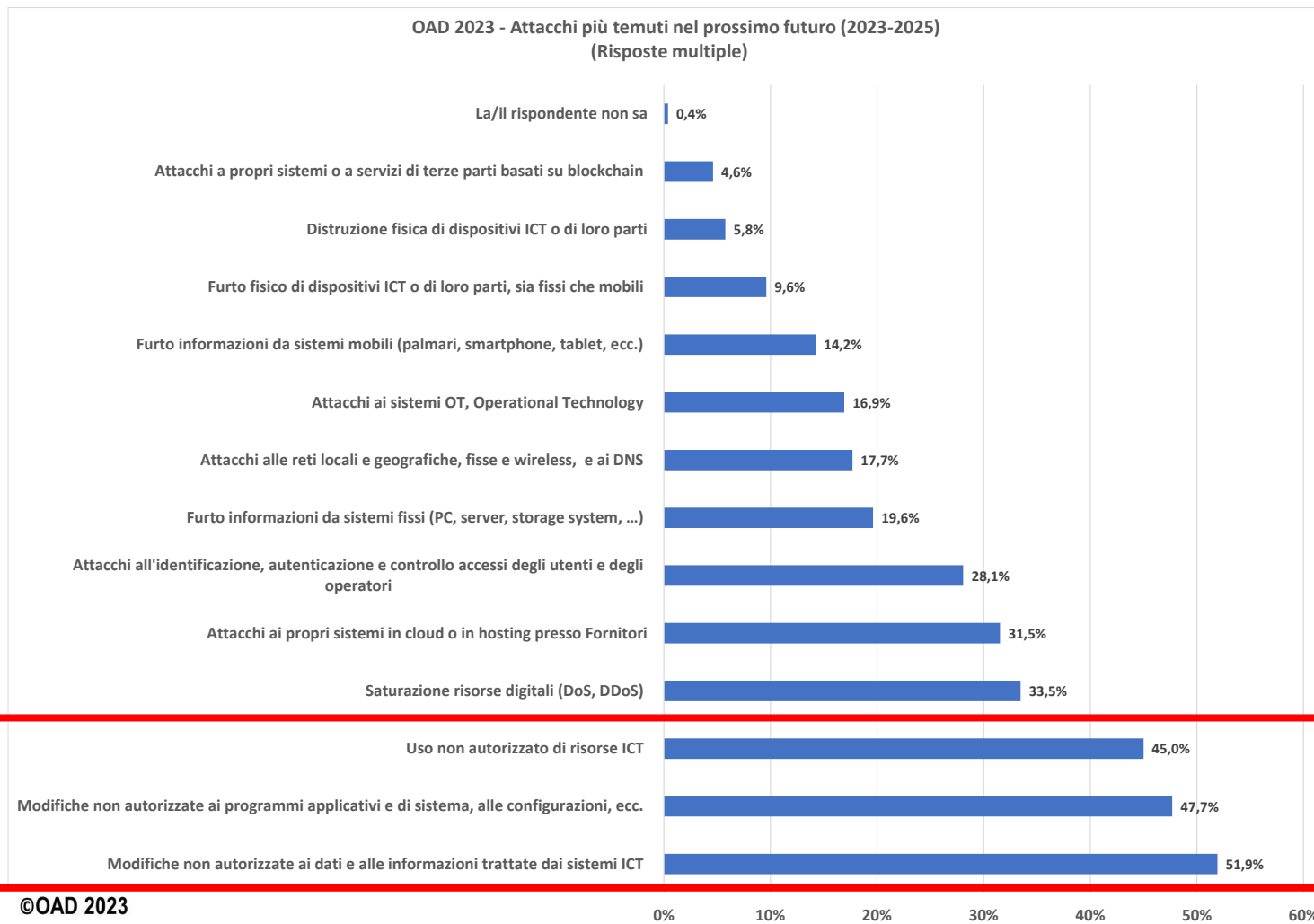
# Impatti economici dall'attacco più grave ai web nel 2022



