

Webinar AIPSI 18 maggio 2022 ore 18



1

***Attacchi e misure di sicurezza
digitali in Italia: la situazione
attuale con riferimento anche
all'ultimo Rapporto OAD***

Marco R. A. Bozzetti

Presidente AIPSI

Fondatore e CEO Malabo Srl

(m.bozzetti@aipsi.org)

- Associazione apolitica e senza fini di lucro → <https://www.aipsi.org/>
- **Capitolo Italiano di ISSA**, Information Systems Security Association, (www.issa.org), la più grande associazione no-profit di professionisti della Sicurezza ICT nel mondo
- **Obiettivo principale**: aiutare i propri Soci nella **crescita professionale e delle loro competenze**, **tramite un insieme di servizi e di opportunità forniti da AIPSI a livello nazionale e da ISSA a livello internazionale**
 - logica della **formazione continua online** e basata sulla **CSCL, Cyber Security Career Lifecycle**, metodologia ISSA seguita e contestualizzata da AIPSI alla realtà italiana → **CSCL-IT**

I principali servizi AIPSI-ISSA

Principali Servizi erogati da AIPSI

- Aperti a tutti gli interessati anche non Soci
 - Indagini annuali: **OAD** e **CSWI**, **Cyber Security Woman Italy**
 - **Webinar ed eventi** anche in collaborazione con Associazioni, Enti ed Aziende
 - Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte
 - **AIPSI Giovani**
- Riservati ai Soli Soci
 - supporto alle certificazioni, in particolare per **eCF Plus** (EN 16234-1:2016) per profili sulla sicurezza digitale con AICA **con sconto**
 - Mentorship
 - SIG di approfondimento e discussione:
 - AI e Cybersec
 - Nuove architetture per Cybersec (SASE, SOAR, Zero Trust, etc.),
 - Crescita professionale Soci
 - Network Soci a livello nazionale

Principali Servizi erogati da ISSA

- ISSA Journal
- ESG ISSA Survey “The Life and Times of Cyber Security Professionals”
- Convegni, workshop, webinar in inglese
- Corsi online in inglese
- SIG, Special Interest Group
 - Privacy
 - Women in Security
- Accordi con sconti per certificazioni individuali
- Network Soci a livello mondiale



L'indagine OAD/OAI dal 2007



- **15 anni consecutivi di indagini** basate su questionari online anonimi
- **Per tutti i settori merceologici + Pubbliche Amministrazioni Centrali e Locali**
- **11 Rapporti pubblicati**
- Un sito ad hoc: www.oadweb.it

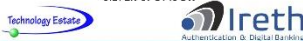
Rapporto OAD 2021 aggiornato ad aprile 2022



GOLD SPONSOR



SILVER SPONSOR



in collaborazione con Polizia Postale e delle Comunicazioni



Indagine effettuata da



Progetto scelto da



Scaricabile da:

- <https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/per-scaricare-il-rapporto-oad-2021-aggiornamento-aprile-2022.html>
- <https://www.oadweb.it/it/oad-extended-2021/per-scaricare-il-rapporto-oad-2021-aggiornamento-aprile-2022.html>



