CONFINDUSTRIA DIGITALE

Anitec-Assinform

IL DIGITALE IN ITALIA 2022

Previsioni 2022-2025 e Policy

CONFINDUSTRIA DIGITALE

Anitec-Assinform

IL DIGITALE IN ITALIA 2022

Previsioni 2022-2025 e Policy

Novembre 2022

Con la collaborazione di

Net Consulting 3
Empowering your Digital Business

In questi anni, il settore digitale ha vissuto un trend sostanzialmente positivo e in controtendenza rispetto all'andamento dell'economia italiana. Anche nel 2020, nonostante la crisi economica innescata dalla pandemia, il comparto ha tenuto dimostrando, anzi, di essere fondamentale per abilitare il lavoro, la quotidianità e l'attività di imprese e PA. Nel 2022 abbiamo raggiunto circa 76 miliardi di euro di fatturato, in crescita del 2% sul 2021 nonostante la difficilissima congiuntura economica, dove imperversano crisi energetica, inflazione, tassi di interesse in rialzo, in un contesto geopolitico in forte fibrillazione a partire dalla guerra in Ucraina.

Sono fattori che gravano sulle prospettive di crescita delle nostre imprese e sui bilanci delle famiglie, con il rischio di vanificare gli sforzi compiuti dopo la pandemia a partire dagli investimenti previsti dal PNRR.

Uscire da questa tempesta perfetta non è semplice e non esistono soluzioni facili.

Ciò detto, appare evidente come sia fondamentale non solo "resistere" – con aiuti in grado di raggiungere le fasce della popolazione più in difficoltà e dare ossigeno alle imprese più esposte – ma soprattutto mettere al sicuro il nostro futuro agendo sulla leva più importante: la nostra produttività.

Investire nelle nuove tecnologie digitali e accelerare la trasformazione digitale delle imprese e della PA è parte della soluzione alla scarsa produttività del nostro tessuto produttivo. Investire nell'innovazione delle competenze delle persone lungo l'intero percorso di vita e di lavoro nonché nell'innovazione di beni e servizi vuol dire accogliere l'ibridazione tra fisico e digitale che già oggi è presente in fabbriche, scuole, uffici pubblici, ospedali e che deve trovare una corsia preferenziale per diventare strutturale. Cloud, Intelligenza artificiale, Analytics, Blockchain, e un domani il Metaverso, servono per rendere più efficiente il nostro modo di produrre, lavorare, vivere e servire la collettività. Aiutano a ridurre divari, disuguaglianze, fanno esplodere talenti e capacità. Raccogliendo, elaborando e utilizzando in maniera sapiente i dati siamo in grado oggi di rendere più competitivo il Paese. Perché ciò accada, però, servono investimenti e ancora di più servono le competenze, persone formate a lavorare per e in un contesto sempre più digitale.

Se nel PNRR abbiamo trovato la cornice strategica all'interno della quale disegnare le priorità della transizione digitale del Paese, è nella realtà di ogni giorno che il digitale deve affermarsi come leva di crescita e di sviluppo, di apprendimento, di nuova conoscenza.

Al contempo, è fondamentale acquisire una cultura del digitale che ci consenta di minimizzare i rischi derivanti da un sempre più diffuso e imprescindibile utilizzo di dati. Per questo abbiamo deciso di dedicare nel secondo rapporto un focus alla Cybersecurity, con l'obiettivo non solo di evidenziare l'importanza di aumentare la rete di protezione dei nostri dati, ma anche di rendere evidente come oggi sia necessario passare dal "se" al "come", costruendo una rete di collaborazioni tra pubblico e privato, che renda possibile massimizzare i benefici della digitalizzazione.

Il momento storico non prevede passi indietro. La trasformazione digitale, semmai, richiede un dialogo costruttivo tra istituzioni e imprese e nel Paese, improntato al realismo e con lo sguardo rivolto al futuro. Solo così potremmo affrontare questa crisi e tornare a crescere, insieme.

Marco Gay
Presidente Anitec-Assinform
Novembre 2022

Come di consueto, l'appuntamento con l'aggiornamento autunnale dei dati del Rapporto Anitec-Assinform "Il Digitale in Italia" ci offre la fotografia dell'andamento del mercato digitale nell'anno in corso sulla base del consolidato del primo semestre e una finestra su quello che ci attende nel prossimo anno.

È doveroso rivolgere i complimenti e un ringraziamento al Presidente Marco Gay e ad Anitec-Assinform per questo lavoro che offre uno strumento preziosissimo a tutti coloro, esperti del settore e non, che vogliano approfondire la conoscenza del mercato italiano delle tecnologie e dei servizi digitali.

Il quadro che ci offre il Rapporto vede il mercato digitale italiano attestarsi su una crescita che è inferiore a quella registrata nello stesso periodo del 2021: il primo semestre 2022 segna una crescita del 3% rispetto al primo semestre 2021, mentre lo scorso anno la crescita sul medesimo periodo segnava un + 5,7%.

Ci troviamo quindi di fronte a un mercato che conferma un trend positivo, ma con un rallentamento della crescita che è del tutto compatibile con il quadro macroeconomico che nel primo semestre del 2022 ha visto un brusco arresto della ripresa post pandemia, arresto della crescita le cui cause sono ben note e che inevitabilmente condizionano anche le previsioni per il 2023.

Il peggioramento generale dell'economia nazionale, l'inasprimento delle condizioni finanziarie, la crisi energetica, la flessione dei consumi delle famiglie, sono tutti fattori che hanno ovviamente contribuito a rallentare significativamente la crescita del settore che aveva caratterizzato il 2021.

Il valore complessivo di questo mercato si è attestato nel primo semestre 2022 a 37,2 miliardi di euro e il Rapporto, come sempre, analizza in dettaglio i singoli segmenti che compongono il mercato. Anche nel 2022 si conferma il divergente risultato del comparto dell'Information Technology rispetto al comparto TLC, che continua a presentare un quadro di forte e crescente sofferenza.

Il Rapporto, come di consueto, analizza in dettaglio l'andamento del primo semestre dell'anno dei diversi segmenti di mercato e le indicazioni che ne emergono sono di grandissima rilevanza, ma ovviamente l'appuntamento autunnale è soprattutto il momento delle previsioni su come si chiuderà il 2022 e sulle prospettive per il prossimo anno.

La prospettiva è quella di chiudere il 2022 con un mercato digitale che presenterà una crescita pari al 2,1%, con un segno marcatamente positivo per software/soluzioni e servizi ICT e per i contenuti digitali e, a far da contraltare, una contrazione dei dispositivi e sistemi e dei servizi TLC.

Le molte incertezze che pesano sull'economia mondiale si riflettono naturalmente sulle previsioni per il 2023 e a influire sul mercato digitale nazionale saranno anche gli impatti dei progetti finanziati con i Fondi del PNRR, così come le politiche in tema di innovazione digitale che saranno adottate dal Governo appena insediato.

Il Rapporto però ci fornisce alcuni punti fermi sia in positivo che in negativo: continuerà a essere un forte traino positivo la crescita del mercato Cloud e il grande sviluppo del mercato delle tecnologie e servizi legati alla protezione, organizzazione e analisi dei dati, ovvero Cybersecurity, Big Data, AI; rischia invece di continuare a essere un elemento di forte debolezza la contrazione dei ricavi generati dai servizi TLC, e occorre anche sottolineare come sul comparto dei servizi TLC pesi molto il rincaro dell'energia.

Il Rapporto contiene un'analisi dettagliata delle previsioni di crescita del mercato 2022-2025 dei cosiddetti Digital Enabler, tra i quali spicca il Cloud Computing, che si stima possa superare quota 10 miliardi di valore di mercato nazionale nel 2025 con un trend di crescita annuale che sfiora il 25%.

Anche il mercato delle soluzioni e servizi per la Cybersecurity, che era già in forte crescita prima dello scoppio del conflitto russo/ucraino, ha subito un'accelerazione mai vista prima e le dinamiche geopolitiche attuali lasciano prevedere che per fronteggiare le minacce Cyber assisteremo a una moltiplicazione degli investimenti.

L'approfondimento dedicato alla Cybersecurity contenuto in questa edizione del Rapporto è particolarmente ricco di dati e desidero raccomandarne la lettura a chi in particolare ha responsabilità di pianificazione degli investimenti in sicurezza nel mondo sia privato che pubblico: troverà indicazioni molto utili su strategie e strumenti da porre in campo per fronteggiare le minacce Cyber.

Massimo Sarmi
Presidente Confindustria Digitale
Novembre 2022

INDICE

LE PREVISIONI 2022-2025 PER IL MERCATO DIGITALE ITALIANO 2

Previsioni per l'economia italiana 4

Andamento complessivo del mercato digitale nel primo semestre 2022 5

Andamento complessivo del mercato digitale nel 2022 6

Previsioni del mercato digitale e dei comparti tecnologici: 2022-2025 7

Previsioni per i Digital Enabler: 2022-2025 8

Previsioni per settori d'utenza: 2022-2025 10

Stato di avanzamento degli investimenti del PNRR con elevato contenuto digitale 18

Scenari di previsione del mercato digitale e impatto del PNRR 20

CYBERSECURITY E TRANSIZIONE DIGITALE 22

Le minacce sul fronte della Cybersecurity: trend attacchi ed esposizione alle minacce 24

Impatti della trasformazione digitale sul fronte Cybersecurity: Smart Working, Cloud, IoT 30

Presenza di team dedicati/direzione con focus sulla Cybersecurity 35

Adozione di misure di Detection and Response 36

Il trend del mercato Cybersecurity, 2021-2025 40

La spesa in Cybersecurity nei settori dell'economia 42

La strategia di cybersicurezza nazionale 45

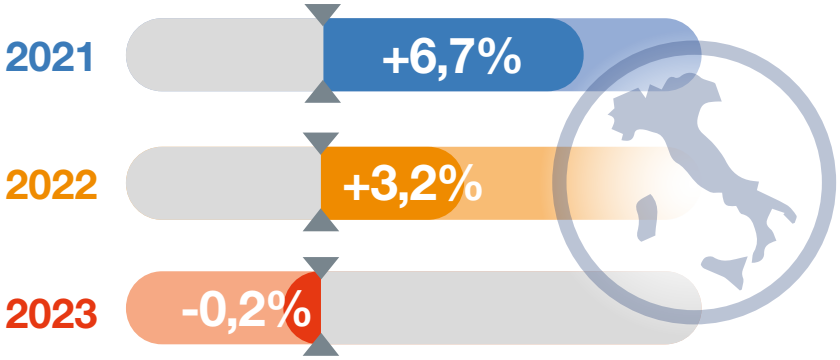
CONCLUSIONI 54

PROFILO ANITEC-ASSINFORM 66

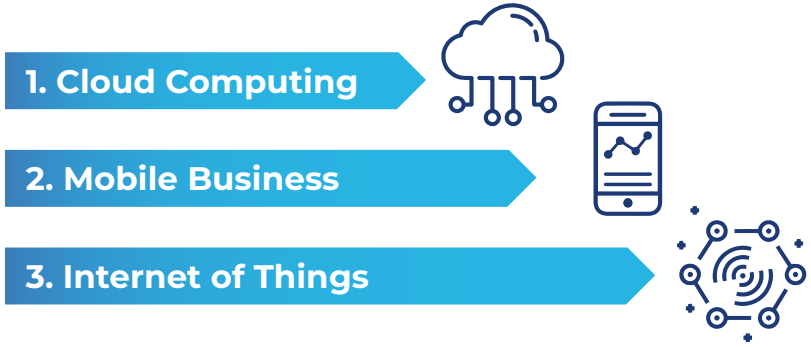
LE PREVISIONI 2022-2025 PER IL MERCATO DIGITALE ITALIANO

L'inizio del 2022 ha segnato un rallentamento della crescita dell'economia globale dopo la robusta ripresa del precedente anno. Secondo le stime, tale dinamica proseguirà anche nel 2023, determinando nei Paesi occidentali, tra cui l'Italia, un andamento del PIL ulteriormente in flessione. Nell'anno in corso, l'andamento del mercato digitale italiano ha rispecchiato questa tendenza. Nel primo semestre del 2022, tutti i settori sono stati in crescita, ma hanno fatto registrare un aumento in termini percentuali inferiore a quanto accaduto nei primi sei mesi del 2021. L'unica eccezione è rappresentata dai Servizi di rete, che hanno avuto in entrambe i semestri un andamento negativo. Nonostante le incertezze dovute allo scenario geopolitico, alle dinamiche inflattive e agli effetti del PNRR, è prevedibile che nei prossimi anni la trasformazione digitale in atto nelle aziende italiane proseguirà dando un rinnovato slancio al mercato.

Crescita del PIL italiano secondo il FMI:



Digital Enabler, i mercati più rilevanti a fine 2022:



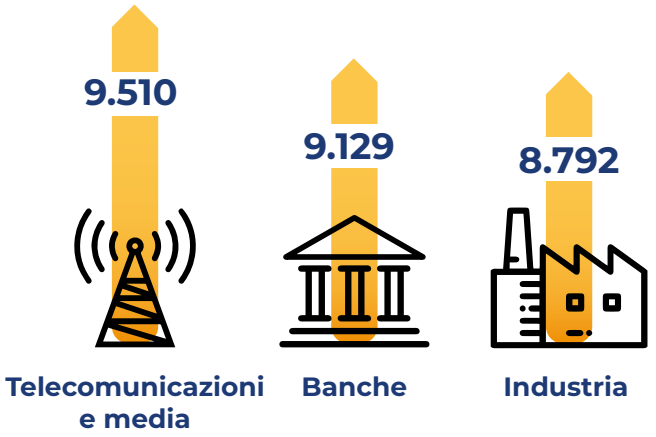
Gli investimenti di aziende e Pubblica amministrazione si stanno concentrando su:

Cloud | Cybersecurity | Big Data

Andamento del mercato digitale italiano:

Dimensioni del mercato per settori di utenza a fine 2022:

(Milioni di euro)



PNRR, spesa sostenuta per la digitalizzazione (al 31 agosto 2022):

128 milioni di euro

(1% della spesa complessiva sostenuta)

LE PREVISIONI 2022-2025 PER IL MERCATO DIGITALE ITALIANO

Previsioni per l'economia italiana

Nel corso dei primi mesi del 2022 si è registrato un arresto della ripresa dell'economia globale dopo l'emergenza Covid-19.
L'aumento del costo della vita, l'inasprimento delle condizioni finanziarie nella maggior parte delle aree del mondo, l'invasione dell'Ucraina da parte della Russia e il persistere della pandemia giocano un importante ruolo sulle prospettive del prossimo anno.

Tabella 1:

Previsioni sull'andamento del PIL nelle principali economie mondiali (2021-2023E)

Crescita % anno su anno	2021	2022	2023E
World Output	**6,0**	**3,2**	**2,7**
Economie avanzate	**5,2**	**2,4**	**1,1**
Stati Uniti	**5,7**	**1,6**	**1,0**
Area Euro	**5,2**	**3,1**	**0,5**
Germania	2,6	1,5	-0,3
Francia	6,8	2,5	0,7
Italia	6,7	3,2	-0,2
Spagna	5,1	4,3	1,2
Giappone	**1,7**	**1,7**	**1,6**
Regno Unito	**7,4**	**3,6**	**0,3**
Canada	**4,5**	**3,3**	**1,5**
Altre economie avanzate	**5,3**	**2,8**	**2,3**
Economie emergenti e in fase di sviluppo	**6,6**	**3,7**	**3,7**

Valori % — Fonte: NetConsulting cube su dati FMI-Word Economic Outlook, Ottobre 2022

Le stime del Fondo Monetario Internazionale per il 2023 prevedono un rallentamento dell'economia mondiale, la cui crescita passerà dal 6% del 2021, al 3,2% del 2022, ad un ulteriore peggioramento previsto nel 2023, anno in cui la crescita si stima sarà del 2,7% (Tab. 1), 0,2 punti in meno rispetto a quanto atteso a luglio e il dato più basso dal 2001, con le sole eccezioni della crisi globale finanziaria del 2008 e di quella scatenata dal Coronavirus nel 2020.
Si prevede inoltre che l'inflazione globale aumenterà dal 4,7% del 2021 all'8,8% del 2022 e che la sua frenata sarà più lenta del previsto: 6,5% nel 2023 e 4,1% nel 2024.
Nelle economie avanzate si assisterà ad un rallentamento della crescita, passando dal 5,2% del 2021, al 2,4% del 2022 sino all'1,1% del 2023.
Se negli Stati Uniti la flessione determinerà un calo della crescita dall'1,6% del 2022 all'1% del successivo anno, nell'Eurozona, in cui l'aumento dell'economia nel corso del 2022 è stato più sostenuto, pari al 3,1%, si avrà un calo più marcato della crescita, che nel 2023 si attesterà intorno allo 0,5%.
I Paesi più colpiti da questa dinamica saranno Germania e Italia, per i quali nel 2023 si prevede una recessione, con una contrazione del PIL pari rispettivamente allo 0,3% e allo 0,2%.
Analizzando più nel dettaglio la situazione italiana, nell'ultimo aggiornamento del Documento di Economia e Finanza (novembre 2022) il Governo stima una crescita del PIL a fine anno del +3,7%, con un incremento, rispetto alle previsioni del DEF di aprile 2022, dello 0,6%. Nel 2023 si prevede un rallenta-

mento (+0,3%), per poi avere un aumento del PIL nell'ordine dell'1,8% nel 2024.
L'indebitamento netto del Paese scenderà nel 2022 al 5,1%, e si attesterà nel 2023 al 3,4%.
Il rapporto debito/PIL è previsto in calo negli ultimi mesi del 2022, posizionandosi al 145,4% (rispetto al 150,3% del 2021); una discesa che si stima proseguirà anche nel prossimo biennio sino ad arrivare al 141,2% del 2025.
Più caute sono invece le previsioni formulate da Confindustria (Tab. 2), che ipotizzano nel 2023 una crescita per l'Italia pari a 0, a causa dello shock energetico: i costi per le imprese legati all'aumento dei prezzi dell'energia sono previsti in crescita di 110 miliardi di euro, con una incidenza che sale dal 4,6% al 9,8% dei costi totali, e con una conseguente contrazione dei margini per le imprese stesse.