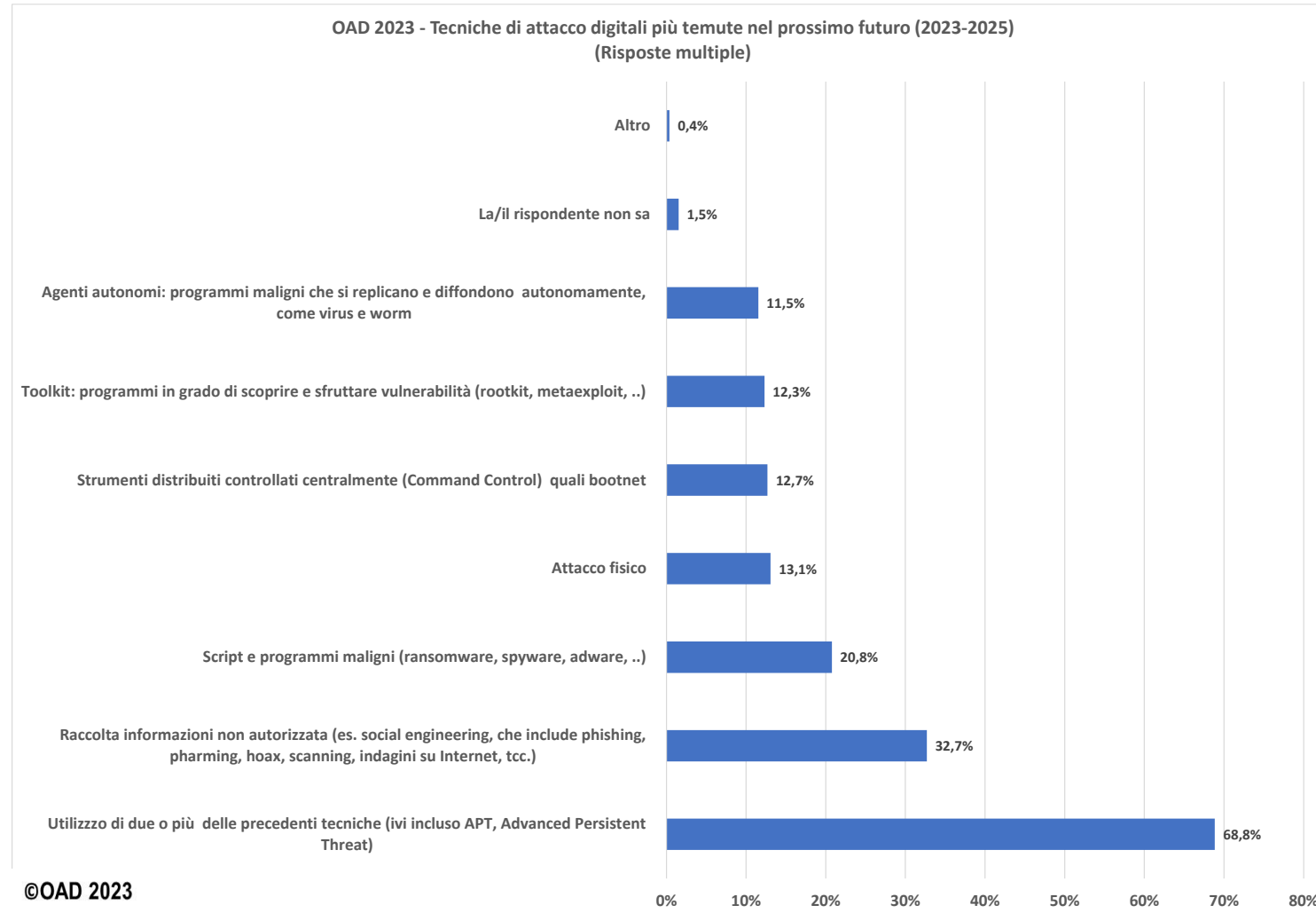
# Probabili motivazioni attacco più grave ai web nel 2022



# Tipologie attacchi più temuti nel prossimo futuro



# Tecniche di attacco più temute nel prossimo futuro





# I dati della Polizia Postale e delle Telecomunicazioni

## Infrastrutture critiche (C.N.A.I.P.I.C.)

Protezione strutture critiche	1 gen - 31 dic 2022	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen - 31 dic 2018	1 gen - 31 dic 2017	1 gen - 31 dic 2016
Attacchi rilevati	13.099	282	509	1181	459	1.032	844
Alert diramati	113.420	24.824	83.416	82.484	80.777	31.524	6.721
Indagini avviate	110	34	103	155	74	72	70
Persone arrestate	n.d.	n.d.	n.d.	3	1	3	3
Persone denunciate/indagate	334	n.d.	105	117	14	1.316	1.226
Perquisizioni	n.d.	n.d.	n.d.	n.d.	n.d.	73	58
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	77	17	69	79	108	83	85

34

## Cyber terrorismo

Cyber Terrorismo	1 gen - 31 dic 2022	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen - 31 dic 2018
Spazi web monitorati	175.572	11.962	37.081	36.377	36.000