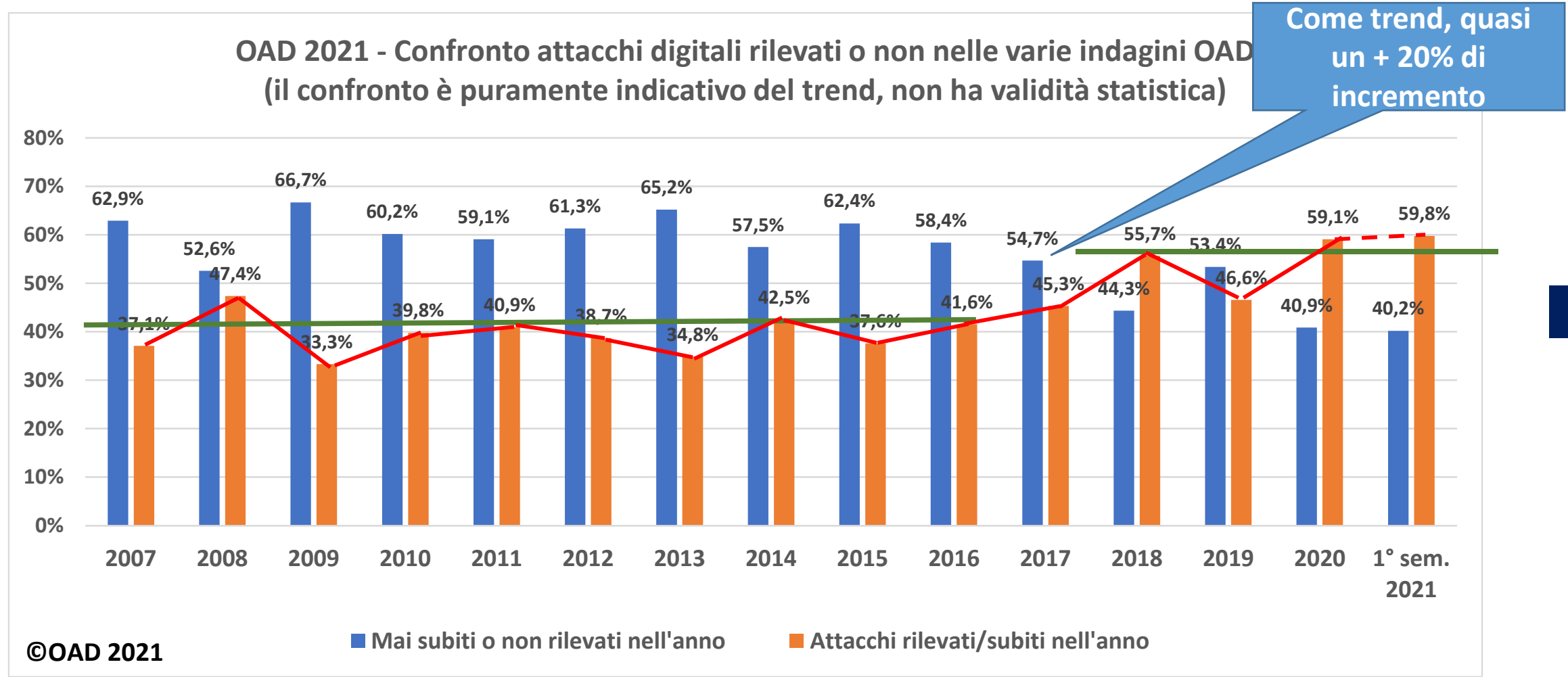
I patrocinatori di OAD 2021



START4.0

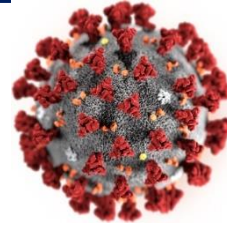


Forte incremento attacchi digitali intenzionali come trend da OAD 2007-2021



L'effetto combinato di Covid, guerra informatica e prevalenza piccole e piccolissime organizzazioni in Italia

- Covid 19
 - Ampio uso servizi Internet
 - Smart working
 - Molte aziende/enti con insufficienti misure di sicurezza
- Invasione Ucraina
 - Cyber warfare
 - Wiper
- La miriade di piccole piccolissime aziende/enti in Italia
 - Dai più recenti dati ISTAT



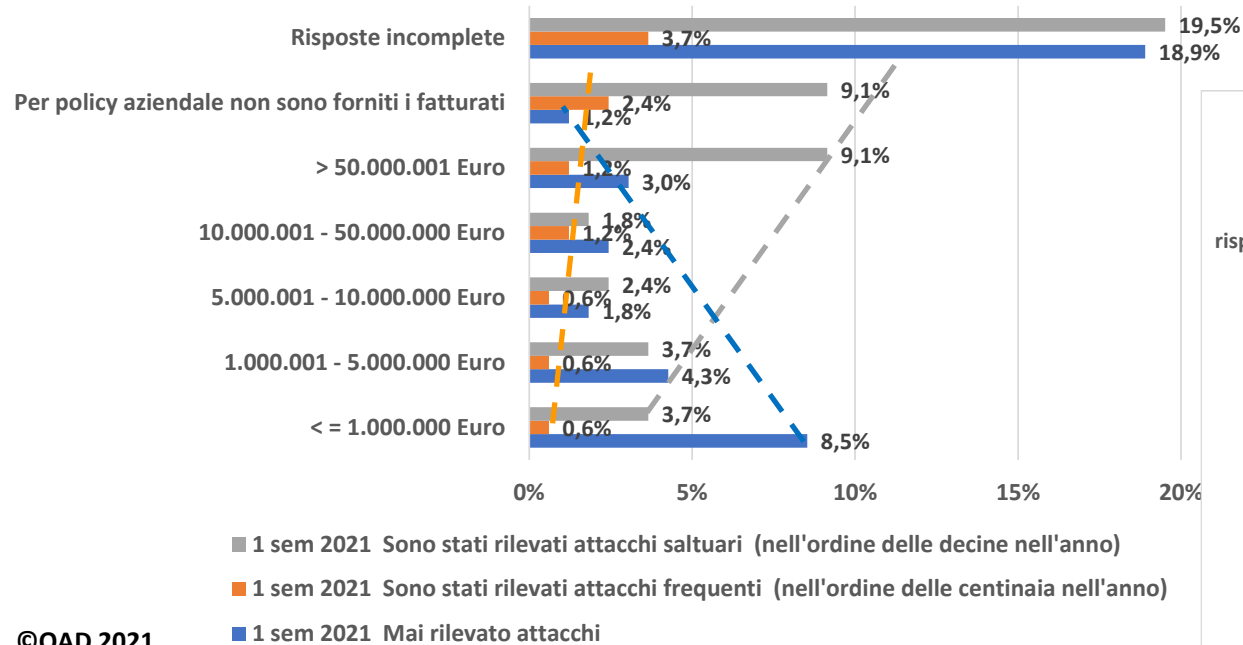
ISTAT: Imprese private per numero dipendenti	ISTAT Numero imprese	% sul totale ISTAT
< 10	4.149.572	94,80%
11-49	199.340	4,55%
50-249	24.288	0,55%
>250	4.179	0,10%
Complessivo	4.377.379	100%