Andamento complessivo del mercato digitale nel primo semestre 2022

In linea con la tendenza generale dell'economia italiana, anche il mercato digitale in Italia è stato caratterizzato, nel primo semestre 2022, da una crescita inferiore rispetto a quella fatta registrare nello stesso periodo del 2021.
Infatti, se nel primo semestre 2021 la crescita era stata del 5,7% rispetto allo stesso periodo del precedente anno, nel primo semestre del 2022 il mercato digitale si è attestato sui 37.163 milioni di euro, con un incremento del 3% rispetto al primo semestre 2021 (Fig. 1).

Il comparto dei Dispositivi e Sistemi ha avuto un incremento del 3,4%, (10.142 milioni di euro). In questo segmento di mercato vanno segnalate le crescite degli apparecchi TV (+20%), degli apparati per la visualizzazione video in streaming e dei decoder (+83,5%), dei server e più in generale di tutti i sistemi enterprise (storage e networking). In forte diminuzione è risultato invece il comparto dei PC, sia Desktop (-9,4%) che Laptop (-10,1%).
Il comparto del Software e delle Soluzioni ICT ha segnato un aumento del 5,5% (3.852 milioni di euro), dovuto ad una crescita della spesa per acquisti di software middleware, nei segmenti dell'Information management, della sicurezza e del software applicativo.
Il valore del mercato dei Servizi ICT ha registrato, sempre nel primo semestre 2022, un valore di 6.921 milioni di euro (+7,2%), confermando sostanzialmente la crescita avuta nell'anno precedente. In tale contesto si segnala la continua e costante crescita

Tabella 2:
Previsioni per l'Italia (2021-2023E)

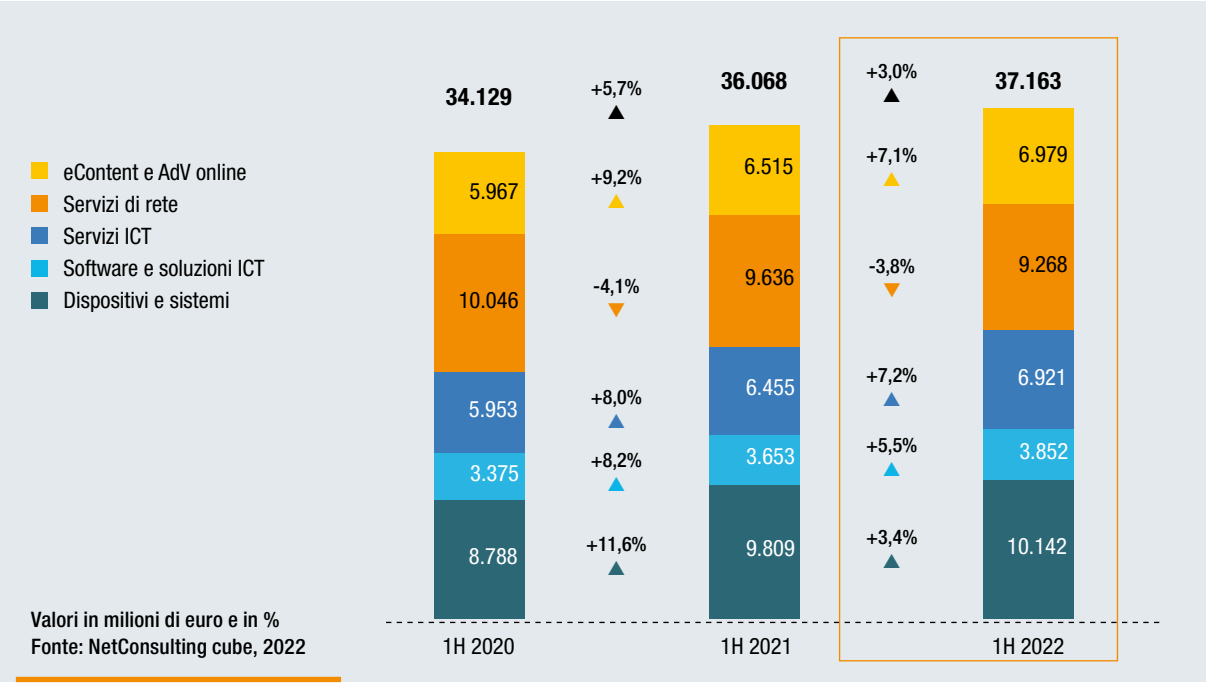
Crescita % anno su anno	2021	2022	2023E
Prodotto Interno Lordo	**6,7**	**3,4**	**0,0**
Consumi delle famiglie residenti	5,2	3,1	-0,1
Investimenti fissi lordi	16,5	10,2	2,4
Esportazioni di beni e servizi	13,4	10,3	1,8
Occupazione totale (ULA - Unità equivalenti di lavoro a tempo pieno)	**7,6**	**4,3**	**-0,1**
Prezzi al consumo	**1,9**	**7,5**	**4,5**
Indebitamento della PA (% del PIL)	**7,2**	**5,1**	**3,5**

Valori % — Fonte: NetConsulting cube su dati Confindustria, Ottobre 2022

del mercato cloud (+25,5%) e dei settori consulenza e system integration anche se, questi ultimi, con aumenti inferiori rispetto allo stesso periodo dell'anno precedente.
I Servizi di Rete hanno prodotto un valore pari a 9.268 milioni di euro, determinando un'ulteriore contrazione (-3,8% nel 2022 e -4,1% nel 2021). In tale contesto si segnala una diminuzione dei servizi di rete fissa (-4,1%), un dato ancora peggiore rispetto a quello dello stesso periodo del 2021 (-1,2%). In diminuzione (-3,6%) sono risultati anche i servizi di rete mobile; una flessione però più contenuta rispetto al primo semestre del 2021 (-6,4%).

Figura 1:

Il mercato digitale in Italia nel primo semestre 2022



Valori in milioni di euro e in %
Fonte: NetConsulting cube, 2022

Il segmento dei Contenuti e della Pubblicità digitale ha chiuso il primo semestre del 2022 con un mercato attestatosi sui 6.979 milioni di euro e una crescita del 7,1%.
In rallentamento è stato il mercato del Digital Advertising (+4,8% nel 2022 rispetto al +11,5% del primo semestre 2021), mentre si sono confermati positivi i mercati del Mobile Entertainment e delle App mobili.

Andamento complessivo del mercato digitale nel 2022

Le dinamiche di questa seconda metà del 2022 sono influenzate da un peggioramento generale dell'economia italiana, soprattutto da una flessione dei consumi delle famiglie e da un rallentamento nell'andamento del PIL.
Nel complesso, nel 2022, quasi tutti i comparti sono comunque previsti in crescita, anche se con un trend inferiore rispetto alle previsioni formulate lo scorso giugno. Per i Servizi di Rete è invece previsto un andamento negativo, proseguendo il calo già osservato negli anni passati.
Un raffronto con le previsioni di giugno consente di mettere in risalto i seguenti aspetti (Fig. 2):

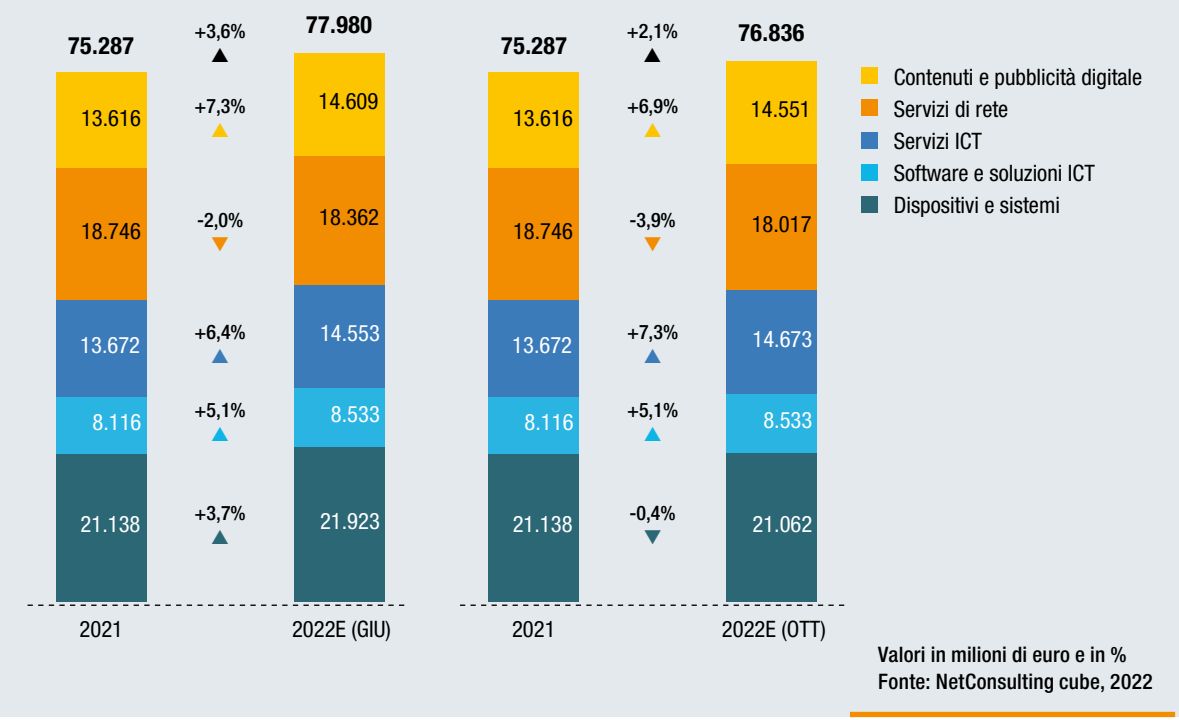
- la flessione dei Dispositivi e Sistemi (-0,4%) a causa del calo più accentuato nei segmenti degli apparecchi TV (-13%), dei Personal computer (-11%) e dei Tablet (-3,1%);
- la conferma della crescita del segmento Software e Soluzioni ICT (+5,1%);
- l'ulteriore aumento del comparto dei Servizi ICT (+7,3%) per effetto dei processi di accelerazio-

ne della digitalizzazione in tutti i comparti grazie all'impiego di servizi Cloud e, più in generale, di Managed Services;
- la sostanziale conferma della crescita del segmento dei Contenuti Digitali (+6,9%).

Previsioni del mercato digitale e dei comparti tecnologici: 2022-2025

Le previsioni sull'andamento del mercato digitale fino al 2025 sono condizionate non solo dalle considerazioni macroeconomiche particolarmente pessimistiche, ma anche dall'entità effettiva dei progetti finanziati dal PNRR destinati alla trasformazione digitale della Pubblica Amministrazione e del sistema produttivo, per i quali non è però ancora possibile stabilire del tutto le ricadute.
Sulla base di queste considerazioni, nel 2023 si prevede tuttavia un aumento del mercato digitale italiano leggermente migliorativo rispetto al 2022, con una crescita pari al 3% e un ammontare complessivo di 79.138 milioni di euro, circa 2,3 miliardi di euro in più rispetto al 2022. Per i successivi anni si ipotizza invece un aumento più sostenuto: +4,8% nel 2024 e +5,3% nel 2025, con un mercato che nel 2025 potrebbe superare gli 87 miliardi di euro (Fig. 3). Nel periodo 2023-2025 tutti i comparti sono previsti in crescita, ad eccezione di quello dei Servizi di Rete, per il quale si stima il proseguimento del calo già osservato negli anni scorsi, anche se in misura tendenzialmente inferiore.
La situazione generale di incertezza avrà un impatto soprattutto sul segmento dei Dispositivi e Sistemi. Per questo comparto si prevede infatti nel 2023 solo un leggero aumento (+0,9%) a 21.249 milioni di euro, dovuto anche alla contrazione negli acquisti degli apparecchi TV (-12%) e dei PC (-7%). Sono previsti andamenti positivi nei segmenti dei sistemi di sicurezza e dei sistemi specializzati per l'esigenza di potenziare le reti e rinnovare i sistemi in alcuni comparti, primo tra tutti quello della Pubblica Amministrazione. Per quanto riguarda i dispositivi mobili, si stima un leggero aumento per gli smartphone e i tablet.

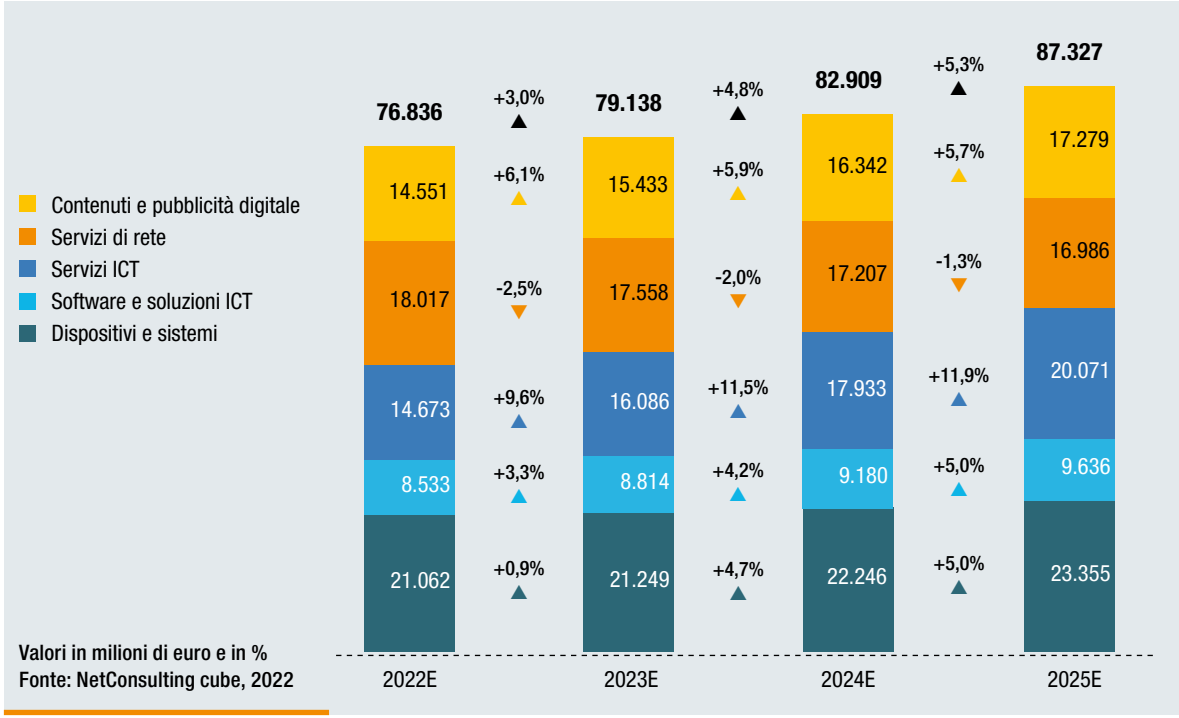
Figura 2:
Il mercato digitale in Italia nel 2022



Valori in milioni di euro e in %
Fonte: NetConsulting cube, 2022

Figura 3:

Il mercato digitale in Italia, previsioni 2022-2025



Valori in milioni di euro e in %
Fonte: NetConsulting cube, 2022

Con l'avvio di nuovi progetti applicativi, infrastrutturali e di trasformazione digitale, in molti casi collegati alle risorse rese disponibili dal PNRR, i comparti di mercato del Software e Soluzioni ICT e dei Servizi ICT sono previsti in aumento. In particolare, nel 2023, per il primo comparto si prospetta un andamento positivo principalmente nei segmenti del Middleware e della Sicurezza informatica.
I Servizi ICT continueranno a beneficiare soprattutto di una crescita dei progetti di digitalizzazione e di replatforming di applicazioni, nonché di una trasformazione rivolta a sostenere la migrazione al Cloud.
Proprio il Cloud proseguirà la sua crescita (+25%), considerata la centralità che assume nei piani di trasformazione digitale delle aziende e il ruolo strategico che gli viene attribuito nella transizione digitale della PA. Nel complesso, si prevede che i Servizi ICT possano raggiungere il ragguardevole valore di 20 miliardi di euro nel 2025.
In crescita saranno anche gli investimenti in Digital Advertising nel segmento più ampio di mercato dei Contenuti e Pubblicità Digitale, che dovrebbe raggiungere nel 2023 i 15.433 milioni di euro (+6,1%).