## Frodi informatiche

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

## Truffe online

	1 gen - 31 dic 2022
Casi trattati	15.699
Persone indagate	3.570
Somme sottratte	€ 116.454.550

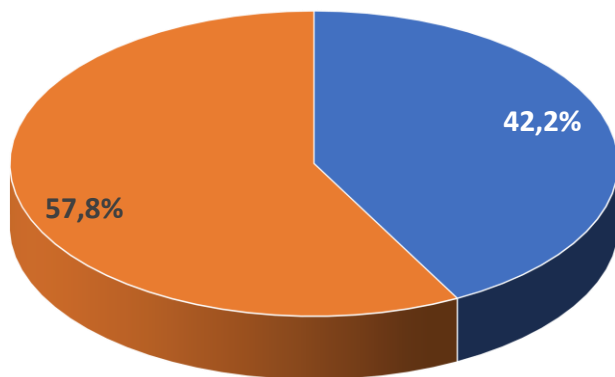
# MISURE DI SICUREZZA DIGITALE

Considerazioni su quanto emerso  
dall'indagine OAD 2023

35

# Quanti hanno risposto e di che settore merceologico

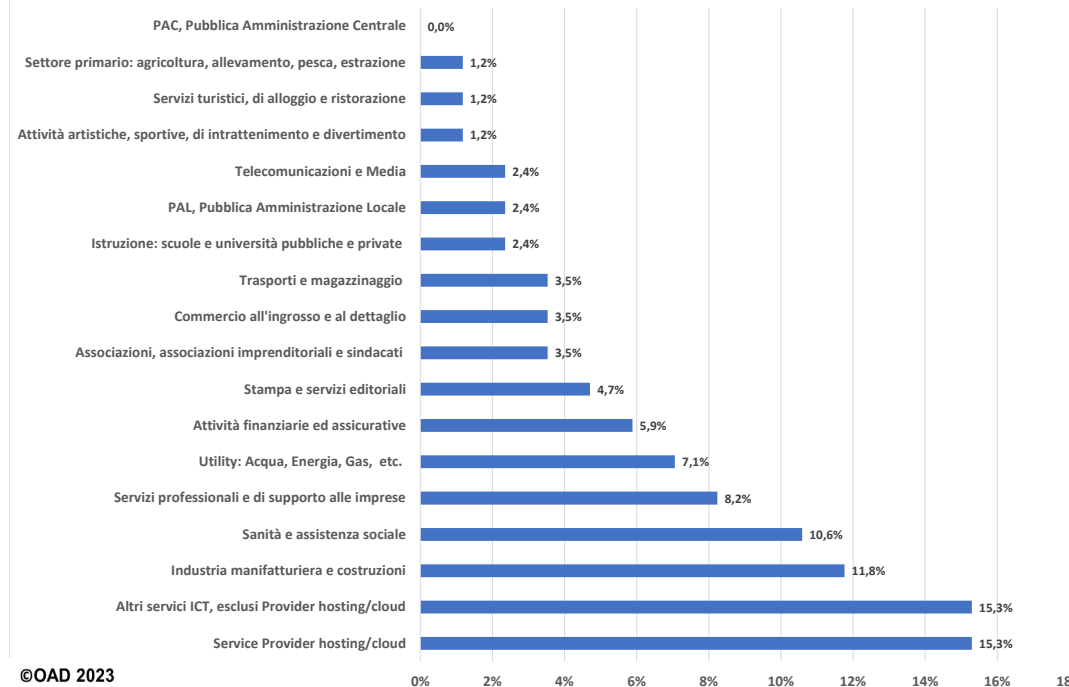
OAD 2023 - % di quanti hanno risposto, o non, alle domande opzionali sulle misure di sicurezza digitale in essere nel sistema informativo della loro azienda/ente



©OAD 2023

■ Hanno risposto ■ NON hanno risposto

OAD 2023 - Ripartizione % per settore merceologico di chi ha risposto alle domande sulle misure di sicurezza digitale



©OAD 2023

# Misure tecniche ed organizzative per la sicurezza digitale considerate in OAD 2023

## Le classi di misure tecniche in OAD 2023

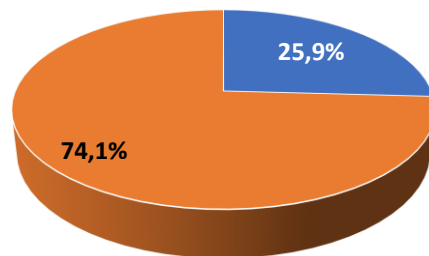
- Architettura complessiva delle misure della sicurezza digitale, integrata con l'intera architettura del sistema informatico
- Contromisure fisiche
- Misure di Identificazione, Autenticazione, Autorizzazione (IAA)
- Contromisure tecniche sicurezza digitale a livello di reti locali e geografiche
- Contromisure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