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

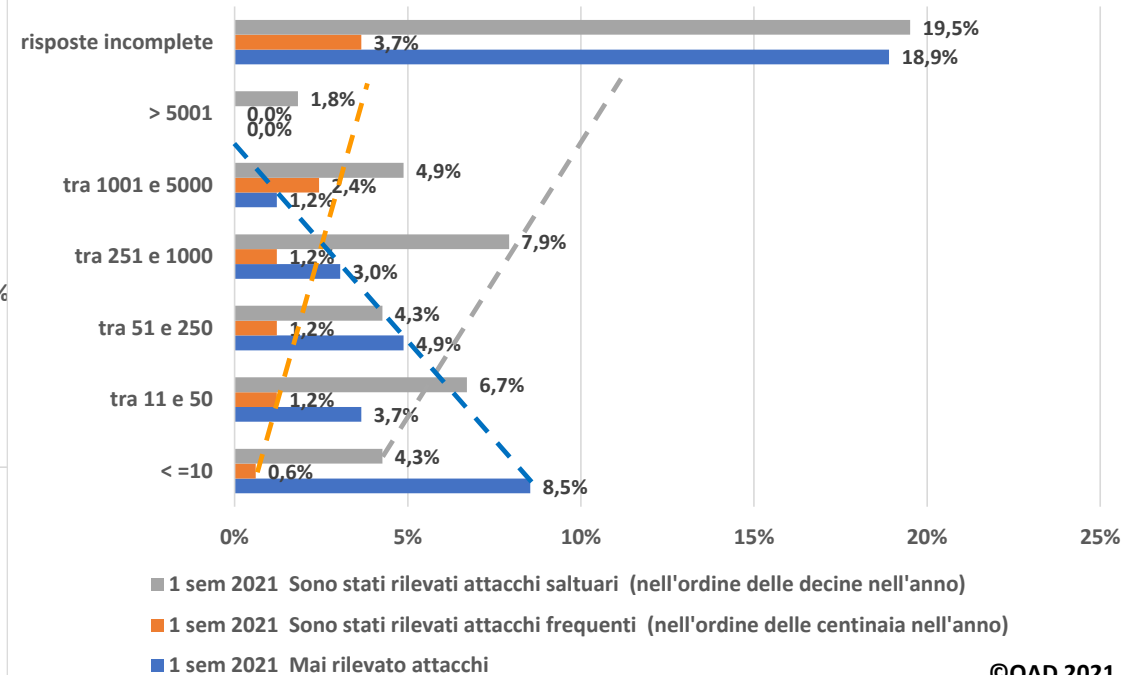
Analisi ISTAT solo
per alcuni ambiti
delle Pubbliche
Amministrazioni

OAD 2021 – Attacchi digitali prevalenti per aziende/enti di grandi dimensioni ed elevati fatturati

OAD 2021 - Distribuzione % nel 1 semestre 2021 di attacchi digitali ad aziende/enti dei rispondenti per fatturato/giro economico

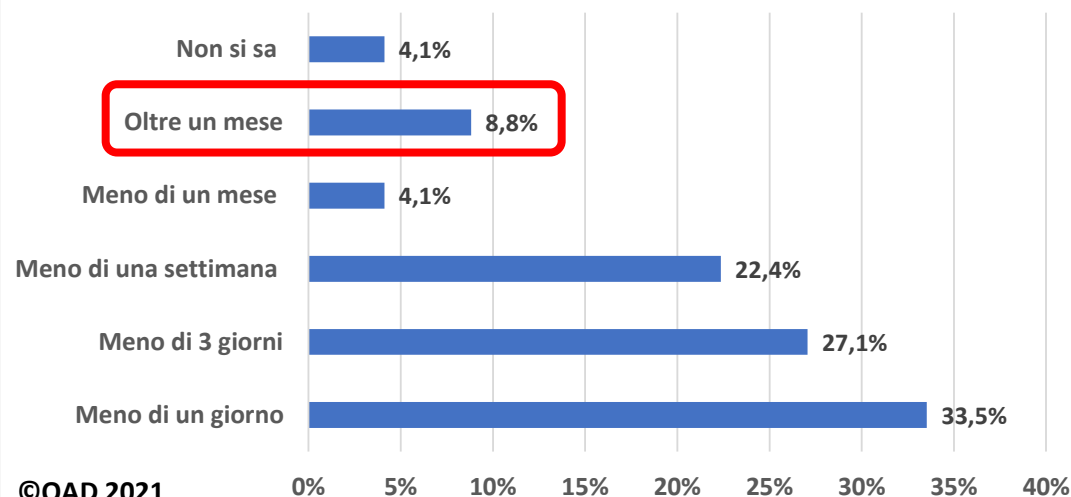


OAD 2021 - Distribuzione % nel 1° semestre 2021 di attacchi digitali ad aziende/enti dei rispondenti per numero dipendenti