Previsioni per i Digital Enabler: 2022-2025

Tra il 2022 e il 2025, i Digital Enabler è prevedibile che continuino ad essere un elemento di traino straordinario per lo sviluppo del mercato digitale italiano, complici le tante iniziative di trasformazione digitale che, nonostante il periodo di incertezza, continueranno a nascere nelle aziende.
Nel dettaglio, è possibile identificare tre cluster di tecnologie. Nel primo si collocano soluzioni e piattaforme che hanno raggiunto valori di mercato rilevanti e che hanno ancora buone prospettive di crescita. È il caso del Cloud Computing, che dovrebbe superare quota 10 miliardi di euro nel 2025 grazie ad una crescita media annua nel periodo 2022-2025 del 24,5%. Il Cloud ha assunto un ruolo baricentrico nella trasformazione digitale e nel supportare priorità tecnologiche e business grazie agli ormai comprovati vantaggi in termini di flessibilità e scalabilità rispetto alle tradizionali logiche on premise. In ter-

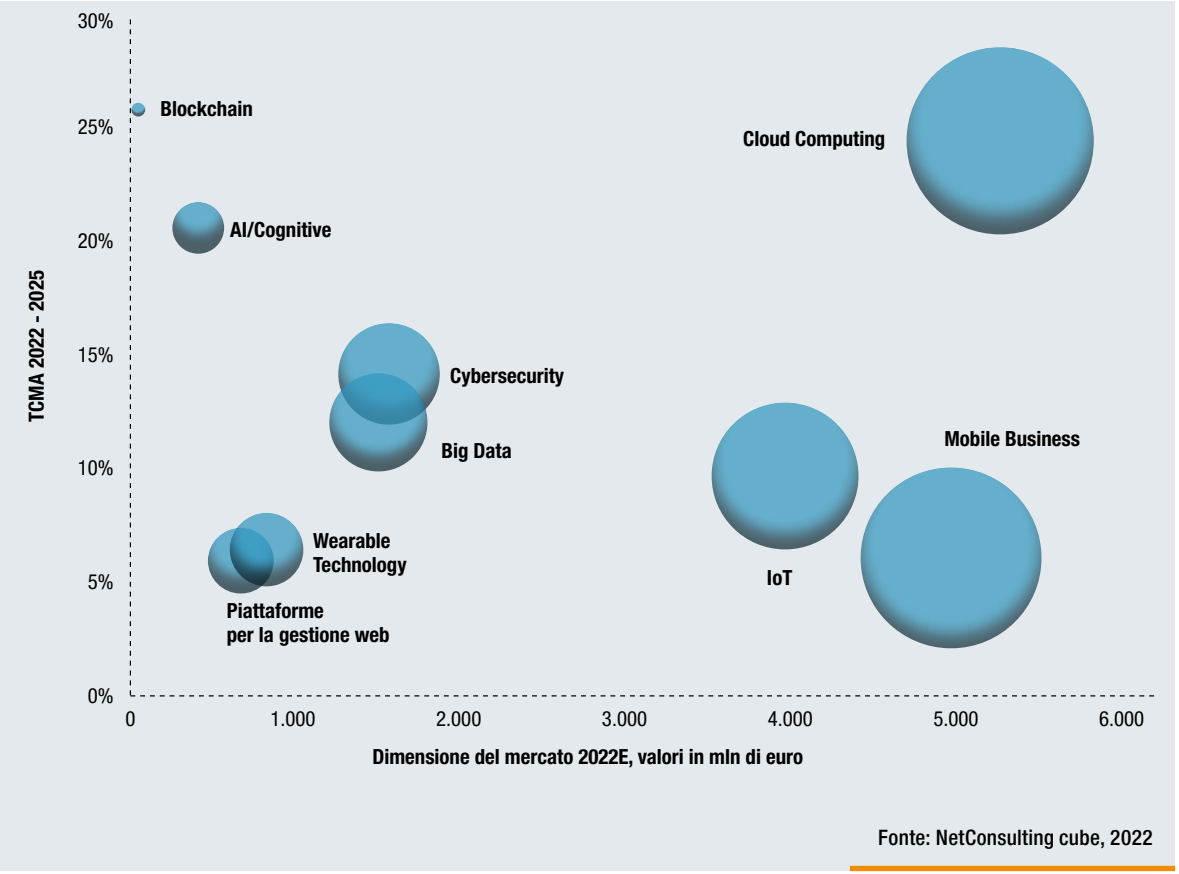
mini di performance segue l'IoT (4 miliardi di euro, +8,8%), che è alla base dell'innovazione tecnologica di processi operativi e produzione e dei filoni di sviluppo del PNRR. Infine va segnalato il Mobile Business (5 miliardi di euro, +6,1%), il cui sviluppo riflette l'aumento continuo della mobilità dei lavoratori pur in presenza di una crescente maturità della domanda di dispositivi e servizi di comunicazione (Fig. 4).

Nel secondo cluster si collocano Cybersecurity (1,6 miliardi di euro, +14%) e Big Data (1,6 miliardi di euro, +12,7%): la prima prosegue la sua crescita costante sulla spinta dell'esigenza di proteggere i dati e le applicazioni dalle incessanti minacce; il mercato dei Big Data continua invece ad essere sostenuto dall'esigenza di gestione e valorizzazione dei dati.

Nel terzo cluster ricadono infine soluzioni e tecnologie di nicchia, o perché caratterizzate da un utilizzo molto specifico o perché i loro casi d'uso non hanno ancora trovato piena concretizzazione. Al primo sottogruppo appartengono le Piattaforme per la gestione Web (674 milioni di euro, +5,2%), che trovano utilizzo nell'ambito di piattaforme social o di commercio elettronico; e le Wearable Technology (828 milioni di euro, +6,7%) che, integrate a soluzioni digitali, supportano attività di assistenza tecnica, manutenzione, sicurezza fisica oltre che soluzioni legate al mondo della sanità e del wellness. Nel secondo sottogruppo si trovano l'Intelligenza artificiale (422 milioni di euro, 21,7%), che abilita scenari innovativi di analisi e interpretazione dei dati nelle più disparate aree business e si applica all'automazione intelligente dei processi; e la Blockchain (43 milioni di euro, +26,5%), il cui valore è riconosciuto in tutti quegli ambiti in cui la certificazione e la notarizzazione sono importanti (caratteristiche chimico-fisiche di prodotti industriali, identità digitali e non, competenze professionali, ecc.) e nel mondo bancario, dove alcune iniziative di sistema, unitamente ad ambiti specifici di applicazione, ne stanno sostenendo la crescita.

Figura 4:

Dimensione e trend dei Digital Enabler, previsioni 2022-2025



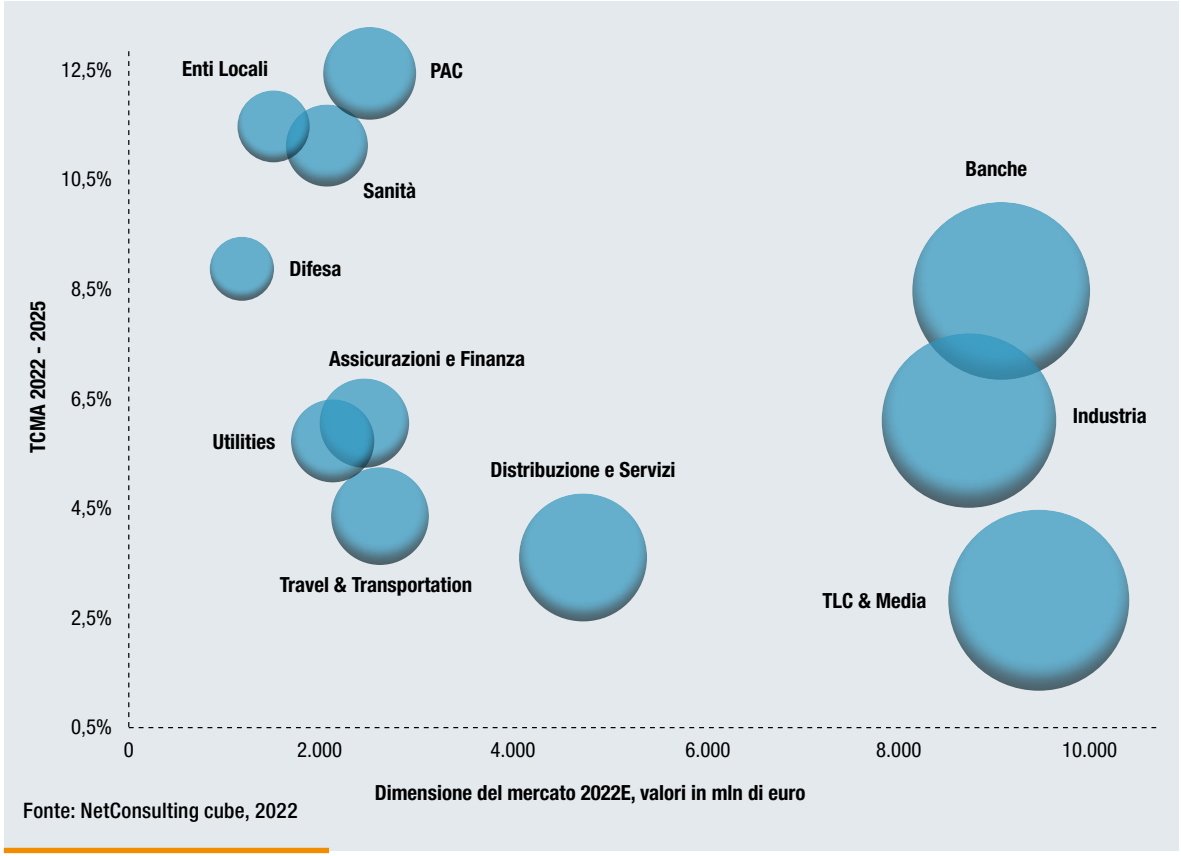
Fonte: NetConsulting cube, 2022

Previsioni per settori d'utenza: 2022-2025

Nel periodo 2022-2025 proseguirà la crescita della domanda digitale della componente business (aziende e amministrazioni), trasversale a tutti i settori (Fig. 5).

Figura 5:

La domanda digitale per settore di utenza, previsioni 2022-2025



Fonte: NetConsulting cube, 2022

La forte spinta alla digitalizzazione dei servizi e la consapevolezza che gli investimenti sul digitale comportino un vantaggio dal punto di vista competitivo stanno sostenendo i piani evolutivi di aziende e Pubblica Amministrazione. Gli investimenti si stanno concentrando, come già evidenziato, sulle principali tecnologie che abilitano la trasformazione digitale: Cloud, Cybersecurity e Big Data sono i principali ambiti di spesa, accompagnati da progetti di modernizzazione architetturale e applicativa. L'impatto del PNRR sull'andamento della spesa digitale delle aziende sarà più intenso a partire dal 2024, soprattutto nei settori della Pubblica Amministrazione, sanità e industria.

Nel settore industriale permane una situazione di incertezza. Le motivazioni sono principalmente di tipo esogeno alle imprese e vanno imputate in gran parte all'aumento dei costi dell'energia, all'inflazione, all'aumento dei tassi, allo shortage di materie prime e ad un'attuazione parziale del PNRR che, ad oggi, ha visto gli investimenti concentrarsi verso progetti legati alla componente materiale della transizione 4.0 piuttosto che a quella immateriale più strettamente riconducibile alla digitalizzazione delle aziende.

La spesa digitale nel settore industriale si posizionerà, alla fine del 2022, a 8.792,5 miliardi di euro, in aumento del 3% rispetto al 2021 (Tab. 5).

Tra gli ambiti progettuali digitali maggiormente indirizzati spiccano le soluzioni di Cybersecurity, in particolare relative al rafforzamento della sicurezza perimetrale e all'introduzione di procedure di Security Governance, le strategie di Data Strategy che si concretizzano in attività di BI di tipo tradizionale piuttosto che verso soluzioni di Advanced Analytics

e le soluzioni per migliorare la visibilità end-to-end dei processi logistici e di Supply Chain.
L'ambito legato alla Smart Factory è trainato dall'Industrial IoT e da soluzioni di Predictive Maintenance. Molte aziende industriali hanno fatto leva sull'e-commerce per migliorare il loro approccio alla multicanalità. Sta proseguendo infine l'adozione del Cloud Computing, sia per le componenti applicative (anche ERP) che per quelle più prettamente infrastrutturali e di piattaforma.
Per le Banche, la previsione è di una domanda digitale in crescita del 5,6% nel 2022 e un mercato che raggiungerà gli 9.129 milioni di euro, per poi crescere ulteriormente del 7% nel 2023. Il settore ha proseguito a investire sul digitale come leva per la trasformazione dei modelli di business e operativi. Le banche italiane, dopo aver dimostrato una intensa resilienza nel periodo pandemico, puntando sul digitale per garantire continuità di servizio alla clientela, nel 2022 hanno acquisito una maggiore consapevolezza delle potenzialità del digitale per supportare le proprie strategie e dell'esigenza di rinnovare le proprie architetture per innovare modelli organizzativi e per competere in uno scenario di mercato caratterizzato da forte evoluzioni e sfide crescenti. La transizione al Cloud e l'evoluzione delle architetture dati e degli Analytics compaiono all'interno dei piani strategici delle principali banche italiane. La trasformazione della relazione con il cliente verso un modello ibrido impone anche un continuo rafforzamento della Cybersecurity, per poter garantire un accesso sicuro ai servizi bancari e nello stesso tempo una Customer Experience ottimale. La modernizzazione applicativa rimane uno dei principali ambiti di investimento, oggetto di progetti pluriennali, guidati sia dall'esigenza di rinnovare applicazioni per renderle più rispondenti alla maggiore flessibilità, che il crescente utilizzo di canali digitali richiede, sia dalla transizione al Cloud che comporta necessariamente un rinnovo di applicazioni o la conteinerizzazione delle stesse per renderle Cloud Ready.
Per il settore Assicurazioni e Finanza la domanda digitale nel 2022 è prevista in crescita del +4,7% (per un valore pari a 2.433 milioni di euro), e del 5,3% nel 2023 (2.563 milioni). La digitalizzazione della relazione con il cliente, in tutte le fasi del rapporto contrattuale, unitamente all'automazione dei processi, in particolare nella gestione dei sinistri e nelle attività legate alla sottoscrizione delle polizze per supportare la crescente diffusione di modelli ibridi, rappresentano il principale ambito di investimento. Analogamente a quanto osservato nel settore bancario, anche nelle compagnie assicurative crescono gli investimenti in Cybersecurity.
L'attenzione ai dati, sia nella gestione della Data Privacy sia in quella della Data Analytics, rappresenta sempre più una priorità, anche se qualità del dato, cultura aziendale e carenza di competenze limitano la capitalizzazione degli investimenti.
La transizione al Cloud comincia ad essere intrapresa da un crescente numero di compagnie, sebbene con una velocità di adozione inferiore a quanto si osserva nelle banche. In forte aumento è l'evoluzione verso un modello data-driven e l'applicazione dell'Intelligenza artificiale sia in ambiti operativi che a supporto della vendita e dello sviluppo di prodotti. Infine, l'evoluzione di ecosistemi è sempre più abilitata dal digitale, con la costruzione di filiere estese nel mondo dell'Health, dell'Automotive e della Mobility, dell'Energy e altri ancora.
La spesa della Pubblica Amministrazione Centrale (PAC) sta proseguendo nella sua crescita a ritmi sostenuti, con un incremento previsto nel 2022 del 10,5% (in aumento anche rispetto alle previsioni dello scorso anno) e un valore del mercato che dovrebbe raggiungere 2.489,5 milioni di euro a fine anno. La PAC si conferma il settore con le migliori performance in termini di dinamica del mercato digitale.
Nella Pubblica Amministrazione Locale, la crescita attesa è del 9,4% (anche in questo caso, un dato più positivo rispetto alle previsioni espresse lo scorso anno), a 1.486 milioni di euro, una crescita che si prevede possa proseguire agli stessi ritmi nel 2023.
In entrambi i mercati l'incremento della spesa e degli investimenti digitali è sostenuto dal PNRR, che assegna alla digitalizzazione della Pubblica Amministrazione il 27% delle risorse complessive.
Tuttavia, pur essendoci stati progressi importanti in termini di diffusione delle piattaforme abilitanti Pago PA, IO, SPID e CIE (Carta d'Identità Elettronica) e pur avendo già allocato attraverso la piattaforma PA Digitale 2026 circa 1,8 miliardi di euro, si riscontra un ritardo rispetto all'avvio dei progetti, dovuto da una parte alla carenza di competenze presso le PA Locali e dall'altra alle rigidità burocratiche per gestire l'approvazione dei fondi.
La Strategia Italia Digitale 2026, formulata nel 2021 per supportare i progetti, in modo orchestrato tra le diverse Pubbliche Amministrazioni, relativi alla transizione digitale, sosterrà la crescita del mercato digitale della PA puntando sulla realizzazione dei seguenti obiettivi:
• l'adozione da parte di PA Locali e Centrali di in-

frastrutture Cloud sicure, moderne ed efficienti, uscendo dalla logica di un utilizzo on premise di centri elaborazione dati locali, piccoli, costosi e ad alto rischio di pirateria informatica. In questo senso un primo passo importante è rappresentato dalla costituzione della società per la realizzazione di un Polo Strategico Nazionale contenente dati e applicazioni critiche di PA e aziende sanitarie;

- l'attivazione di tutte le anagrafi dati nazionali previste, le principali delle quali sono l'Anagrafe nazionale della popolazione residente (Interno), l'Anagrafe degli assistiti (MEF), l'Anagrafe nazionale dell'istruzione (Istruzione), l'Anagrafe nazionale dell'istruzione superiore (MUR) e l'Anagrafe dei dipendenti pubblici (PA);
- la realizzazione di una piattaforma di interoperabilità per lo scambio e integrazione dei dati in modalità sicura: la c.d. Piattaforma Digitale Nazionale Dati (PDND), per consentire alle PA di scambiarsi dati automaticamente senza chiedere al cittadino di fornire più volte informazioni già disponibili;
- l'erogazione di servizi della PA attraverso sistemi di identità digitale quali SPID e CIE, e l'assegnazione di un domicilio digitale, garantendo la trasmissione e la consegna di comunicazioni e notifiche digitali, in tempi certi e con notevoli risparmi di costo, attraverso la Piattaforma Notifiche e il wallet digitale in App IO;
- l'esposizione di attributi digitali, certificati direttamente sui dispositivi dei cittadini, verificabili e aggiornabili in tempo reale (per esempio patente, certificati e permessi).