## Le classi di misure organizzative in OAD 2023

- Struttura organizzativa per la sicurezza digitale (CISO)
- Policy e procedure organizzative per la sicurezza digitale
- Analisi dei rischi digitali e dei possibili impatti
- Auditing sulla sicurezza digitale
- Certificazioni aziendali e individuali sulla sicurezza digitale

# Misure organizzative: dati più significativi emersi (1)

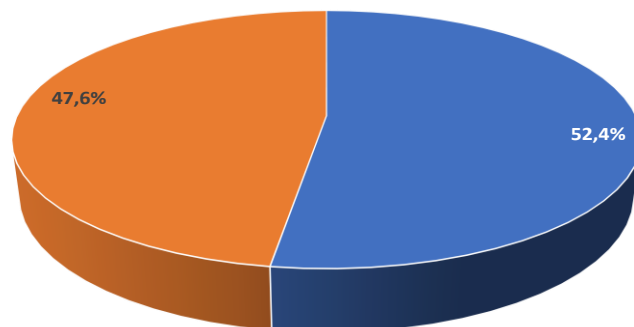
OAD 2023 - Attuazione della struttura organizzativa per la sicurezza digitale nelle aziende/enti rispondenti



©OAD 2023

■ NO ■ SI

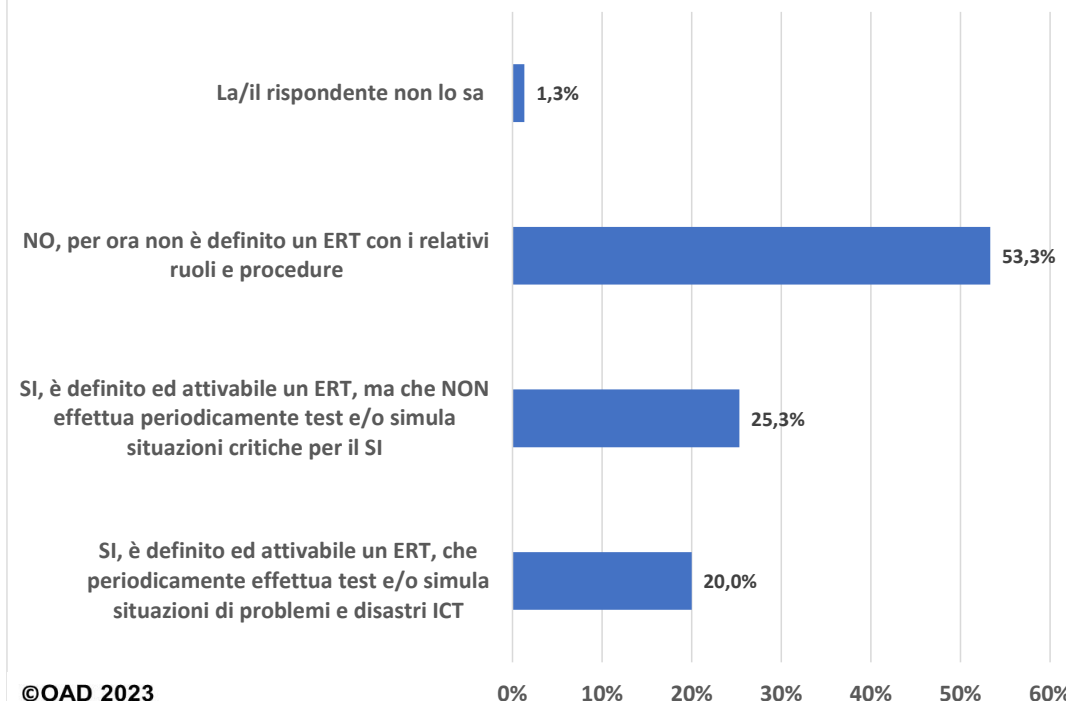
OAD 2023 - Da chi dipende il CISO e la sua struttura nelle aziende/enti che l'hanno attuata



©OAD 2023

■ Alla/al responsabile dell'intero Sistema Informativo (CIO)  
 ■ Ad altre strutture organizzative dell'azienda/ente rispondente