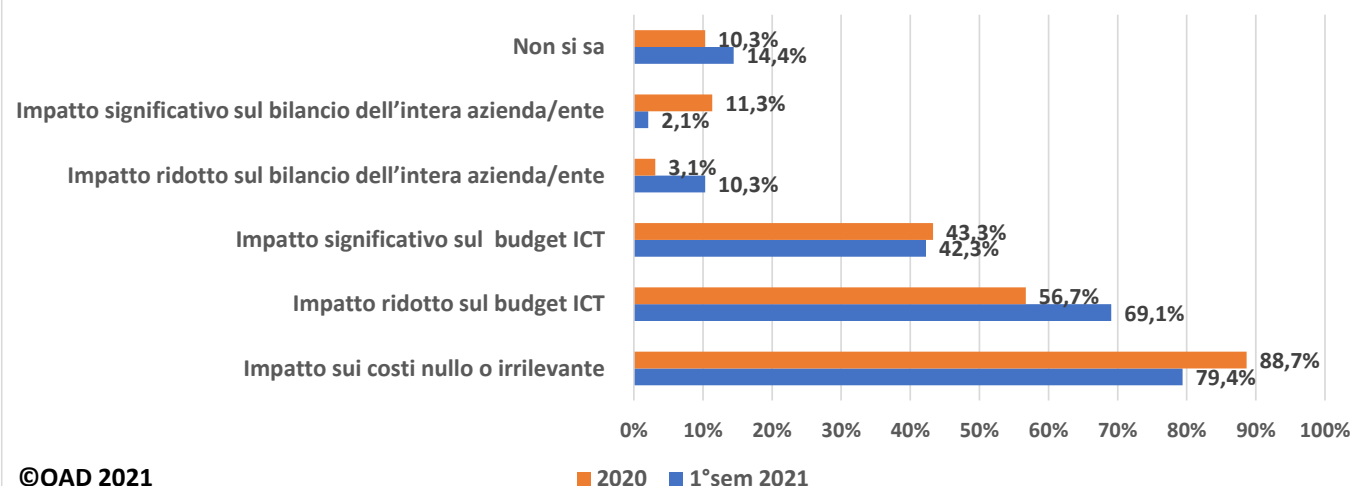


OAD 2021 – Tempi di ripristino e impatto economico dell'attacco digitale più grave

OAD 2021 - Distribuzione % del tempo massimo per ripristino da attacco più grave subito tra i Sistemi Informativi delle/dei rispondenti