Nella Difesa, anch'essa destinataria di fondi PNRR, la domanda digitale registrerà una crescita del 6,5% nel 2022, per un valore di 1.161 milioni di euro, e del 7,7% nel 2023, attestandosi a 1.250 milioni di euro. La Cybersecurity rappresenterà uno dei principali driver di investimento: lo spazio cibernetico deve essere sempre più protetto, rientrando ormai a pieno titolo nei target d'attacco da parte di governi stranieri, con un ruolo coordinato tra ACN e Ministero della Difesa per difendere le infrastrutture critiche nazionali.

Tabella 3:

Bandi aperti (*) per la realizzazione del PNRR

MISSIONE 1 - Digitalizzazione, innovazione, cultura e turismo

Data scadenza	Data pubblicazione su OReP	Tipologia bando
30/11/22	02/11/22	Avviso dell'Agenzia per la Cybersicurezza nazionale n.5/2022 per l'erogazione di contributi per l'attivazione di laboratori di prova per l'area di accreditamento software e network (Missione 1, Componente 1, Investimento 1.5)
25/11/22	14/09/22	Avviso "Adozione appIO" Comuni (Missione 1, Componente 1, Investimento 1.4.3)
25/11/22	14/09/22	Avviso "Adozione piattaforma pagoPA" Comuni (Missione 1, Componente 1, Investimento 1.4.3)
25/11/22	14/09/22	Avviso "Estensione dell'utilizzo delle piattaforme nazionali di identità digitale – SPID CIE" Comuni (Missione 1, Componente 1, Investimento 1.4.4)
17/11/22	19/10/22	Gara da 18,6 milioni per la digitalizzazione dei depositi museali (Missione 1, Componente 3, Investimento 1.1.5)
13/01/23	14/09/22	Avviso "Adozione appIO" per altri Enti pubblici (Missione 1, Componente 1, Investimento 1.4.3
13/01/23	14/09/22	Avviso "Adozione piattaforma pagoPA" altri Enti (Missione 1, Componente 1, Investimento 1.4.3)
13/01/23	14/09/22	Avviso "Estensione dell'utilizzo delle piattaforme nazionali di identità digitale – SPID CIE" Amministrazioni Pubbliche diverse da Comuni e Istituzioni Scolastiche (Missione 1, Componente 1, Investimento 1.4.4)
01/02/23	21/10/22	Avviso pubblico MIC "Capacity building per gli operatori della cultura per gestire la transizione digitale e verde" azione A II (Missione 1, Componente 3, Investimento 3.3.2)
17/02/23	24/10/22	Avviso per i Comuni per l'adesione alla Piattaforma Digitale Nazionale Dati (Missione 1, Componente 1, Investimento 1.3.1)
30/09/25	23/09/22	Avviso pubblico del MITUR per la Digitalizzazione di agenzie e tour operator (Missione 1, Componente 3, Investimento 4.2.2)

MISSIONE 3 - Infrastrutture per una mobilità sostenibile

Data scadenza	Data pubblicazione su OReP	Tipologia bando
21/11/22	21/10/22	Gara da 22,4 milioni di euro per i Servizi di connettività per il monitoraggio di Ponti, Viadotti e Sovrappassi di ANAS, inclusi i servizi di realizzazione e manutenzione dell'infrastruttura di rete, assistenza specialistica e progettuale ad hoc (Missione 3, Componente 1, Fondo complementare)
28/11/22	21/10/22	Gara da 37,7 milioni di euro per i Servizi per la messa a disposizione e l'erogazione di una piattaforma per il monitoraggio dinamico delle opere d'arte (Missione 3, Componente 1, Fondo complementare)

MISSIONE 6 - Infrastrutture per una mobilità sostenibile

Data scadenza	Data pubblicazione su OReP	Tipologia bando
01/12/22	24/10/22	Avviso di dialogo competitivo per l'affidamento della piattaforma di intelligenza artificiale per l'assistenza sanitaria (Missione 6, Componente 1)

Fonte: Osservatorio Recovery Plan

(*) al 14 novembre 2022

Tabella 4:

Bandi chiusi (*) per la realizzazione del PNRR

MISSIONE 1 - Digitalizzazione, innovazione, cultura e turismo

Data scadenza	Data pubblicazione su OReP	Tipologia bando
14/11/22	12/10/22	Gara da 16,9 mln di euro per la digitalizzazione degli archivi fotografici delle soprintendenze archeologia, belle arti e paesaggio (Missione 1, Componente 3, Investimento 1.1.5)
07/11/22	05/10/22	Gara da 27,9 milioni di euro per la digitalizzazione del patrimonio culturale – digital library (Missione 1, Componente 3, Investimento 1.1.5)
12/10/22	26/09/22	MITUR: avvio e accesso alla piattaforma online per "Digitalizzazione agenzie e tour operator" (Missione 1, Componente 3, Investimento 4.2.2)
31/10/22	16/09/22	Avviso pubblico per le attività di valorizzazione dei brevetti promosse dalle Università, dagli Enti pubblici di ricerca e dagli IRCCS attraverso i progetti PoC- proof of concept (Missione 1, Componente 2, Riforma 1)
20/09/22	15/09/22	Accordo Quadro multilaterale con più fornitori per l'affidamento dei servizi di digitalizzazione dei microfilm di manoscritti del Centro Nazionale per lo Studio del Manoscritto conservati presso la Biblioteca Nazionale Centrale di Roma (9,2 milioni/EUR – Missione 1, Componente 3, Sub-Investimento 1.1.5)
21/10/22	15/09/22	Avviso di proroga al 21 ottobre per la presentazione delle candidature "Esperienza del cittadino nei servizi pubblici-Scuola" (Missione 1, Componente 1, Investimento 1.4.1)
21/10/22	15/09/22	Avviso di proroga al 21 ottobre per la presentazione delle candidature "Abilitazione al Cloud per le PA-Scuole" (Missione 1, Componente 1, Investimento 1.2)
11/10/22	14/09/22	Avviso "Piattaforme Notifiche Digitali" per i Comuni (Missione 1, Componente 1, Investimento 1.4.5)
27/09/22	01/09/22	Bando MISE Brevetti + 2022
30/09/22	01/09/22	Avviso dell'Agenzia per la cybersicurezza per interventi di potenziamento della resilienza cyber (Missione 1, Componente 1, Investimento 1.5)

MISSIONE 2 - Rivoluzione verde e transizione ecologica

Data scadenza	Data pubblicazione su OReP	Tipologia bando
19/05/22	16/03/22	Avviso MIMS – Procedure per la presentazione delle proposte per interventi finalizzati alla riduzione delle perdite nelle reti di distribuzione dell'acqua, compresa la digitalizzazione e il monitoraggio delle reti (900 milioni/EUR – Missione 2, Componente 4, Investimento 4.2)

MISSIONE 3 - Infrastrutture per una mobilità Sostenibile

Data scadenza	Data pubblicazione su OReP	Tipologia bando
30/09/21	10/11/21	Avviso di gara per la progettazione, implementazione e realizzazione di un Sistema di "MONITORAGGIO DINAMICO" per il controllo da remoto di ponti, viadotti, tunnel ed opere geotecniche di sostegno, di Sistemi Tecnologici "SMART ROAD" e di una "STAZIONE CENTRO DI CONTROLLO" di elaborazione, gestione e monitoraggio dei dati per le AUTOSTRADE A24 e A25 (M3C1 Fondo Complementare)

Fonte: Osservatorio Recovery Plan

(*) al 14 novembre 2022

MISSIONE 4 - Istruzione e Ricerca

Data scadenza	Data pubblicazione su OReP	Tipologia bando
26/10/22	14/10/22	Avviso pubblico n.84750 del MUR per i poli di formazione alla transizione digitale del personale scolastico (Missione 4, Componente 1, Investimento 2.1)
24/02/22	31/12/21	Avviso MUR da 1,3 miliardi per gli ecosistemi dell'innovazione territoriale (Missione 4, Componente 2, Investimento 1.5)
10/03/22	29/12/21	Avviso MUR n. 3265 da 500 milioni per la creazione o l'ammodernamento di almeno 10 Infrastrutture Tecnologiche di Innovazione (Missione 4, Componente 2, Investimento 3.1)

MISSIONE 6 - Salute

Data scadenza	Data pubblicazione su OReP	Tipologia bando
14/11/22	13/10/22	Piattaforma Nazionale di Telemedicina: pubblicata la procedura per l'affidamento (Missione 6, Componente 1, Investimento 1.2.3)
19/08/22	24/06/22	Avviso pubblico MUR per la concessione di finanziamenti destinati ad iniziative di ricerca per tecnologie e percorsi innovativi in ambito Sanitario e Assistenziale (Missione 6, Componente 2, Piano Complementare)
06/06/22	09/05/22	Gara a procedura aperta per la conclusione di un Accordo Quadro, avente ad oggetto l'affidamento di servizi applicativi e l'affidamento di servizi di supporto in ambito "Sanità digitale – Sistemi informativi gestionali" per le PA del SSN (Missione 6, Componente 2)
19/05/22	19/04/22	Gara comunitaria centralizzata a procedura aperta finalizzata all'acquisizione di acceleratori lineari per le aziende sanitarie e ospedaliere IFO, San Giovanni Addolorata, Roma 1, Viterbo, Frosinone (M6C2I1.1.2)
18/05/22	23/03/22	Avviso per la manifestazione di interesse per la presentazione di proposte di Partnership Pubblico Privato per l'affidamento in concessione per la "Progettazione, realizzazione e gestione dei Servizi abilitanti della Piattaforma nazionale di Telemedicina PNRR" (Missione 6, Componente 1, Sub-Investimento 1.2.3)
12/07/21	15/01/22	Gara CONSIP a procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l'affidamento di servizi applicativi e l'affidamento di servizi di supporto in ambito "Sanità digitale – sistemi informativi clinico-assistenziali" per le pubbliche amministrazioni del SSN (Prima gara di Sanità Digitale – 600 milioni/EUR – Missione 6, Componente 2, Investimento 1.3)
31/01/22	14/01/22	Gara CONSIP a procedura aperta per la conclusione di un Accordo Quadro, per l'affidamento di servizi applicativi e servizi di supporto in ambito "Sanità digitale – Sistemi informativi sanitari e servizi al cittadino" per le Pubbliche Amministrazioni del SSN (Seconda gara di Sanità digitale – 540 milioni/EUR – Missione 6, Componente 2, Investimento 1.3)

Fonte: Osservatorio Recovery Plan

(*) al 14 novembre 2022

Per il settore della Sanità si riscontra un incremento del mercato digitale dell'8,8%, passando da 1.869,5 milioni del 2021 a 2.034,1 milioni del 2022, con un trend in leggera contrazione rispetto al biennio precedente, che registrava una crescita del 9,6%. Si stima inoltre un'ulteriore crescita del mercato per il 2023 (+10,5%, pari a 2.248,5 milioni). A trainare la crescita del mercato digitale in ambito sanitario sono gli investimenti previsti dall'obiettivo 6 del PNRR. Le azioni strategiche si concentrano su Fascicolo Sanitario Elettronico, Cartella Clinica Elettronica Ospedaliera, Telemedicina e Cloud Computing, con una crescente attenzione alla Cybersecurity, oltre che sulla componente più digitale dei dispositivi medici – quali apparati medicali e robotica chirurgica connessi ed equipaggiati da sistemi per la raccolta e l'analisi dei dati, con tool di intelligenza artificiale o augmented reality – e sul Business Process Outsourcing. Un mercato quindi in crescita, nonostante le criticità dovute ai ritardi nella produzione e nella supply chain di materiali e materie prime e ai maggiori costi dell'energia.

In generale si riscontra un processo di adeguamento ai capisaldi della modernizzazione, che pervade l'intero sistema sanità.

La spesa digitale nel settore delle Utility è valutata in crescita anche nel 2022, sebbene in rallentamento rispetto alle performance registrate nel 2021. Il mercato dovrebbe raggiungere i 2.110,8 milioni di euro a fine 2022, rispetto ai 2.034,6 del 2021, con un incremento del 3,7%. Influiscono sul rallentamento l'aumento dei prezzi dell'energia e i maggiori rischi da NPL (per copertura e credito), gli interventi regolatori (price cap e svincolo del prezzo dell'energia da quello del gas) e la ricerca di fonti alternative di approvvigionamento per la piena transizione energetica ed elettrificazione, come promosso da UN Sustainable Development Goal ed European Green Deal. Nel corso dell'anno e, soprattutto, nella seconda parte dell'anno l'attenzione delle aziende del settore si è concentrata sulla modernizzazione dei processi e sul recupero delle efficienze, senza tuttavia dimenticare la cura del cliente. I progetti riguardano sia la modernizzazione applicativa, anche attraverso la realizzazione di piattaforme a micro servizi, che un impiego più intensivo e capillare del Cloud, a livello infrastrutturale ed applicativo (anche e soprattutto verso il CRM) per rendere l'azienda agile e flessibile nella capacità di rispondere alle evoluzioni del contesto. Unitamente, forte è l'attenzione agli investimenti per la digitalizzazione delle reti, agli Smart Meter, per la raccolta del conferito agli stabilimenti di produzione dell'energia, per attività di manutenzione predittiva delle reti di distribuzione e impianti e di asset management. In diversi casi si inizia a vedere il fiorire di soluzioni di Digital Twin per la creazione di modelli di simulazione del funzionamento di stabilimenti e reti di distribuzione di gas ed energia. Una considerazione crescente è riservata agli investimenti in BI/Analytics per la realizzazione di un'architettura di data management che garantisca qualità dei dati a tutti i livelli d'azienda e abiliti la formulazione di scenari. Fondamentali e continui sono gli investimenti in Cybersecurity, considerati anche gli attacchi subiti durante l'estate, volti a costruire una security by design davvero a tutti i livelli, incluse le componenti di Network e IOT. Con progetti indirizzati alla Identity Governance, al rafforzamento delle soluzioni di Disaster Recovery e Business Continuity.

Nel corso del 2022, il settore Telecomunicazioni e Media arriverà ad una spesa digitale complessiva di 9.510 milioni di euro, con una crescita pari all'1,5%, fortemente rallentata rispetto agli anni precedenti. La spesa si sta distribuendo su più fronti ma è polarizzata su due filoni prevalenti. Da un lato l'esigenza di estendere l'infrastruttura di comunicazione sul territorio nazionale, con la necessità di mantenere un elevato flusso di investimenti. Dall'altro, l'esigenza di accelerare il processo di ammodernamento delle dotazioni tecnologiche che è stato più volte rinviato e che si rende necessario ancor più in questo particolare momento storico, in cui mantenere sistemi datati può costituire un dispendio di risorse. Per quanto riguarda le specifiche aree tecnologiche oggetto dei progetti più rilevanti, si conferma la tendenza ad aumentare in modo significativo l'utilizzo di architetture Cloud – in particolare in presenza di refresh tecnologico – in aggiunta all'incremento dello sfruttamento di soluzioni di Business Intelligence finalizzate ad intercettare in modo più efficace le esigenze dei clienti (Media) oltre che a prevenire l'intenzione a cambiare il fornitore (Telco).

Nel settore Distribuzione e Servizi le stime prevedono una crescita del mercato digitale pari al 2,8%, in rallentamento rispetto alle previsioni di inizio anno e ancor più rispetto al 7,1% registrato nel 2021, per un valore atteso nel 2022 di 4.736 milioni di euro.

Già da agosto le tensioni inflattive, unitamente al costo dell'energia, dei trasporti e dei canoni di affitto, alle tensioni sulla supply chain e la riduzione della propensione al consumo da parte dei clienti hanno comportato una progressiva riduzione della marginalità da parte degli operatori.

L'attenzione, pertanto, si sta concentrando sull'ot-

timizzazione dei costi, l'orchestrazione dei canali, l'integrazione dei processi e relazione di filiera e supply chain, la creazione di un modello fisico-virtuale (phygital di vendita) supportato da un servizio di delivery veloce e puntuale. In un quadro di sostenibilità che coniuga le ovvie esigenze di risparmio energetico ad un approccio circolare che investe gli store, i prodotti ed i servizi offerti.