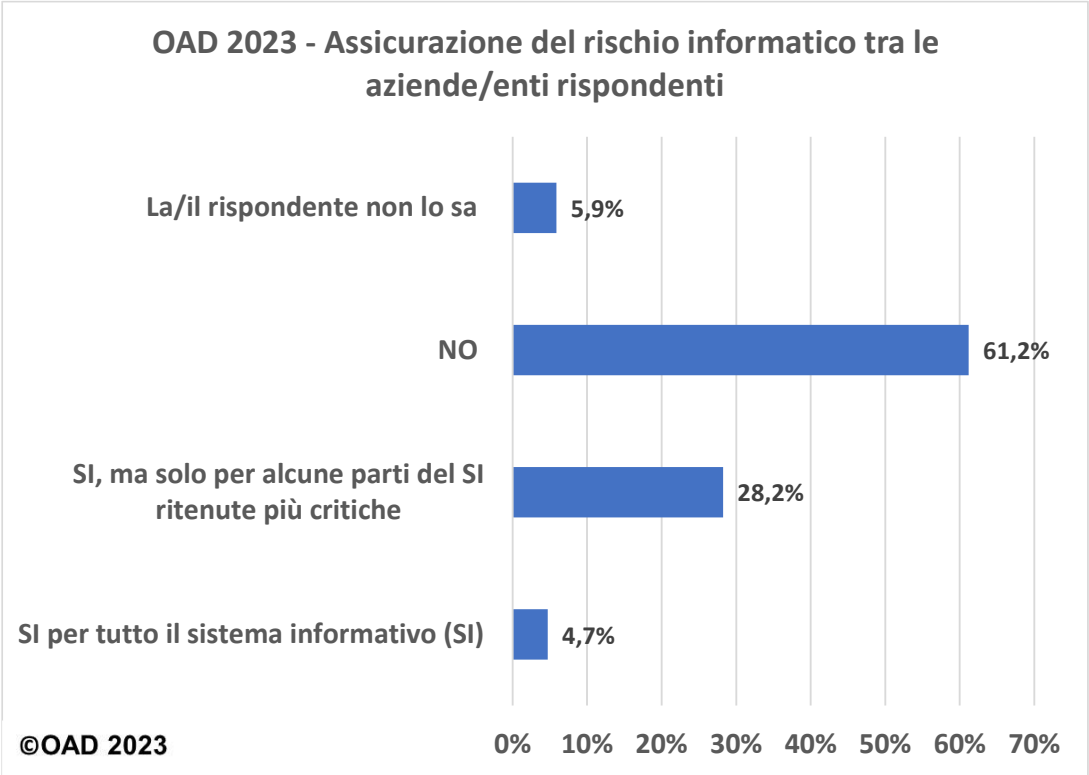
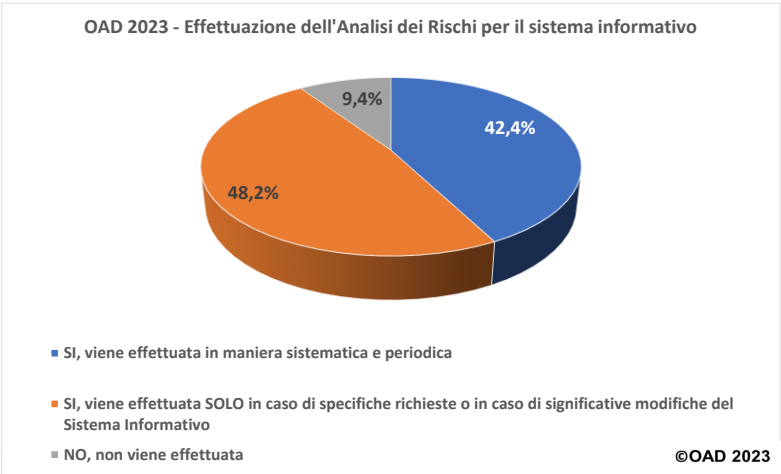
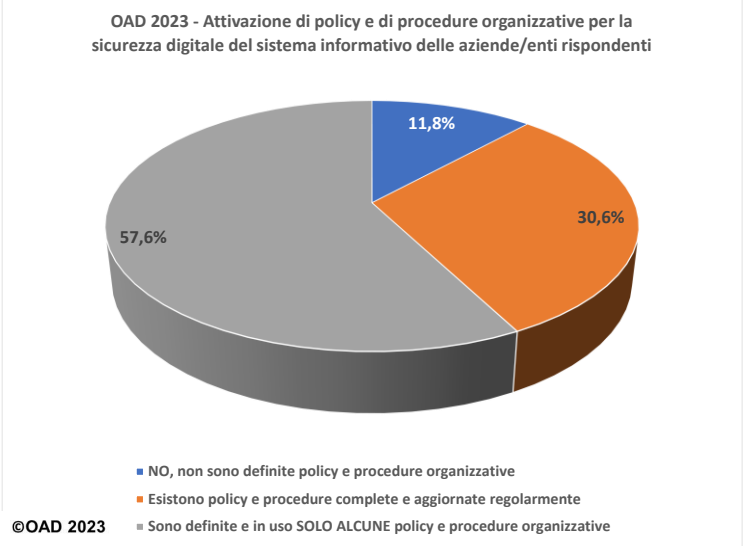
OAD 2023 - Esistenza ERT con la definizione dei relativi ruoli e procedure