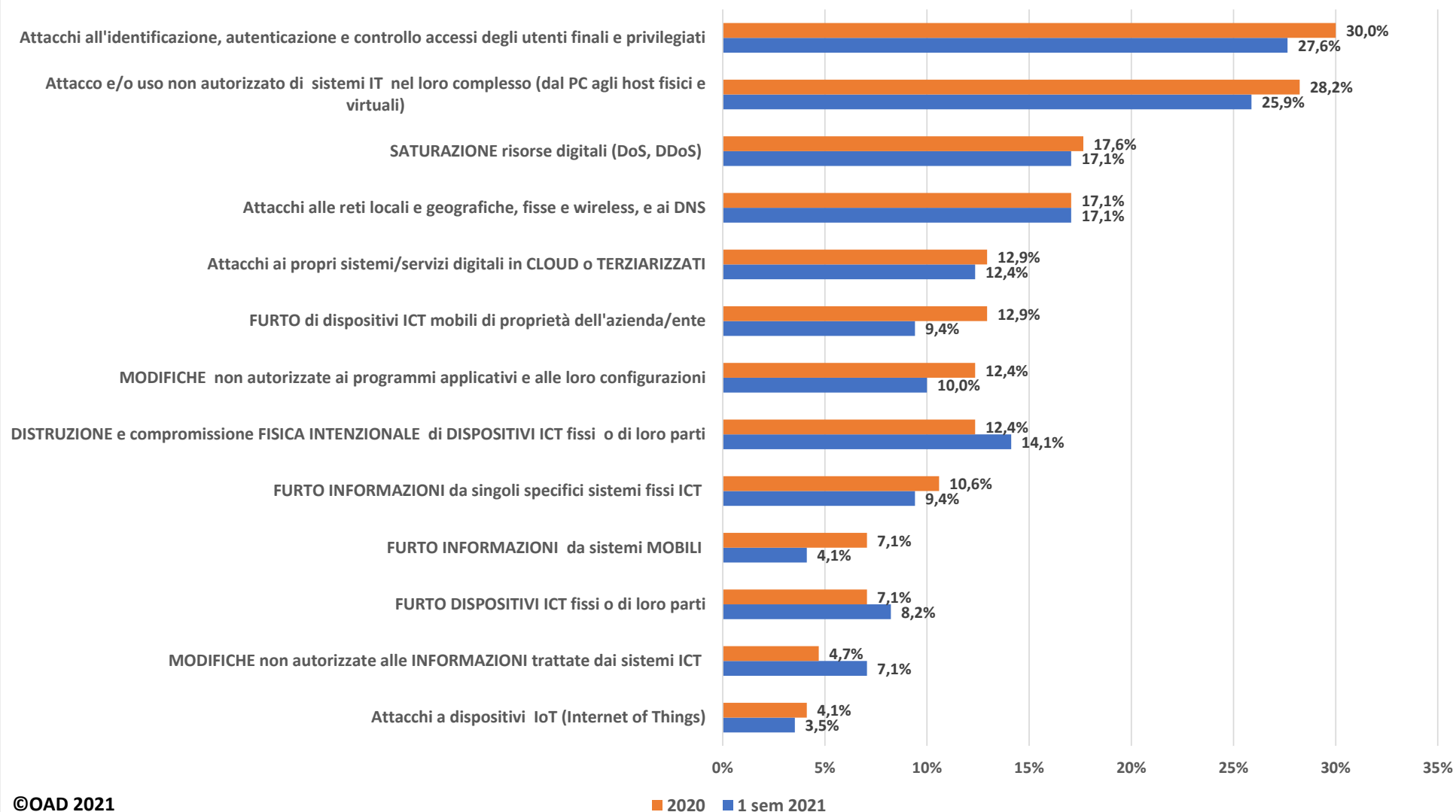


OAD 2021 - Distribuzione % impatti sui costi ICT e dell'azienda/ente per i più gravi attacchi digitali subiti (risposte multiple solo da questionario completo)



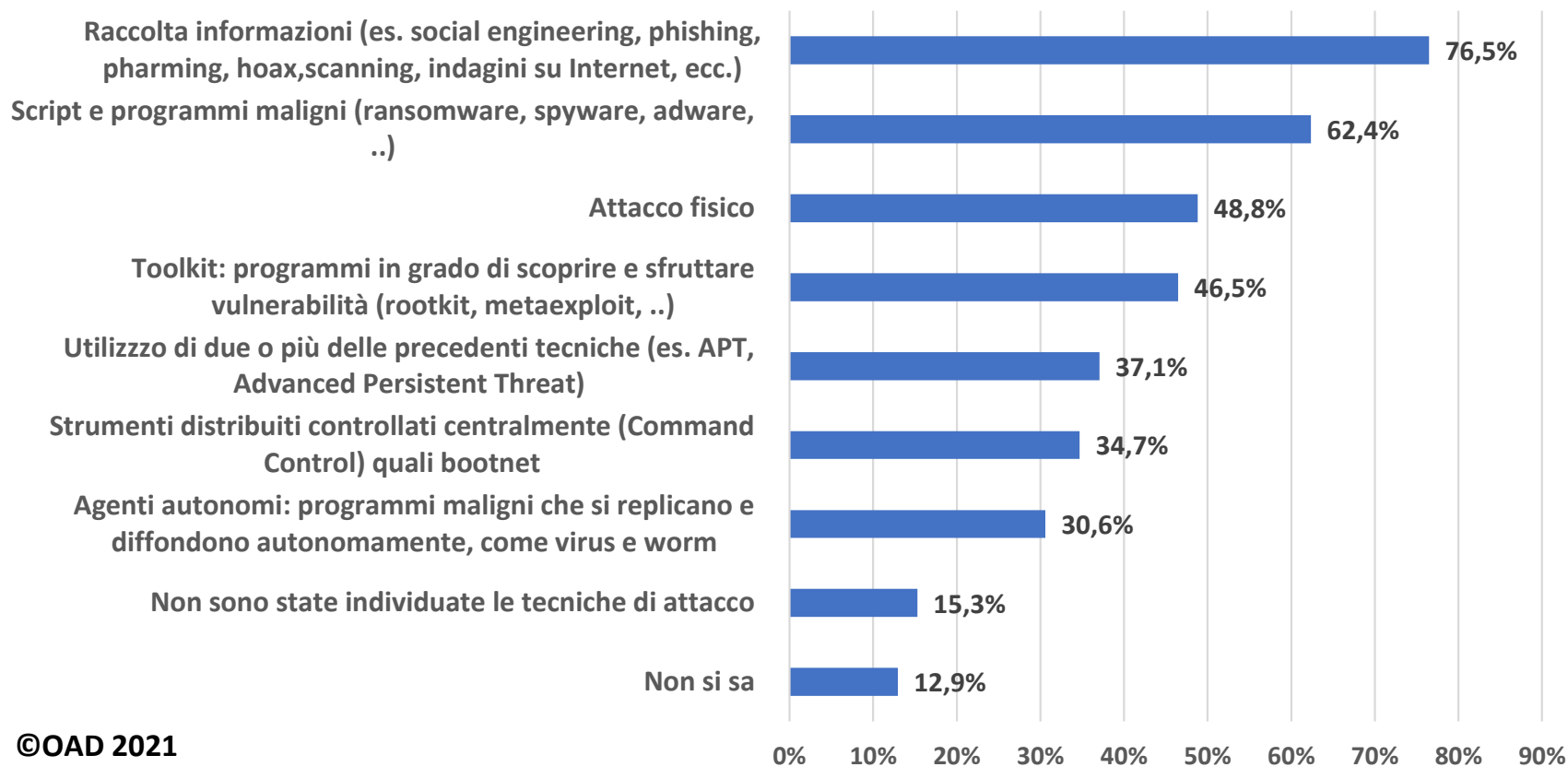
OAD 2021 – Distribuzione % tipologia attacchi digitali