Gli investimenti indirizzano la omnicanalità (everywhere retail-commerce): CRM integrato, chioschi digitali, gestione code, sistema di cassa evoluti, pop-up/flagship store, advertising geolocalizzato, click&collect, soluzioni di shop&play. Con la realizzazione di una effettiva Customer Data Strategy (collection, analysis, execution) per l'analisi comportamentale del journey omnicanale. Gli investimenti in Cloud (in tutte le componenti) abilitano le esigenze di velocità e supporto ai processi delle aziende. Non ultimi sono i crescenti investimenti in Cybersecurity per contrastare furti di dati e indisponibilità del servizio.

A fine 2022, la spesa digitale del settore Travel & Transportation dovrebbe raggiungere i 2.596,5 milioni di euro grazie ad una crescita del 3,4%. Nel 2023, la spesa del settore crescerà ulteriormente e sfiorerà quota 2.700 milioni (+3,3%). Dopo un biennio di forti difficoltà e di calo della domanda (in particolare nel comparto passeggeri), il settore sta tornando ad investire a supporto dell'ottimizzazione dei processi business, soprattutto in ambito Operations e Customer Service, Marketing e Vendite. Ciò si sta traducendo nell'esigenza di rendere disponibili e di valorizzare i dati (BI e Reporting, Advanced Analytics), proteggendoli adeguatamente, insieme alle infrastrutture IT che li ospitano (Cybersecurity), nell'adozione di applicazioni business e nella loro modernizzazione. Gli investimenti in ambito applicativo riguardano, da un lato, l'adozione di soluzioni tecniche/core business evolute che abilitano una gestione più intelligente delle attività in un'ottica di smart enterprise, grazie all'integrazione di funzionalità mutuate dai più recenti paradigmi digitali, in primis Cloud e IoT (Smart Warehouse Management, Smart Transport Management etc.); dall'altro, le aziende continuano a lavorare all'implementazione di soluzioni in ambito Digital Customer, a supporto del raggiungimento degli obiettivi commerciali (tematica importante soprattutto per le realtà B2C), e di piattaforme di Digital Employee, anche se i progetti in questo campo sono caratterizzati da una strategicità in graduale calo.

Tabella 5:

Il mercato digitale in Italia nei settori economici, 2021-2025E

Dati in mln di euro	2021	2022E	2023E	2024E	2025E	22E/21	23E/22E	24E/23E	25E/24E	TCMA 22/25
Industria	8.533,9	8.792,5	9.109,2	9.679,6	10.508,8	3,0%	3,6%	6,3%	8,6%	6,1%
Banche	8.647,4	9.129,0	9.766,8	10.719,0	11.671,2	5,6%	7,0%	9,7%	8,9%	8,5%
Assicurazioni e finanziarie	2.324,6	2.433,8	2.563,0	2.733,2	2.903,3	4,7%	5,3%	6,6%	6,2%	6,1%
PAC	2.252,9	2.489,5	2.778,2	3.133,9	3.541,3	10,5%	11,6%	12,8%	13,0%	12,5%
Difesa	1.090,0	1.160,9	1.250,2	1.362,8	1.499,0	6,5%	7,7%	9,0%	10,0%	8,9%
Enti locali	1.358,6	1.486,0	1.629,4	1.820,6	2.059,4	9,4%	9,7%	11,7%	13,1%	11,5%
Sanità	1.869,5	2.034,1	2.248,5	2.495,8	2.795,3	8,8%	10,5%	11,0%	12,0%	11,2%
Utilities	2.034,6	2.110,8	2.221,5	2.360,1	2.498,6	3,7%	5,2%	6,2%	5,9%	5,8%
Telecomunicazioni & Media	9.368,2	9.510,0	9.750,0	9.980,0	10.342,0	1,5%	2,5%	2,4%	3,6%	2,8%
Distribuzione e Servizi	4.607,3	4.736,3	4.873,6	5.060,0	5.268,6	2,8%	2,9%	3,8%	4,1%	3,6%
Travel & Transportation	2.510,7	2.596,5	2.682,4	2.811,5	2.953,1	3,4%	3,3%	4,8%	5,0%	4,4%
Consumer	30.689,3	30.356,7	30.265,4	30.752,9	31.286,8	-1,1%	-0,3%	1,6%	1,7%	1,0%
Totale Mercato Digitale	**75.287,0**	**76.835,9**	**79.138,4**	**82.909,2**	**87.327,5**	**2,1%**	**3,0%**	**4,8%**	**5,3%**	**4,4%**

Stato di avanzamento degli investimenti del PNRR con elevato contenuto digitale

Le misure previste dal Piano Nazionale di Ripresa e Resilienza si articolano intorno a tre assi strategici condivisi a livello europeo: digitalizzazione e innovazione, transizione ecologica, inclusione sociale.
Seguendo le linee guida elaborate dalla Commissione Europea, inoltre, il Piano raggruppa i progetti di investimento e di riforma in 16 Componenti, raggruppate a loro volta in 6 Missioni: 1. Digitalizzazione, innovazione, competitività, cultura e turismo; 2. Rivoluzione verde e transizione ecologica; 3. Infrastrutture per una mobilità sostenibile; 4. Istruzione e ricerca; 5. Coesione e inclusione; 6. Salute.
Il Governo ha richiesto all'Unione Europea il massimo delle risorse disponibili per l'Italia, pari a 191,5 miliardi di euro, di cui 68,9 miliardi in sovvenzioni e 122,6 miliardi in prestiti. Di questi, sono 48 i milioni di euro destinati alla transizione digitale, pari al 25,1% delle risorse totali richieste, più del doppio rispetto al secondo Paese per investimenti in transizione digitale, la Germania, che vi destina quasi 20 milioni di euro.
In Europa sono 109 i miliardi destinati alla Transizione Digitale, di cui il 44% destinati all'Italia, un valore molto più elevato rispetto al valore medio degli altri Stati che si aggira intorno al 6%.
Considerando l'importo complessivo di fondi europei pari a 412 miliardi di euro, l'11% sarà utilizzato dall'Italia, contro un valore medio degli altri Stati dell'1,6%.
Al 31 agosto 2022 sono 11.794 i miliardi di euro effettivamente spesi, che rappresentano il 7% dei fondi stanziati: l'area digitalizzazione pesa per l'1%, con 128 milioni di euro spesi (Tab. 6).
Nella NADEF di fine settembre è stato dichiarato che la spesa effettivamente erogata al termine dell'anno sarà in linea con le previsioni, arrivando quindi a 15 miliardi di euro per il 2022, a cui vanno sommati i 5,5 dell'anno precedente, per un totale di 21 miliardi complessivi.
La NADEF ha evidenziato ritardi nella capacità di spesa da parte dello Stato con possibili ripercussioni nell'approvvigionamento di soluzioni e risorse per i beneficiari finali. Tale lentezza può essere attribuita all'impennata dei costi delle materie prime e dell'energia e ai tempi di adattamento alle procedure innovative del PNRR. Nonostante ciò, l'Italia non è in ritardo sul PNRR e il cronoprogramma al momento è rispettato. Grazie a questo fattore, l'Europa, dopo il primo anticipo di 24,9 mi-

Tabella 6:

Spese sostenute al 31 agosto 2022, per missione e componente

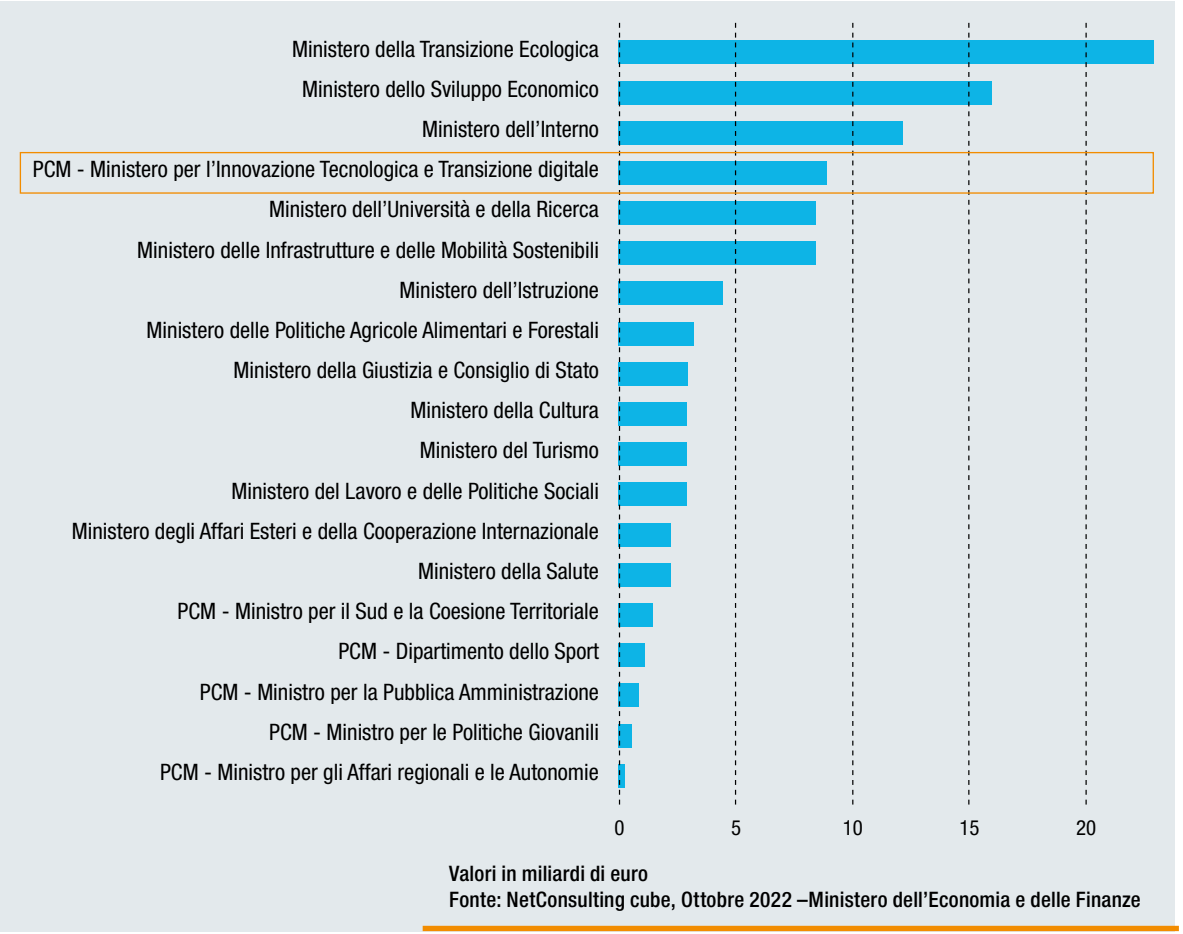
Linee di intervento	Spese sostenute
Infrastrutture e trasporti	3.617
Transizione 4.0	2.965
Ecobonus - Sismabonus	2.774
Resilienza e valorizzazione dei territori comunali	1.200
Scuole innovative - Sicurezza edifici scolastici	396
Rifinanziamento fondo SIMEST	398
Gestione risorse idriche - Riduzione rischio idrogeologico	181
Digitalizzazione	128
Altro	90
Totale	**11.790**

Valori in milioni di euro — Fonte: NetConsulting cube, Ottobre 2022 – Ministero dell'Economia e delle Finanze – sistema ReGiS

liardi di euro, ha elargito due rate semestrali da 21 miliardi ciascuna.
La terza rata del 2022, pari a 19 miliardi, arriverà al raggiungimento dei 55 obiettivi nell'ultimo trimestre dell'anno, di cui 10 all'interno dell'area "Innovazione tecnologica".
Occorre tuttavia considerare che, soprattutto nella Pubblica Amministrazione, gran parte dei progetti, inclusa la transizione al Cloud, su cui si focalizza la Strategia Cloud nazionale, sono rallentati dalla complessità burocratica nell'accesso ai fondi e dai tempi che riguardano gli iter legati agli avvisi e all'emissione dei bandi.
Alla data del 5 ottobre sono 334 i bandi e gli avvisi emanati, distinti in quattro diverse tipologie (appalti pubblici, bandi per l'individuazione delle proposte progettuali, bandi per la selezione di esperti e contributi e crediti di imposta), per un importo complessivo di 94,7 miliardi di euro. Alla medesima data, 43 di queste procedure risultavano ancora aperte, per un valore di circa 32,3 miliardi di euro, con pagamenti, alla data del 31 agosto 2022, pari a 11,8 miliardi di euro, che si prevede arrivino a fine anno a 20,5/21 miliardi di euro, una cifra quindi inferiore rispetto a quanto previsto. Osservando la distribuzione di bandi e avvisi per l'amministrazione titolare, alla Presidenza del Consiglio, a cui fa capo il Dipartimento per l'innovazione digitale e al Ministro per l'Innovazione e la transizione digitale, fanno riferimento bandi per circa 9 miliardi di euro (Fig. 6).
Occorre sottolineare come molte misure per la transizione digitale entreranno nella fase attuativa nel secondo semestre del 2022:
• per la realizzazione del Polo Strategico Nazio-

Figura 6:

Avanzamento PNRR: importo dei bandi emanati per amministrazione titolare



Valori in miliardi di euro
Fonte: NetConsulting cube, Ottobre 2022 –Ministero dell'Economia e delle Finanze

nale (PSN), entro dicembre 2022 è previsto il completamento dell'infrastruttura del Polo, nella quale dovranno essere trasferiti i data center delle Pubbliche Amministrazioni, con l'attestazione della conclusione delle verifiche di quattro data center;

- ugualmente entro dicembre è previsto il rilascio della Piattaforma Digitale Nazionale Dati (PDND) per garantire l'interoperabilità dei sistemi informativi e delle basi di dati delle Pubbliche Amministrazioni e dei gestori di servizi pubblici, rispetto alla quale sono state approvate le linee guida sull'interoperabilità dei sistemi informativi e sono stati stipulati accordi di collaborazione con l'ISTAT e con il CNR per la realizzazione del Catalogo Nazionale Dati;
- con riferimento alla sicurezza informatica, dopo la costituzione, avvenuta lo scorso anno, dell'Agenzia per la Cybersicurezza Nazionale, si prevede che vengano realizzati almeno cinque interventi per migliorare le strutture di sicurezza cibernetica nell'ambito del PSNC (Perimetro di Sicurezza Nazionale Cibernetico) e dei NIS;
- nell'investimento che mira a migliorare l'efficienza dell'Istituto Nazionale per la Previdenza Sociale (INPS) e dell'Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro (INAIL) si prevede la messa a disposizione di ulteriori 35 servizi supplementari sul sito web istituzionale dell'INPS in vari ambiti istituzionali dell'Istituto (prestazioni pensionistiche, ammortizzatori sociali, indennità di disoccupazione, prestazioni d'invalidità, rimborsi, raccolta dei contributi da parte delle imprese, servizi per i lavoratori agricoli, servizi antifrode, anticorruzione e di trasparenza);
- infine, in ambito sanitario, entro la fine del 2022 si prevede la pubblicazione delle procedure di gara e degli accordi quadro Consip e la conclusione dei relativi contratti per l'acquisto di sistemi necessari per l'aggiornamento dei sistemi informativi delle strutture ospedaliere.

Scenari di previsione del mercato digitale e impatto del PNRR

L'andamento fino al 2025 del mercato digitale in Italia sarà condizionato in misura crescente dagli investimenti in ICT finanziati attraverso il PNRR. La valutazione dell'impatto effettivo del PNRR è tutt'altro che semplice, in quanto alcuni progetti nel comparto della Pubblica Amministrazione sono già oggetto di gare pubbliche anche se non è del tutto chiara la reale disponibilità delle risorse finanziarie previste dal Piano.
Inoltre, occorre tenere presente che non tutti gli investimenti ICT attuati tramite la disponibilità delle risorse del PNRR sono da considerare come mercato del tutto aggiuntivo. In parte bisogna considerare l'utilizzo di risorse PNRR anche per finanziare progetti e iniziative già previste in precedenza.
Nel prevedere un utilizzo massiccio delle risorse del PNRR, occorre inoltre tenere in considerazione alcuni assunti fondamentali:

- il consolidamento della ripresa economica che, almeno nel 2023, non è previsto in Italia;
- l'esecuzione delle riforme e la progressione degli

investimenti come da cronoprogramma del PNRR e l'effettivo e pieno utilizzo delle risorse previste per la trasformazione digitale;
- il raggiungimento di una situazione di ancora maggiore tranquillità sul piano pandemico.

Nel 2022 lo scenario prevede, a fronte di un mercato digitale di 76,1 miliardi di euro, un impatto del PNRR pari a 741 milioni aggiuntivi per un totale complessivo di oltre 76,8 miliardi di euro (Fig. 7).

Nel 2023 si prevede, a fronte di un mercato digitale di 77,1 miliardi di euro, un impatto del PNRR di 2 miliardi di euro, per un totale complessivo di oltre 79,1 miliardi e un incremento del 3% rispetto all'1,3% che si registrerebbe al netto del PNRR.