©OAD 2023

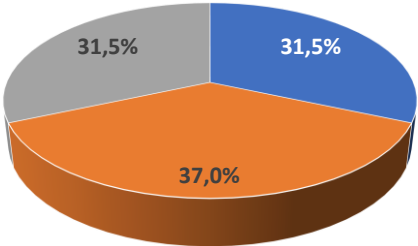
0% 10% 20% 30% 40% 50% 60%

# Misure organizzative: dati più significativi emersi (2)



# Misure tecniche: dati più significativi emersi (1)

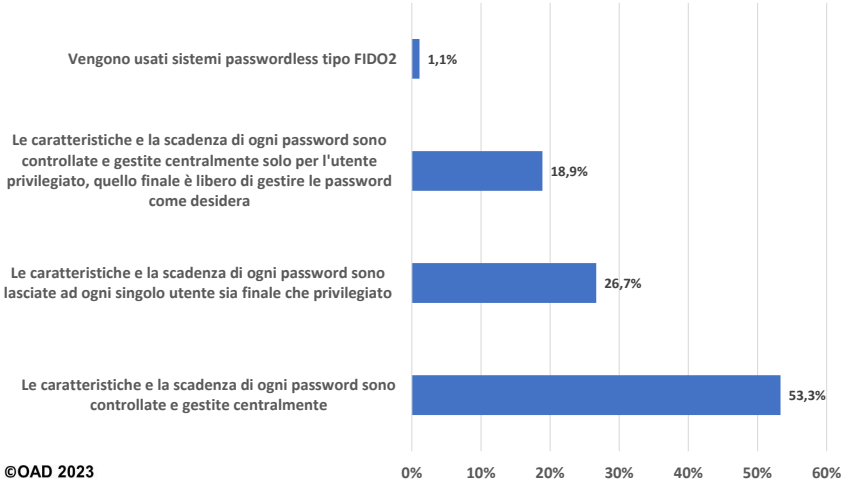
OAD 2023 - Definizione ed implementazione di una architettura per la sicurezza digitale nel sistema informativo dell'azienda/ente rispondente



- NO, non è definita un'architettura per la sicurezza digitale
- SI, è definita, ma solo per le parti più critiche del Sistema Informativo
- SI, è definita per l'intero Sistema Informativo

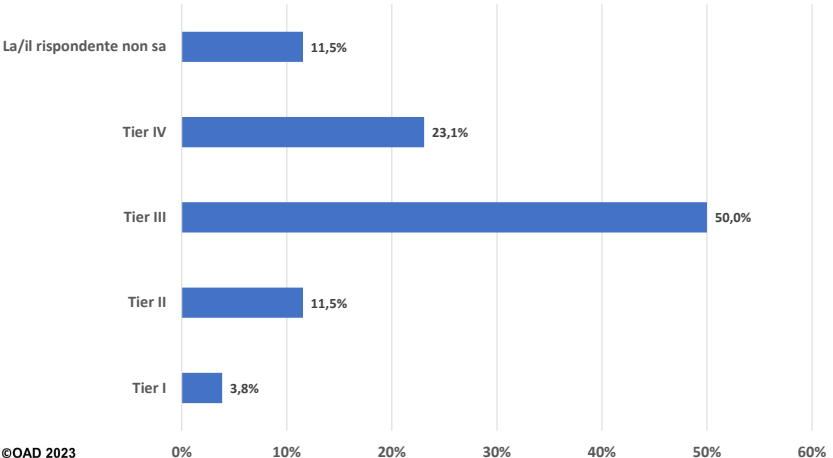
©OAD 2023

OAD 2023 - Controllo e gestione delle password dell'utenza nei sistemi informativi delle aziende/enti rispondenti