OAD 2021 - Diffusione % delle tipologie di attacchi digitali tra le/i rispondenti nel 2020 e nel 1° semestre 2021
(risposte multiple)

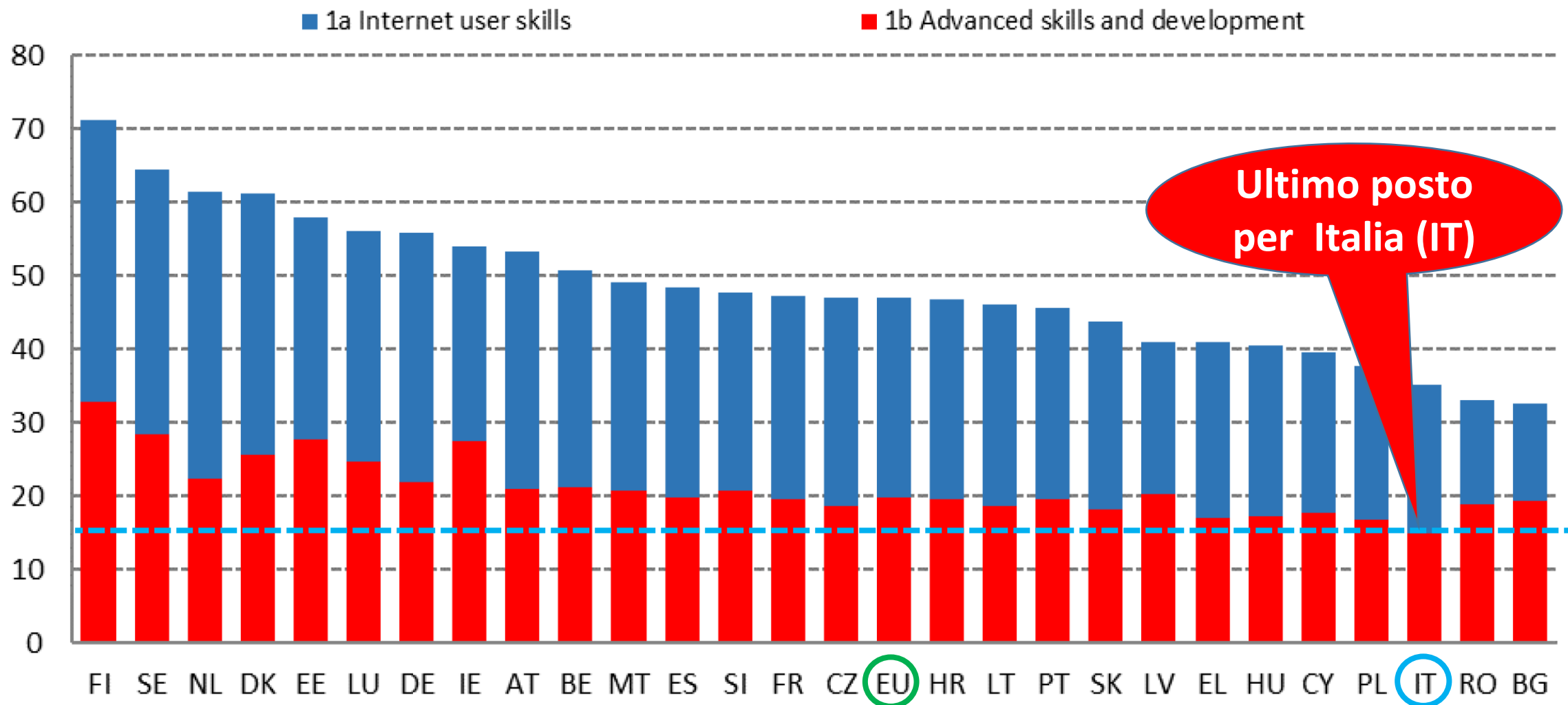


OAD 2021 – Distribuzione % macro-tecniche di attacco digitale

OAD 2021 - Distribuzione % tecniche di attacco tra le varie tipologie di attacco digitale rilevate dalle/dai rispondenti (risposte multiple)