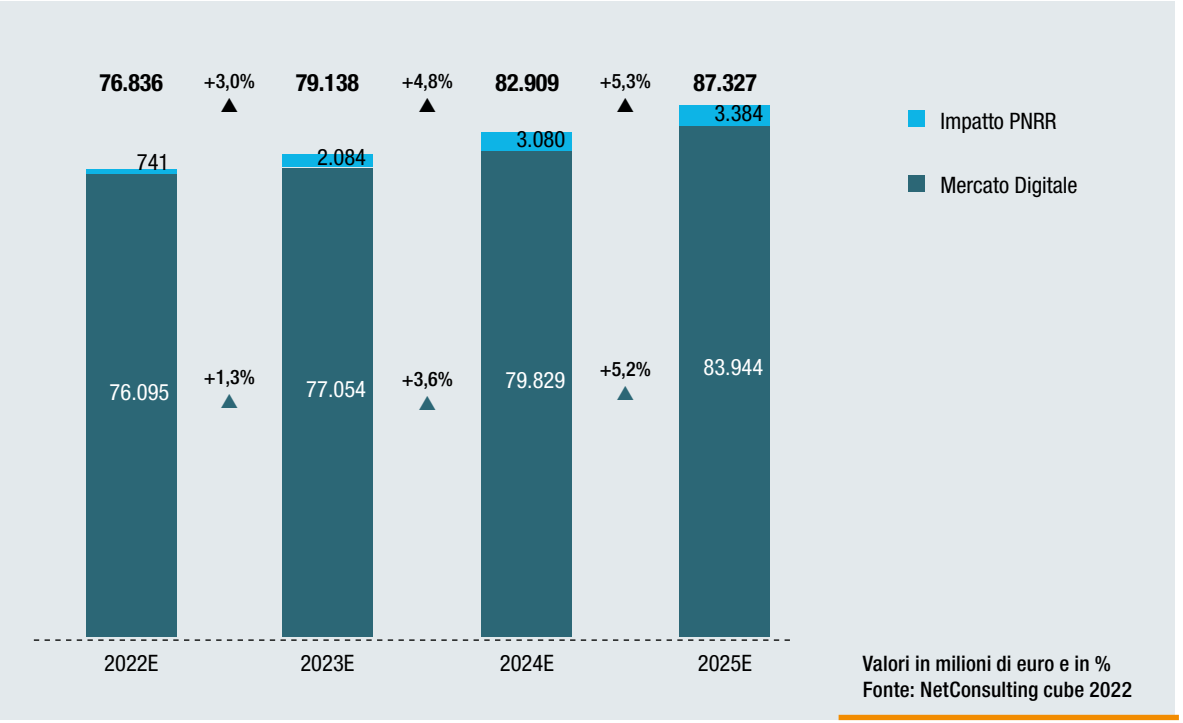
Nel 2024 lo scenario prevede, a fronte di un mercato digitale di 79,8 miliardi di euro, un impatto del PNRR pari a 3 miliardi aggiuntivi per un totale complessivo di oltre 82,9 miliardi di euro e un incremento del 4,8% rispetto al 3,6% che si registrerebbe al netto del PNRR.

Nel 2025 si prevede, a fronte di un mercato digitale di 83,9 miliardi di euro, un impatto del PNRR pari a 3,4 miliardi per un totale complessivo di oltre 87,3 miliardi di euro e un incremento del 5,3% rispetto all'anno precedente. Industria, Pubblica Amministrazione, Sanità e Telecomunicazioni saranno i settori che beneficeranno in modo diretto degli investimenti previsti dal Piano.

Come si evince dagli scenari delineati, i maggiori impatti del PNRR sul mercato digitale in Italia sono previsti negli anni 2024 e 2025, poiché l'accesso ai fondi comporta delle implicazioni di tipo burocratico che possono avere effetti sui tempi di avvio e di implementazione.

Figura 7:

L'impatto del PNRR sul mercato digitale secondo lo Scenario Base, 2022E-2025E



Valori in milioni di euro e in %
Fonte: NetConsulting cube 2022

CYBER-SECURITY E TRANSIZIONE DIGITALE

Gli attacchi informatici sono continuati a crescere numericamente, a livello globale, nel corso del 2022, rappresentando una seria minaccia per la trasformazione digitale in corso. Da una parte, sono proprio una diretta conseguenza della crescente digitalizzazione e della diffusione dello smart working, dall'altra, l'aumento può essere imputato anche all'esplosione del conflitto russo-ucraino. Aziende e Pubbliche amministrazioni sono pertanto particolarmente esposte e la sicurezza informatica è divenuta centrale nelle loro strategie. Il trend del mercato Cybersecurity risulta in forte espansione. Il Barometro Cybersecurity 2022 analizza quali siano le principali tecniche di attacco, gli obiettivi di tali attacchi, gli strumenti, sia tecnici che organizzativi, per difendersi e le lacune che le aziende devono colmare. Infine, un ruolo importante per la difesa e la gestione lo avranno anche la normativa e la strategia di Cybersicurezza nazionale.

Numero di attacchi informatici gravi nel primo semestre 2022:

1.169

+8,4%
rispetto al primo semestre 2021

Il mercato della Cybersecurity in Italia nel 2022:

1.576 milioni di euro

+13%
rispetto al 2021

I malware rappresentano la principale tecnica di attacco

L'Italia è al primo posto in Europa per attacchi ransomware

Andamento della spesa in Cybersecurity per settori (TCMA 2022-2025):

- **Sanità** + 20%
- **Pubblica Amministrazione** + 19%

I principali obiettivi degli attacchi informatici:

- **Pubblica Amministrazione** 24,2%
- **Digital Service Provider** 13,1%
- **Consumatori e general public** 12,4%

Le principali priorità in ambito Cybersecurity per imprese e PA:

1. Attività di formazione e/o awareness del personale
2. Incremento delle risorse interne ed esterne
3. Incremento/adozione di logiche di Security by Design

CYBER POWER E SOVRANITÀ: NUOVI SCENARI

di Fabio Rugge
Vice Rappresentante Permanente d'Italia, Consiglio Atlantico
Senior Associate Research Fellow, ISPI

Lo sviluppo di internet e delle tecnologie digitali caratterizza la nostra era. È attraverso lo spazio cibernetico che il cittadino forma le proprie opinioni e realizza la sua socialità, si promuove la crescita e l'innovazione delle aziende, si trasformano in ogni ambito i processi di produzione, di interazione e di scambio. Sono passati circa trent'anni dalla nascita di internet, ma siamo solo all'inizio: l'intelligenza artificiale abiliterà l'automazione e la robotica, la nuova sensoristica moltiplicherà esponenzialmente i dati, la sempre maggiore potenza di calcolo accrescerà a dismisura la capacità di trarre da questi dati utili informazioni. Tecnologie dirompenti quali i computer quantistici e gli impianti neurali si aggiungeranno a queste e ad altre trasformazioni, rivoluzionando ulteriormente la nostra vita. Queste tecnologie, a loro volta, si combineranno tra loro, facendo emergere problemi e soluzioni inattesi. Siamo quindi nel mezzo di una rivoluzione che a livello politico e culturale possiamo a malapena comprendere. Il futuro ci viene incontro privandoci dell'illusione di poterlo indirizzare: siamo già seduti in una macchina a pilotaggio remoto e non abbiamo una mappa per orientare la nostra rotta.

Se non è possibile immaginare un futuro senza internet, molto più complesso è immaginare che internet avremo in futuro. Forse è proprio il senso dell'ineluttabilità e dell'imponderabilità delle trasformazioni in corso che collettivamente ci deresponsabilizza dal riflettere sulle loro implicazioni morali, culturali, politico-istituzionali e strategiche. Ma poiché è certo che il "mondo reale" e lo spazio cibernetico s'intersecheranno in maniera sempre più indistinguibile, la questione di sapere che internet avremo in futuro è una questione che ci riguarda da vicino: **la nostra libertà e la nostra sicurezza dipenderanno, in misura crescente, da quanto libero e sicuro sarà il web.**

Più cresce la rilevanza di internet e la "superficie d'attacco" accessibile per il suo tramite, più la sicurezza cibernetica rappresenta un fattore di rischio in ascesa. Il World-Wide Web, nato anarchico per connettere le persone a livello globale ignorando distanze geografiche e frontiere politiche, è divenuto uno dei più destabilizzanti campi di gioco della competizione tra gli Stati. Lo spazio cibernetico è infatti ormai troppo importante per la sicurezza nazionale per non essere anche il teatro dove questi interessi naturalmente collidono. Tutte le maggiori potenze sono quindi impegnate nel rafforzare la loro "superiorità cibernetica", ossia la capacità di condurre operazioni nel dominio cibernetico negando ogni vantaggio strategico, tattico od operativo agli avversari. Nulla di nuovo, per un certo verso: man mano che la confidenzialità, la disponibilità e l'integrità dei dati divengono più rilevanti per la sicurezza nazionale, più urgente diventa per gli Stati rafforzare la propria sicurezza cibernetica e potenzialmente più vantaggiose risultano le azioni offensive nello spazio cibernetico. In questo senso, **il Cyber power è semplicemente un'altra dimensione in cui si estrinseca la sovranità nel XXI secolo.**

Il dominio cibernetico si caratterizza per la sua ubiquità: esso è il sistema nervoso che collega tra loro a livello interpersonale, locale, nazionale, internazionale e transnazionale le dimensioni politico-strategica, militare, informativa, economico-finanziaria, industriale, infrastrutturale. La crescente complessità di queste interdipendenze moltiplica il rischio che una crisi possa propagarsi dal dominio cibernetico a quello convenzionale e strategico: una crisi cibernetica può cioè divenire (in un caso certamente estremo, ma non impossibile) una minaccia alla stabilità nucleare strategica.

Cittadini ed aziende sono oggi divenuti gli abituali obiettivi di questa conflittualità sulle reti, e chiedono protezione. Assicurarla significa però dover ripensare dottrine, paradigmi ed approcci alla sicurezza, perché i bersagli di oggi erano fino a pochi anni fa ben protetti dentro i confini nazionali, mentre oggi sono per definizione "in prima linea", ed anche perché il "campo di battaglia" è perlopiù sviluppato, detenuto ed operato dai privati. Nello spazio cibernetico non ci sono barriere d'ingresso. Chiunque disponga di un accesso alla rete, di motivazione e di capacità informatiche (ma ahinoi queste sono sempre meno necessarie, perché le armi cibernetiche si comprano e si vendono nel mercato del crimine informatico) può entrare nel "grande gioco" degli interessi nazionali e della sicurezza internazionale. A volte contando nell'anonimato, altre invece ostentando falsa bandiera. Attori non-statali, che sfruttano il vantaggio asimmetrico (attaccare costa molto meno che difendere) e l'ampio anonimato concessi dello spazio cibernetico, contribuiscono significativamente a rendere volatile questo dominio: le organizzazioni dedite al crimine informatico transnazionale, che investono enormi capitali nella ricerca e sviluppo di sempre più efficaci armi cibernetiche; hacker solitari, motivati da interessi o ideologia; agenti provocatori al servizio di Stati ansiosi di non comparire direttamente; in prospettiva, terroristi. Tutti questi attori utilizzano il medesimo dominio operativo, lo stesso hardware ed hanno a disposizione gli stessi strumenti d'attacco, utilizzando tattiche, strumenti e procedure note e condivise. Tutto ciò complica enormemente l'identificazione dell'attaccante e dunque aumenta la volatilità dello spazio cibernetico, rendendolo per antonomasia il dominio dell'ambiguità. E dunque gli Stati sovrani finiscono per non sapere se stanno difendendosi da un servizio di intelligence alleato o nemico o da qualcuno che lavora per loro conto, da "talpe" interne, da "hacktivisti" quali Anonymus, o da semplici individui motivati da soldi facili e dal desiderio di fama nell'ambito della comunità degli hacker, non a caso definita "underground".

A rendere il quadro ancora più opaco c'è infine il fatto che le armi cibernetiche sono efficaci *in quanto* sfruttano vulnerabilità non note pubblicamente; non sappiamo, dunque, cosa sia pronto negli arsenali cibernetici degli Stati. Possiamo presumere che le reti globali, il

campo da gioco di un eventuale futuro conflitto, siano state mappate nel dettaglio, ma non sappiamo quale sia l'equivalente cibernetico di un conflitto nucleare. Il che forse riduce il nostro livello di allarme. Certamente preoccupa, per il momento, il fatto che le armi cibernetiche finora svelate al pubblico grazie ai vari *leaks* siano state già utilizzate per scatenare attacchi di proporzioni globali, alimentando una corsa alla proliferazione aperta a tutti: non disintegrandosi all'utilizzo, le armi cibernetiche possono essere studiate, e fornire utili idee su come confezionarne di sempre più sofisticate.

I progressi nel campo dell'intelligenza artificiale, ad esempio, renderanno possibile automatizzare i sistemi d'arma (anche quelli per il dominio cibernetico) e ottimizzare la pianificazione delle operazioni militari, consentiranno di manipolare molto più efficacemente le opinioni pubbliche mediante *deep-fakes* e propaganda computazionale, eleveranno in maniera esponenziale la velocità dei futuri conflitti, i quali saranno sempre più tra sistemi operativi capaci di decidere autonomamente (ossia tra sistemi di algoritmi). In questo contesto, **la tutela e la promozione del vantaggio tecnologico è un obiettivo prioritario, perché da esso sempre più dipenderà la nostra capacità di non soccombere nella competizione globale tra sistemi alternativi.**

Se tutti ci sentiamo rassicurati da uno Stato capace di difendere le reti in uso a livello nazionale, l'effetto di questo processo, a livello sistemico, è **una perdurante conflittualità sulle reti che alimenta un colossale "paradosso della sicurezza", in cui la le capacità cibernetiche (il "Cyber power") altrui vengono viste come una potenziale minaccia alla sicurezza delle mie reti.** Ciò, a sua volta, mina alle fondamenta la fiducia tra gli Stati, che pure rappresenterebbe il presupposto necessario per definire le "regole del gioco" dell'arena digitale globale.

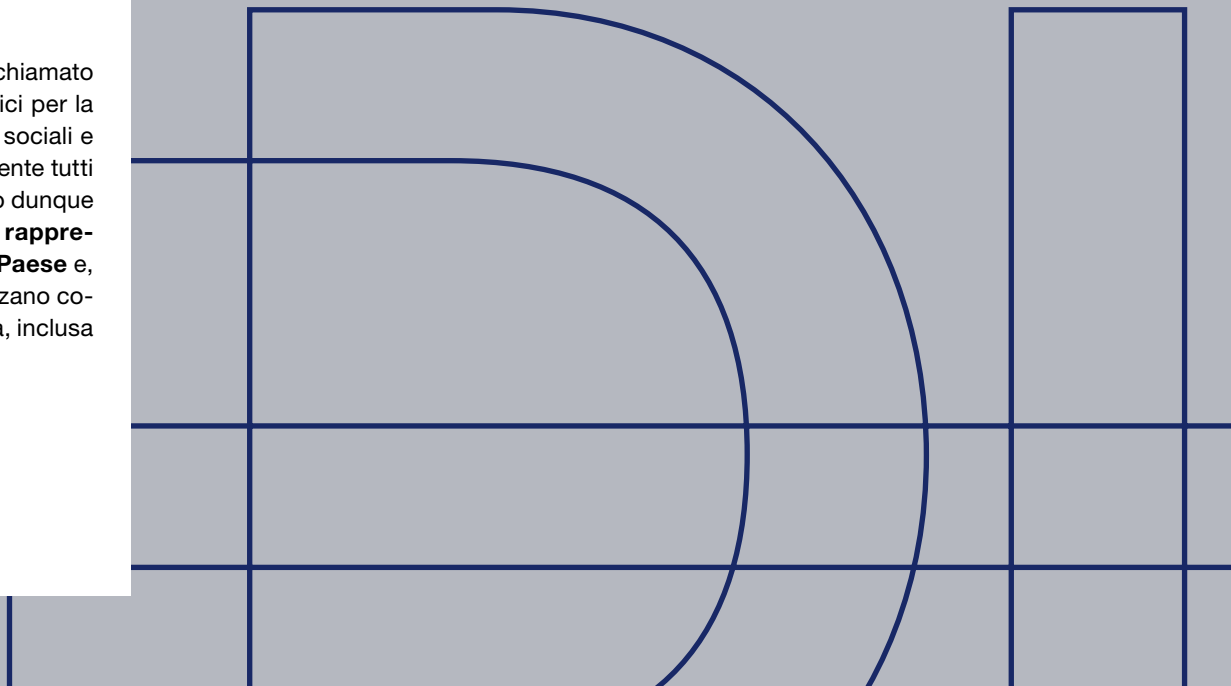
Tutto fa ritenere che l'attuale trend di crescita della minaccia cibernetica risulterà confermato ed accentuato nei prossimi anni. In un clima internazionale di ritorno sulla scena degli Stati sovrani, è prevedibile ch'essi siano chiamati a trovare soluzioni nazionali o regionali alla sicurezza cibernetica ed al trattamento dei dati, che potrebbero sfociare nella sostanziale "balcanizzazione" di internet così come lo conosciamo oggi. Senza arrivare a questi estremi (ma avvisaglie se ne vedono eccome), è assai probabile che si farà più pressante la necessità d'imporre, a livello nazionale o regionale, standard e requisiti di sicurezza informatica sempre più stringenti, che potrebbero dar vita ad un *normative patchwork* a livello internazionale ed al proliferare di barriere non tariffarie al commercio internazionale, specie nell'ambito della sicurezza della *supply chain* nei settori ad alto contenuto tecnologico, per antonomasia integrata a livello globale ed al contempo intrinsecamente vulnerabile a pericolosissime compromissioni. Nella competizione tra le Grandi Potenze, anche il traffico internet si segmenta in diversi sistemi tra loro connessi, ma all'occorrenza potenzialmente autarchici: è il caso del Grande Firewall cinese, o del controllo sovrano esercitato dalla Russia sulle proprie reti. **Sono evoluzioni che discendono dalla (e al contempo rafforzano la) competizione tra blocchi contrapposti, ed è forse qui che osserviamo più profonde le linee di faglia del mondo che verrà:** se per gli uni la "libertà di internet" è condizione ideologicamente irrinunciabile per il godimento nel XXI secolo dei fondamentali diritti di informazione, espressione e associazione, per gli altri essa rappresenta una minaccia esistenziale per la propria stabilità politica e la propria sicurezza. Sono posizioni irreconciliabili come quelle che vediamo in azione sul territorio dell'Ucraina (ed in effetti, ne rappresentano la logica prosecuzione), e che contribuiranno a mantenere il dominio cibernetico come un *far west* per molto tempo.