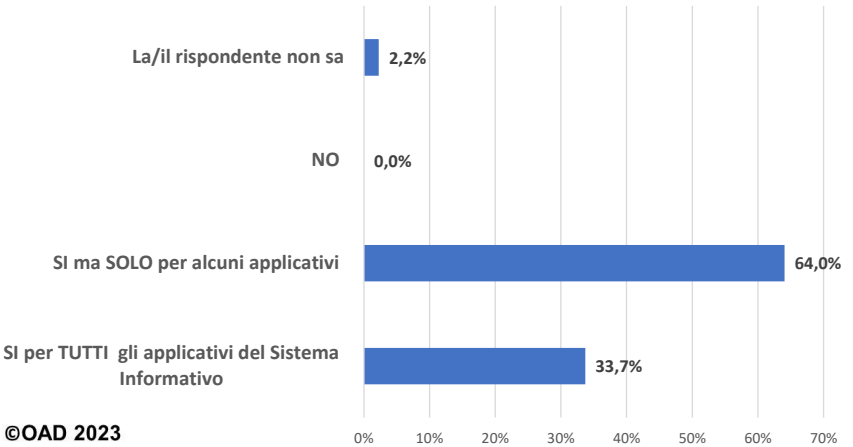
©OAD 2023

OAD 2023 - Livello di affidabilità del principale Data Center in Italia dei sistemi informativi delle aziende/enti rispondenti secondo lo standard ANSI/TIA 942