DESI 2021: competenze umane sull'ICT

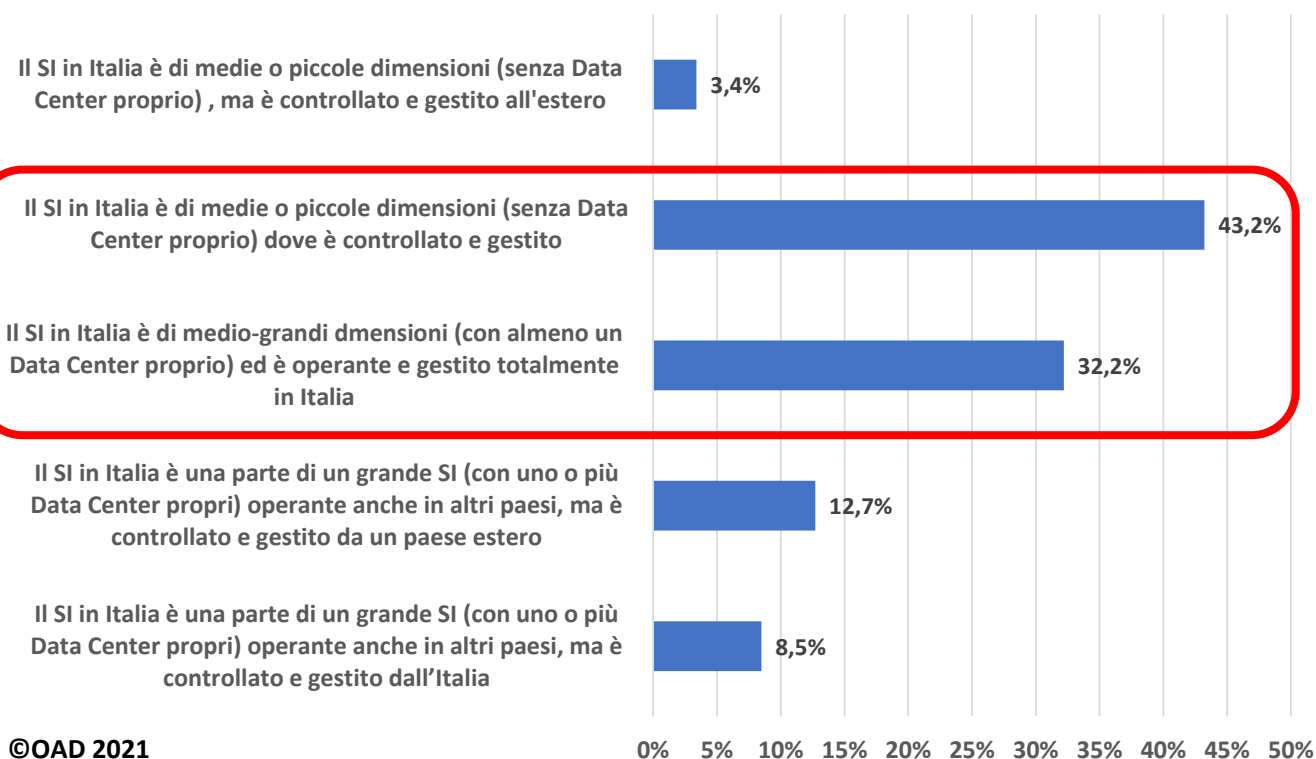


Considerazioni su quanto emerso
dall'indagine OAD:
**MISURE DI SICUREZZA
DIGITALE**

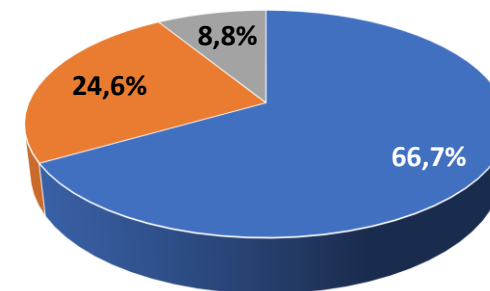
15

OAD 2021 – Il Sistema Informativo dei rispondenti

OAD 2021 - Macro tipologia del Sistema Informativo (SI) delle aziende/enti rispondenti



OAD 2021- Rilevanza del SI per l'azienda/ente rispondente

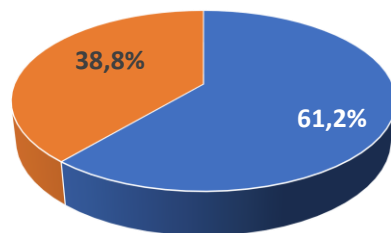


- SI Essenziale, le attività più importanti sono tutte on line e dipendono dal suo continuo e corretto funzionamento
- SI Importante ma non essenziale: le principali attività/processi non dipendono totalmente dal suo buon funzionamento
- SI di solo supporto a talune attività e processi dell'azienda/ente

©OAD 2021

OAD 2021 - Misure organizzative per la sicurezza digitale

OAD 2021 - E' definita una struttura organizzativa per la sicurezza digitale con una/un CISO?