Le aziende ad alto contenuto tecnologico e con know-how avanzato, e quelle che gestiscono informazioni a vario titolo pregiate, sono troppo spesso ignari obiettivi di un'intensa e globale attività di spionaggio industriale, mentre quelle che detengono ed operano infrastrutture critiche, servizi di pubblica utilità e *media outlets* sono regolarmente target di azioni potenzialmente ostili, di matrice statuale e non. **È dunque imperativo che le aziende "si pongano il problema"** – a livello strategico e culturale, prima ancora che tecnologico – di come minimizzare i rischi impliciti nella loro presenza su internet. Anche a prescindere da azioni ostili dirette specificamente contro di loro, la crescente conflittualità potrebbe infatti comunque compromettere la loro *business continuity* in maniera indiretta, ad esempio attraverso attacchi ai network dei fornitori o delle piattaforme di e-commerce, o magari, ancora, per effetto di una nuova esplosione sottomarina, questa volta ai danni di una delle dorsali che trasferiscono dati attraverso il mondo.

La minaccia cibernetica ha lo stesso effetto del monossido di carbonio: non la si percepisce ma esiste. Lo si comprende bene se si osserva quanto tempo è necessario perché le aziende rilevino (magari grazie al supporto delle preposte autorità) un attacco alle loro reti, cullandosi troppo a lungo e troppo spesso in un falso senso di sicurezza. Sebbene questi tempi si siano significativamente accorciati negli ultimi anni (una buona notizia, che testimonia la crescita delle istituzioni nazionali preposte alla difesa, oltre che della *cyber preparedness* nazionale), rimane il fatto che virtualmente tutti questi incidenti informatici hanno offerto all'attaccante il tempo necessario per esfiltrare dalle reti aziendali ogni dato potenzialmente sensibile. Anche senza dover attendere una "Caporetto 2.0" o un "11 settembre cibernetico", occorre quindi, da subito, porre attenzione a quanto già accade nel tessuto produttivo italiano. **Per un Paese come l'Italia**, che fa dell'innovazione la pietra angolare della propria crescita, e per la quale il furto del know-how scientifico, tecnologico ed aziendale comporta un danno diretto e grave alla capacità di rimanere competitivi nei mercati internazionali, **il danno potenziale è incalcolabile.** Specie se si considera che le piccole-medie imprese, vera spina dorsale della nostra economia e dove pure risiede il 30% circa degli investimenti nazionali in ricerca e sviluppo, sono troppo spesso poco consapevoli dell'effettivo valore dei dati da esse gestito e della reale minaccia spionistica che incombe su di loro da oltre frontiera (sebbene, magari, al soldo del concorrente che ha gli stabilimenti produttivi di rimpetto), oppure ritengono troppo caro l'accedere a servizi di Cybersecurity affidabili.

La sfida che abbiamo dinnanzi non è dunque solo tecnologica, ma è innanzitutto culturale, perché a mutare deve essere, in primo luogo, il modo in cui in azienda si pensa alla protezione dei dati e dei sistemi ICT, dimostrandosi all'altezza della rivoluzione organizzativa in atto: non possono esservi scuse per il management che fallisca nel promuovere, top-down, il necessario cambiamento su questi temi. Il vertice aziendale deve attestarsi quale centro di comando e controllo delle reti aziendali e delle informazioni strategiche, oltre che il primario custode della riservatezza delle comunicazioni ed il responsabile dell'integrità dei sistemi ICT. Una nuova sensibilità è necessaria anche nelle politiche del personale, e non solo nel senso che è necessario diffondere, a tutti i livelli, consapevolezza circa la minaccia cibernetica, oltre che a promuovere la scrupolosa aderenza alle politiche di sicurezza aziendali. Più critico – e difficile – appare infatti far sì che alle figure più direttamente coinvolte con la sicurezza cibernetica venga riconosciuto un ruolo adeguato al rilievo che esse assumono, nel nuovo contesto di sicurezza, per la vita dell'azienda, e venga riservato un canale di comunicazione diretto con il vertice aziendale, rendendo così possibile anche un sostanziale *reverse-mentoring*, che non può prescindere dall'avvio di un diverso approccio, in azienda, alla gestione dei rapporti inter-generazionali. Si tratta di un aspetto critico, perché il *brain drain* nel settore della Cybersecurity ha raggiunto una soglia allarmante, visto che, a fronte di una domanda di esperti in Cybersecurity in assoluta esplosione, i brillantissimi giovani che riusciamo a formare lasciano troppo spesso il Paese perché attratti da salari certamente più alti, oltre che da responsabilità e status decisamente più rilevanti. Ed è infine imperativo fare squadra, perché questa è l'unica strategia sensata in uno scenario strategico asimmetrico quale quello cibernetico, dove diventa fondamentale ragionare in una logica di sistema, e dove occorre quindi imparare che il mio concorrente sul mercato può e deve anche essere il mio alleato nell'*early warning*, nell'*info-sharing* e nella gestione delle emergenze.

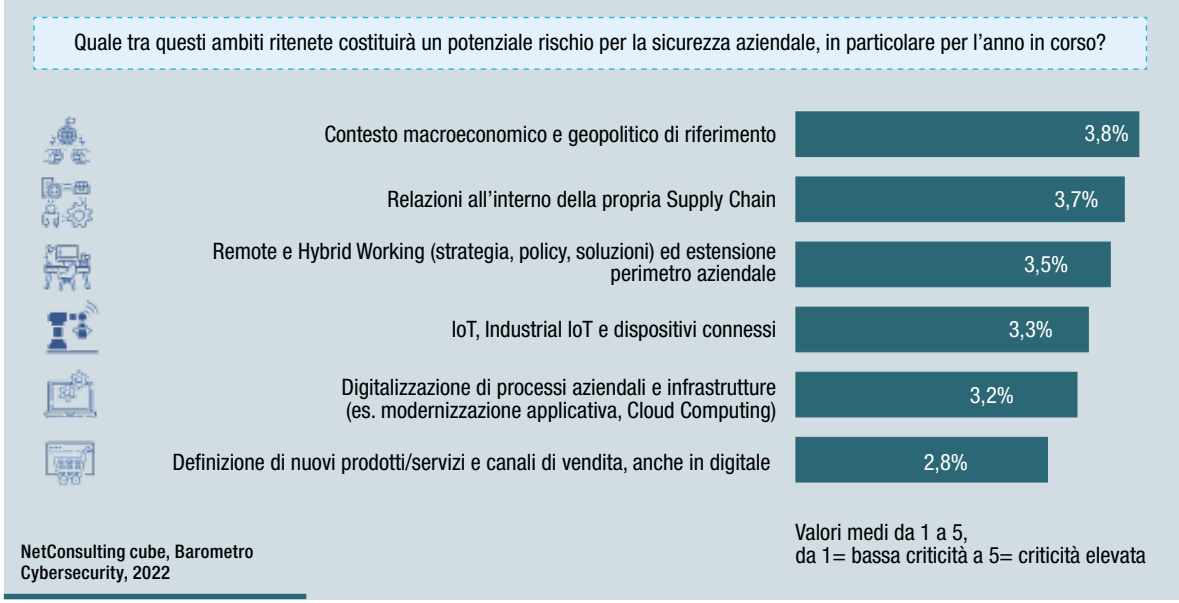
Per far tutto questo, il Paese nel suo complesso – e ciascuno per la sua parte – è chiamato a concorrere alla messa in opera di un piano straordinario di investimenti strategici per la sicurezza cibernetica, non solo economici, ma anche – e, forse, primariamente – sociali e progettuali. Il tema della sicurezza cibernetica interseca trasversalmente praticamente tutti gli ambiti della vita civile, politica, strategico-militare ed economica, e va affrontato dunque secondo una logica olistica e centripeta. **Riuscire ad imprimere questa logica rappresenta una sfida il cui esito definirà nel profondo il futuro del nostro sistema Paese** e, come abbiamo visto all'inizio, la nostra capacità di tutelare i valori che ci caratterizzano come Occidente. La radice valoriale è infatti il fondamento di ogni politica di sicurezza, inclusa quella per lo spazio cibernetico.



Le minacce sul fronte della Cybersecurity: trend attacchi ed esposizione alle minacce

Il numero di attacchi informatici ha continuato a crescere a livello mondiale, raggiungendo i 1.169 attacchi gravi nel primo semestre 2022, con un incremento dell'8,4% rispetto al primo semestre 2021, e un picco di 225 attacchi fatto registrare nel marzo 2022, il valore più alto mai verificatosi.[1]
Preoccupante è anche il trend in aumento degli attacchi gravi: +66% rispetto al 2017.
L'incremento maggiore ha riguardato gli attacchi che rientrano nella categoria "Hacktivism" (più che quadruplicati), seguiti dalla categoria '"Information Warfare" cresciuta del 119%. In forte aumento sono anche gli attacchi con finalità di "Espionage" (+62% rispetto al primo semestre 2021), mentre sono diminuiti del 3,4% gli attacchi classificati come attività di "Cybercrime", pur confermandosi al primo posto delle motivazioni di attacco a livello globale, rappresentando il 78,4% degli attacchi globali.
Una delle cause principali di questa crescita è da imputare all'esplosione del conflitto russo-ucraino che, unitamente alla crescente digitalizzazione e alla penetrazione dello smart working, ha determinato, da una parte, un aumento degli attacchi anche in termini di capacità di colpire target multipli, sostenuti da attività di cyber intelligence, dall'altro ha amplificato l'esposizione di aziende e organizzazioni con conseguenti impatti economici.
Questa valutazione è confermata anche dal Barometro Cybersecurity 2022: la survey svolta da NetConsulting cube su 81 aziende e organizzazioni pubbliche, da cui emerge come l'instabilità dello scenario geopolitico rappresenti la principale preoccupazione in termini di rischi per la sicurezza, seguita dalle relazioni all'interno della supply chain che, in seguito alla digitalizzazione degli scambi di dati e informazioni lungo la filiera, estendono il perimetro delle aziende e le espongono a maggiori rischi (Fig. 1).
I malware rappresentano la principale tecnica di attacco, pari al 38% del totale. Ransomware e attacchi

Figura 1:
Principali rischi per la sicurezza nel 2022



NetConsulting cube, Barometro Cybersecurity, 2022

finalizzati a rendere indisponibili applicazioni e servizi, in particolare DDoS, sono cresciuti in modo esponenziale con lo scoppio del conflitto sul territorio ucraino. Le tecniche sconosciute (categoria "Unknown") si posizionano al secondo posto, con un aumento del 10% rispetto al primo semestre 2021, superando la categoria "Vulnerabilità" (-26,8%) e "Phishing / Social Engineering", in crescita però del 63,8%.

L'inasprimento degli attacchi è strettamente correlato allo sviluppo di una nuova ondata di hactivism e gli attacchi cyber sono diventati una delle armi per far leva sulla disinformazione durante il conflitto. Gli exploit zero-day sono stati una delle principali risorse utilizzate per raggiungere obiettivi strategici e indebolire le organizzazioni. Infine si è assistito, già a partire dal 2021, alla crescente diffusione del modello Hacker as a service oltre che a un incremento negli attacchi alla supply chain e in particolare contro i Managed service provider.

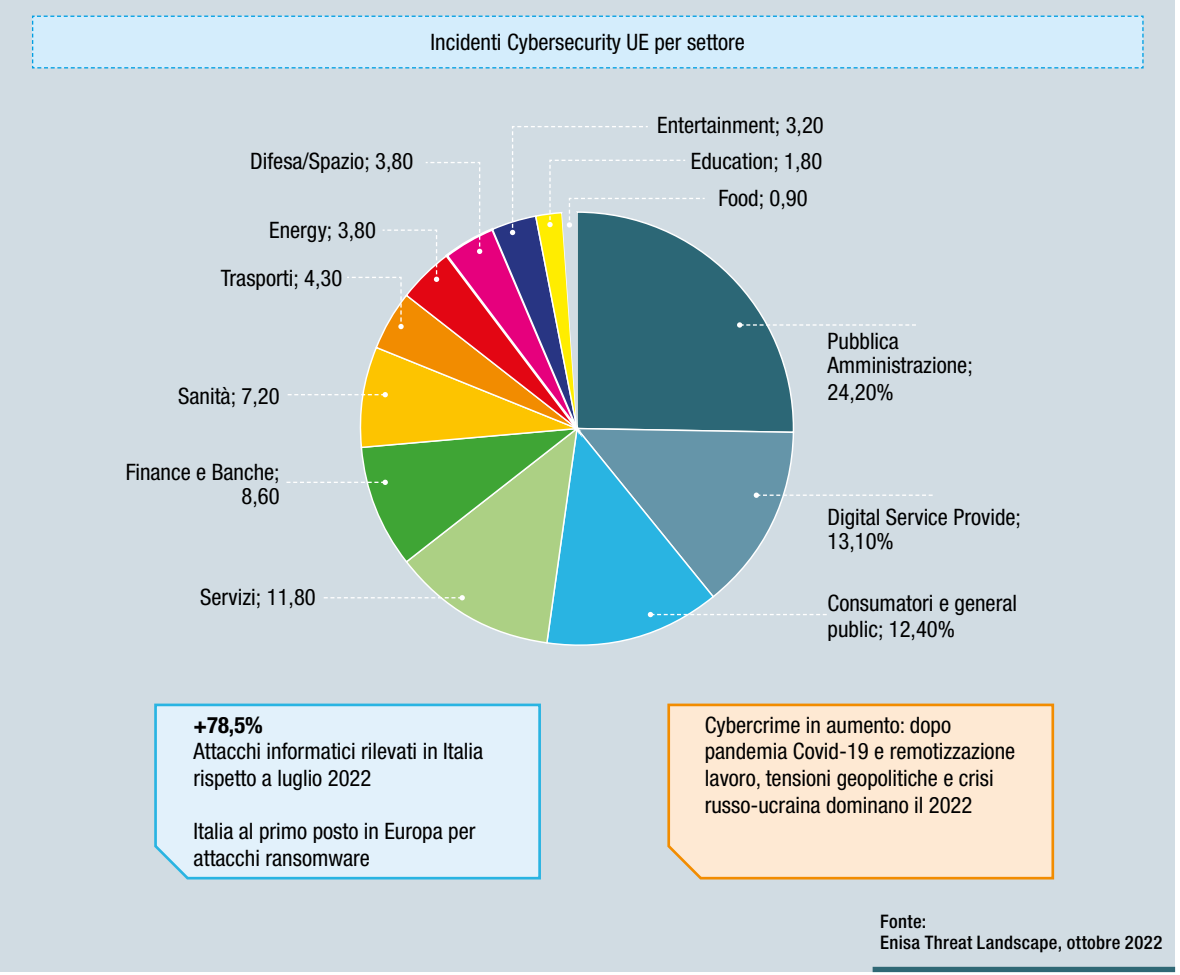
I dati relativi all'Italia, contenuti nel report pubblicato dal Viminale ad agosto, evidenziano un trend in aumento, con una crescita del 78,5% registrata a luglio 2022. Il nostro Paese, inoltre, risulta al primo posto in Europa per attacchi ransomware.

I principali obiettivi degli attaccanti sono rappresentati dagli enti della Pubblica Amministrazione: in tutta Europa si è avuto un aumento degli incidenti superiore a quanto accaduto negli altri settori, con conseguente indisponibilità dei servizi online, che rappresentano i principali obiettivi degli attaccanti, seguiti dai Digital service provider (Fig. 2).