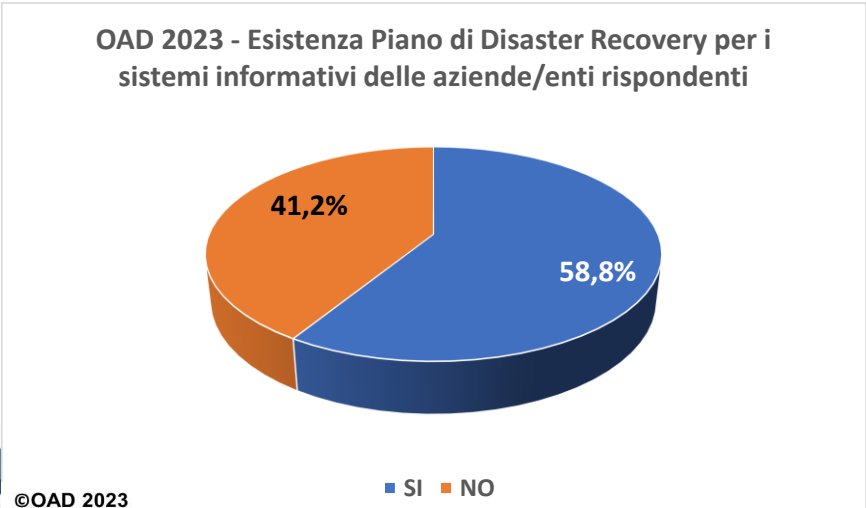
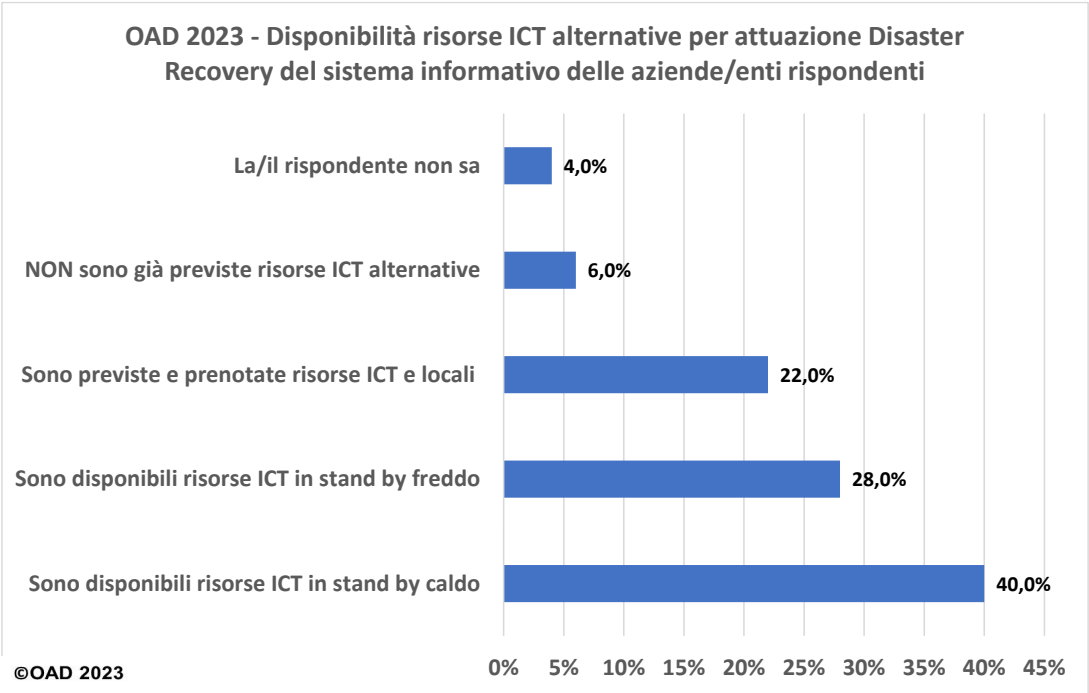
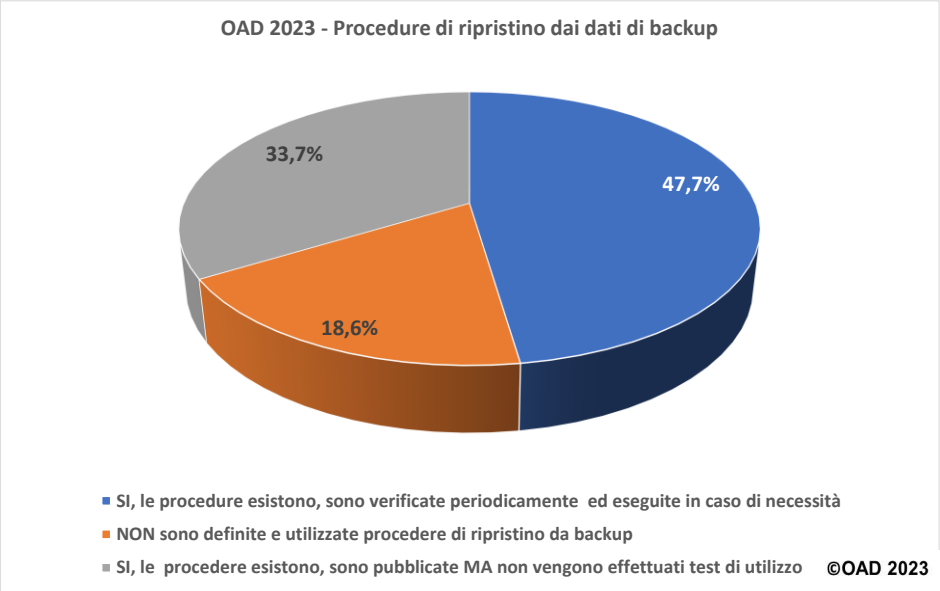
©OAD 2023

OAD 2023 - Controllo degli accessi e delle autorizzazioni agli applicativi dei sistemi informativi delle aziende/enti rispondenti



©OAD 2023

# Misure tecniche: dati più significativi emersi (2)





# Le principali necessità e opportunità in Italia

- Forte sensibilizzazione e incremento consapevolezza dei **decisori di aziende/enti** sull'importanza dell'informatica e della sua sicurezza
- Necessità di **creare competenze** sulla sicurezza digitale e per **gestirle** all'interno di aziende/enti (**ruolo, compenso**, etc.)
- **Comportamento ETICO sia lato offerta che lato domanda**
- **Migliorare le misure di sicurezza** tecniche ed organizzative grazie a progetti di trasformazione digitale
- L'opportunità di **terziarizzare**, soprattutto per le piccole realtà, la gestione della sicurezza digitale:
  - **MSS**, Managed Security Services
  - **CSaaS**, CyberSecurity as a Service
- Maggior accentramento decisionale e di controllo con **ACN, Agenzia Cybersicurezza Nazionale**
- Compliance alle nuove direttive-regolamenti europei (**NIS2, DORA, CORE**, etc.)
- Sfruttare i progetti in ambito **PNRR** soprattutto per la digitalizzazione delle PA

# Grazie per l'attenzione, ci sono domande?

---

Questa presentazione sarà scaricabile in pdf anche dal sito AIPSI



Scaricate e leggete il Rapporto 2023 OAD

44

Per informazioni: [segreteria@aipsi.org](mailto:segreteria@aipsi.org)