©OAD 2021

■ SI ■ NO

OAD 2021 - Policy e procedure organizzative per la sicurezza digitale

SI, sono definite e attuate SOLO ALCUNE policy e procedure organizzative per la sicurezza digitale

53,4%

SI, sono definite ed attuate policy e procedure complete e aggiornate regolarmente

26,2%

NO, non sono definite policy e procedure organizzative per la sicurezza digitale

20,4%

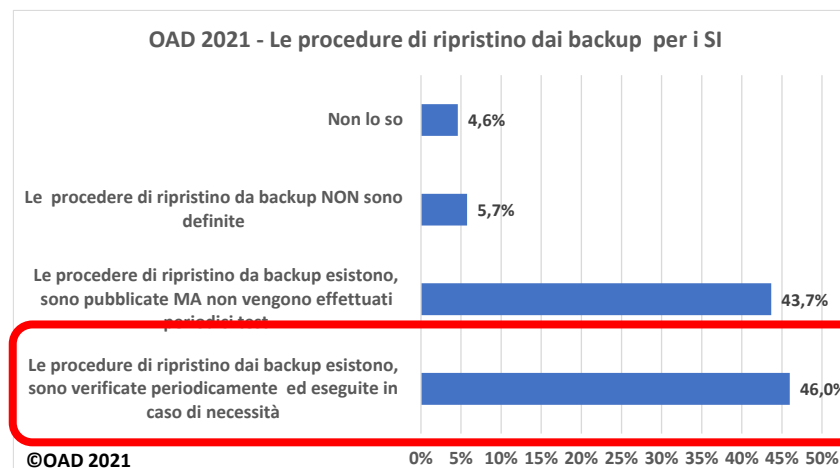
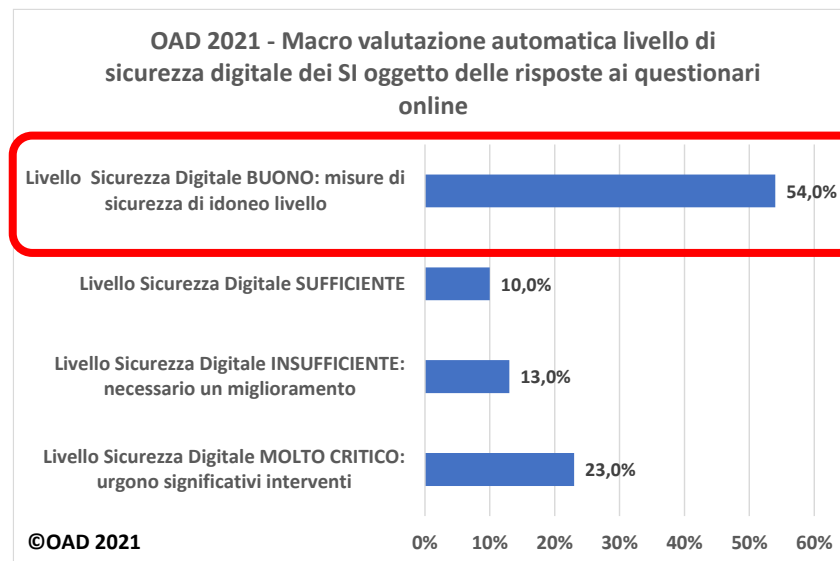
©OAD 2021

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

OAD 2021 - Misure tecniche per la sicurezza digitale

Le classi di misure tecniche considerate in OAD

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



Come far fronte nel prossimo futuro agli attacchi digitali

19

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
- Forti incentivi per **creare competenze** sulla sicurezza digitale e per **gestirle** all'interno di aziende/enti (**ruolo, compenso**, etc.)
- **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**
- Prossimo passaggio da **Da NIS a NIS2** per le infrastrutture critiche/servizi essenziali
- Progetti in ambito **PNRR**

20

Lo discuteremo con la Tavola Rotonda che segue

Coordinatore: Massimo Chirivì (Vice Presidente AIPSI)

- **Luca Bertoletti** (Marketing & Business Development Executive Ireth)
- **Massimiliano Brolli** (Head del Red Team di TIM e Fondatore Red Hot Cyber)
- **Roger Cataldi** (CISO & Head of Cyber security Almaviva, in rappresentanza Anitec-Assinform)
- **Paola Generali** (Presidente Assintel)
- **Mario Pitassi** (CEO Technology Estate)



21