In Italia, le categorie più colpite sono state la Sanità e la Pubblica Amministrazione, ciascuna con circa il 12% degli attacchi totali; a seguire gli Operatori ICT (11%) e il Finance (9%).[2]

Figura 2:

Incidenti Cybersecurity in Europa per settore, giugno 2021 - giugno 2022



Impatti della trasformazione digitale sul fronte Cybersecurity: Smart Working, Cloud, IoT

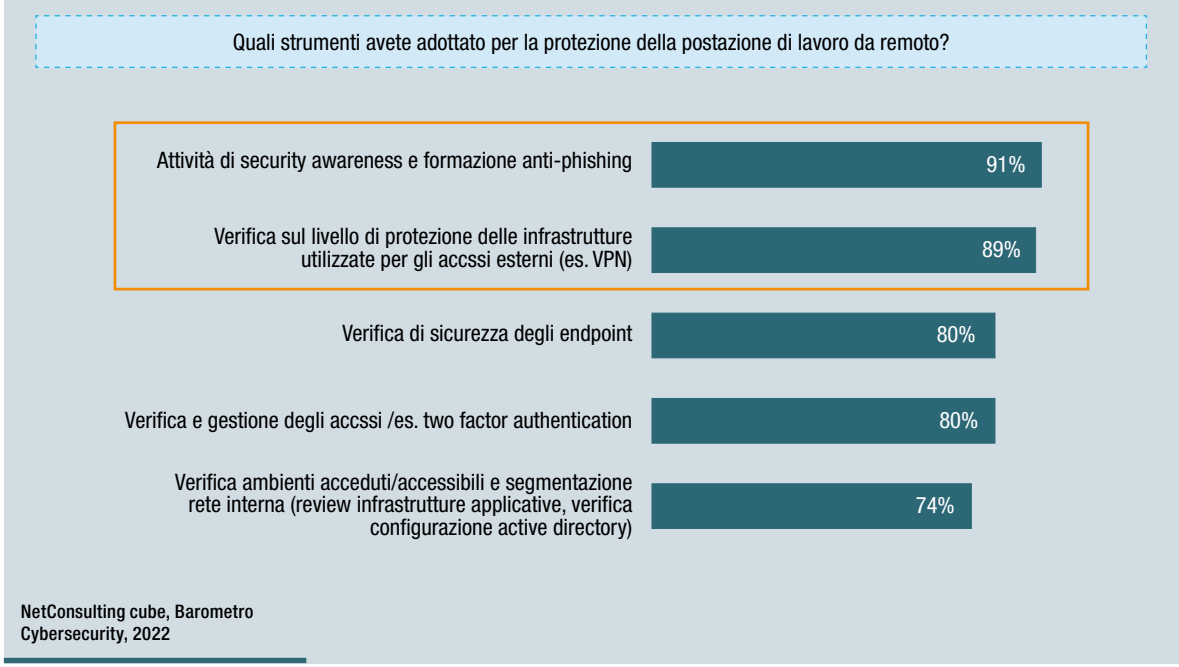
La digitalizzazione di attività, processi interni ed esterni, modelli di business e di lavoro continua la sua corsa grazie non solo agli evidenti benefici per l'efficienza e l'efficacia di aziende ed enti, ma anche alle misure previste dal PNRR nelle sue Missioni. Tuttavia, la trasformazione digitale non è esente da criticità e aree di attenzione, primo fra tutti il significativo incremento dei rischi di attacco alla sicurezza delle diverse organizzazioni a fronte dell'inarrestabile ampliamento e apertura dei confini aziendali. Non è un caso che, ad oggi, come evidenziato dal Barometro Cybersecurity, tra le principali fonti di rischio per la sicurezza aziendale spicchino proprio la digitalizzazione dei modelli lavorativi, dei processi di business interni ed esterni e delle operation.

La revisione in chiave digitale dell'organizzazione del lavoro è un lascito importante del periodo pandemico. Dal Barometro Cybersecurity emerge che i modelli di Remote e Smart Working, introdotti come risposta emergenziale per garantire la continuità operativa delle aziende nel periodo dei lockdown, continueranno ad essere usati prevalentemente in chiave ibrida, ovvero in integrazione con il lavoro in presenza (68% delle risposte). L'utilizzo in via definitiva di un modello di Hybrid Working potrebbe crescere ulteriormente se si pensa che il 20% delle organizzazioni del panel, pur in mancanza di una decisione finale in merito, ha dichiarato la preferenza per un'organizzazione del lavoro ibrida. L'utilizzo esclusivo di un modello da remoto appare, invece, minoritario (2% delle risposte) così come la preferenza per il ritorno alla sola operatività in presenza (10%).

Alla luce di questa tendenza, è prevedibile che i rischi per la sicurezza aziendale riconducibili all'organizzazione del lavoro continueranno ad essere molto intensi. Il possibile utilizzo di reti non sicure o comunque non presidiate direttamente dal datore di lavoro, l'uso di dispositivi personali in un'ottica BYOD e la condivisione non attenta di documenti e dati aziendali contribuiranno a rendere le aziende più vulnerabili ai tentativi di attacco che si prevedono in crescita anche nei prossimi anni. A questo

Figura 3:

Principali strumenti per la sicurezza del lavoro da remoto



NetConsulting cube, Barometro Cybersecurity, 2022

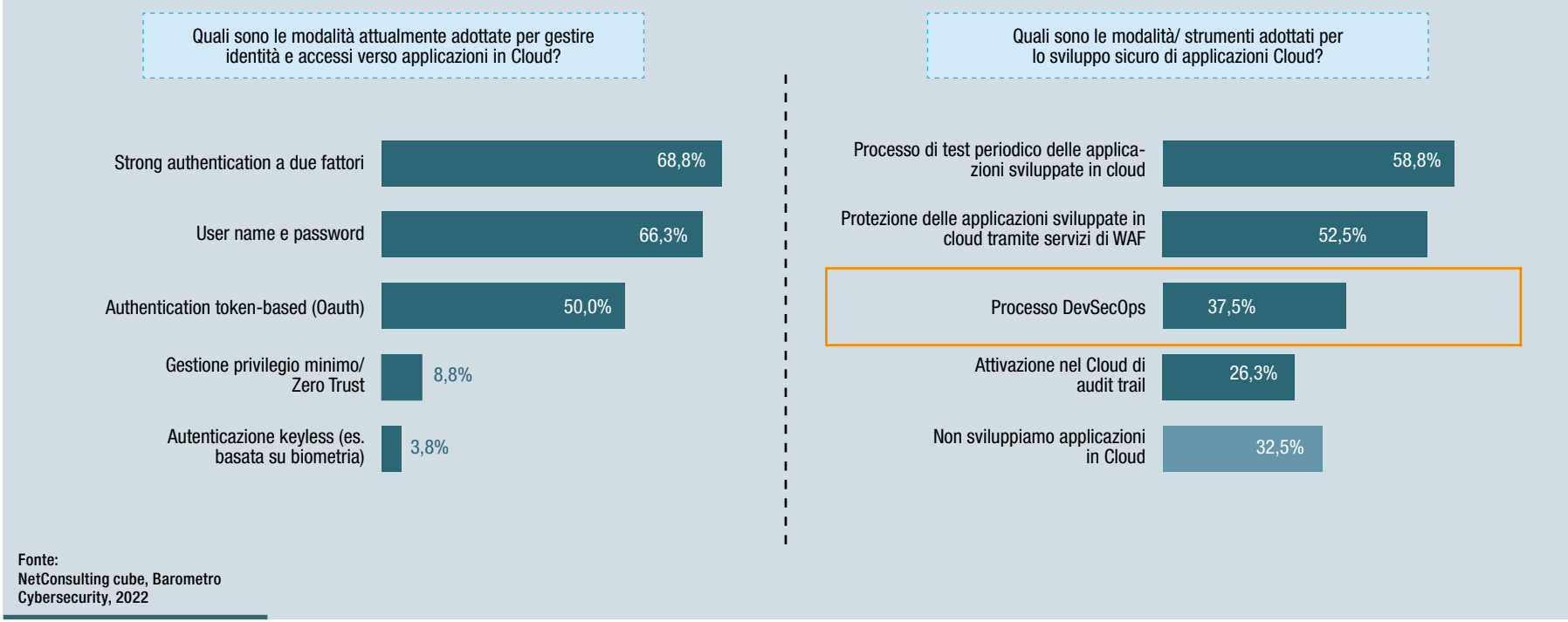
proposito, sempre dalla citata indagine, è emerso che i principali tentativi di attacco osservati nel corso del 2021 (e in crescita nel 2022) sono stati il phishing, il social engineering e gli attacchi non mirati ad applicativi web e mobile.
Per far fronte all'aumento delle minacce che incombono sulle postazioni di lavoro da remoto e, allo stesso tempo, per proteggerle adeguatamente, le aziende hanno messo in atto un'ampia gamma di azioni, che trovano riscontro in una elevata percentuale del campione, superiore al 70% (Fig. 3).
Le azioni più frequenti puntano sul fattore umano (91% delle risposte), ovvero sull'avvio di iniziative volte ad aumentare la consapevolezza del personale relativamente a rischi e pericoli in ambito sicurezza, soprattutto di quelli associati agli attacchi di phishing. Seguono azioni basate sull'adozione di soluzioni per la sicurezza delle VPN, citate dall'89% del panel, a dimostrazione di come il lavoro da remoto stia gradualmente diventando una condizione di normalità e dell'esigenza di proteggere gli accessi al server aziendale. La verifica della sicurezza degli endpoint è stata citata dall'80% dei partecipanti all'indagine: si tratta di un'attività in genere prevista dalle funzioni tecniche delle aziende che in quest'ultimo biennio ha registrato un rinnovato interesse. Un ulteriore 80% del panel ha segnalato l'adozione di strumenti per la verifica e la gestione degli accessi a qualunque tipo di risorsa digitale, applicativi, account, VPN e siti. Tali strumenti garantiscono un livello di protezione particolarmente elevato perché richiedono all'utente di fornire un set più ampio di credenziali. È una caratteristica di interesse soprattutto nel caso di risorse ICT particolarmente critiche ai fini delle attività aziendali. Infine, nel 74% dei casi, è stato segnalato l'uso di strumenti di Network Security per verificare gli eventuali accessi o gli ambienti accessibili.
Il Cloud Computing rappresenta l'elemento tecnologico abilitante per antonomasia, alla base di pressoché tutte le iniziative di digitalizzazione, modernizzazione applicativa, implementazione di soluzioni e piattaforme digitali, etc. All'interno del panel che ha partecipato all'ultima edizione del Barometro Cybersecurity, il Cloud Computing appare molto utilizzato (99% circa). Prevale l'adozione di modelli di Hybrid Cloud (72,5%) e MultiCloud (51,3%) e di servizi SaaS e IaaS (rispettivamente nel 92,5% e 85% dei casi). Al crescere dell'utilizzo di modelli e servizi Cloud aumentano anche i rischi in ambito sicurezza. In prima battuta, la difficoltà di controllo dei livelli di sicurezza messi a disposizione dal Cloud provider rende vulnerabili le aziende, soprattutto alla luce della condivisione delle risorse IT tra diversi utenti, che è alla base del Cloud. Secondariamente, la localizzazione geografica dei Cloud provider e delle loro infrastrutture determina problematiche di privacy e protezione dei dati, e rischi di violazione e perdita di dati, relativamente anche alle diverse normative vigenti nelle varie zone. Infine, è necessario porre molta attenzione alle clausole di sicurezza personalizzate, perché siano approvate in modo consapevole e informato.
Alla luce di questi rischi va letta la predilezione delle aziende, anche all'interno del campione, verso l'utilizzo di modelli di Hybrid e MultiCloud, che consentono di ridurre la dipendenza da un singolo fornitore, e l'attenzione – nei processi di migrazione e adozione – verso aspetti di sicurezza end-to-end, di recupero di dati e di protezione delle applicazioni.
L'attenzione sui dati si traduce nella contrattualizzazione – con i Cloud provider – dei requisiti minimi di sicurezza e diritti di audit: il 60% del panel, infatti, ha dichiarato di aver contrattualizzato requisiti minimi di sicurezza e diritti di audit, in egual misura, sia con i principali che con tutti gli altri fornitori; mentre il 22% circa di imprese prevede di introdurre al più presto clausole contrattuali che coprano questi aspetti. Il restante 18% del campione si polarizza su realtà che si concentrano sui soli requisiti minimi di sicurezza in relazione, soprattutto, ai Cloud provider principali.
In genere, i fornitori di servizi Cloud danno evidenza delle certificazioni delle procedure di Cybersecurity adottate (68,8%) e delle procedure stesse (38,8%) dando – in alcuni casi – evidenza dei test effettuati (17,5%).
Per quanto riguarda le applicazioni in ambienti Cloud, le misure di sicurezza riguardano la protezione dell'accesso e delle attività di sviluppo.
L'accesso alle applicazioni in Cloud è protetto principalmente da strong authentication a due fattori (68,8%), user name e password (66,3%) e authen-

Figura 4:

Modalità adottate per gestire identità e accessi verso applicativi in Cloud e strumenti adottati per lo sviluppo sicuro delle applicazioni

tication token-based (50%) (Fig. 4). Nonostante l'utilizzo dei soli user name e password sia ancora molto diffuso, le risposte del panel suggeriscono quanto le aziende siano impegnate ad adottare misure di sicurezza a protezione delle applicazioni in Cloud sempre più inattaccabili perché basate su un insieme di fattori di autenticazione, non solo credenziali di cui l'utente è a conoscenza (password, PIN, etc.) ma anche elementi di cui l'utente è possessore esclusivo (token, smart card, etc.). Modalità più evolute di gestione di identità e accessi sono state citate da percentuali inferiori di aziende. Si segnala, in prima istanza, la gestione del privilegio minimo/ Zero Trust, indicato dall'8,8% del campione: in questo caso, l'accesso all'applicazione non dipende solo dall'identità dell'utente ma anche dal contesto della sua richiesta di accesso (dispositivo, localizzazione, funzionalità da attivare, etc.). Ancor meno citata è l'autenticazione keyless (3,8%), basata su una caratteristica biometrica dell'utente: l'impronta digitale, il timbro della voce, il volto, l'iride, etc.

Lo sviluppo sicuro di applicazioni Cloud poggia prevalentemente sullo svolgimento di test periodici (58,8% delle risposte) e sull'adozione di Web Ap-



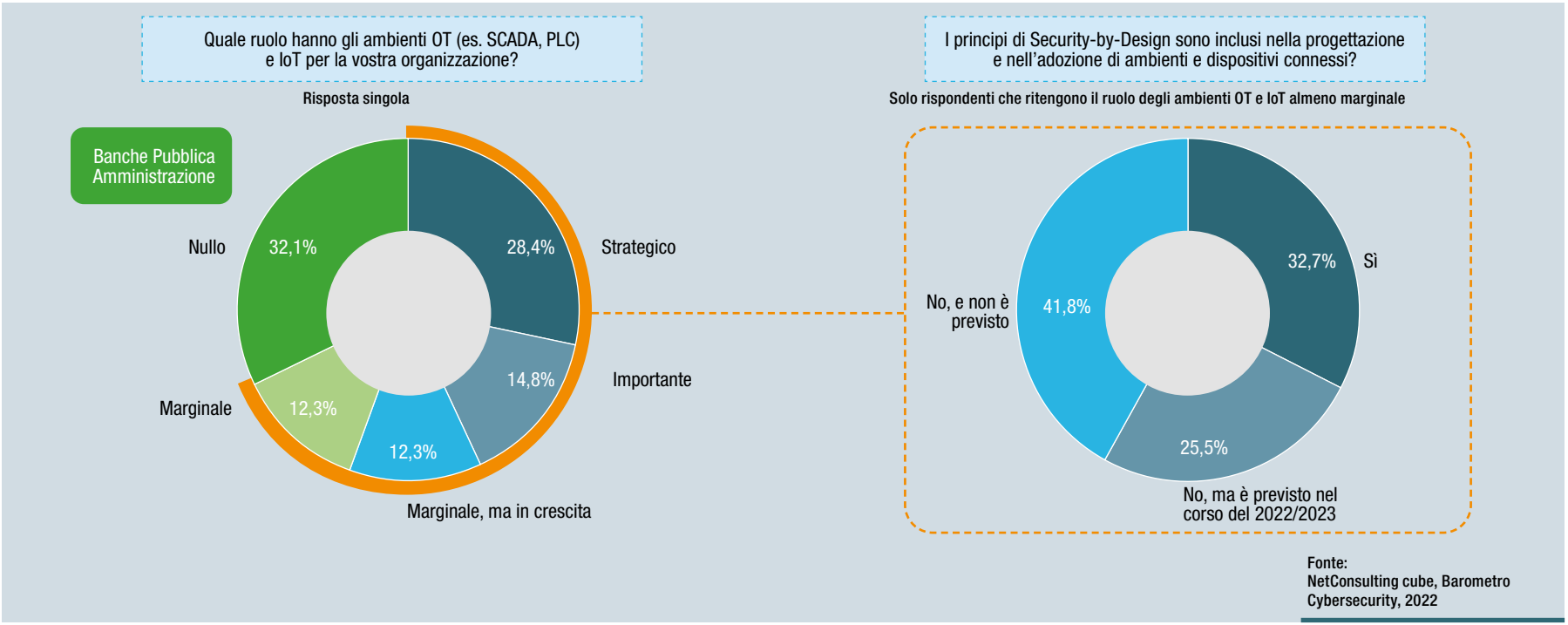
Fonte:
NetConsulting cube, Barometro Cybersecurity, 2022

plication Firewall (WAF) (52,5%). Solo il 37,5% delle realtà, soprattutto nei settori industria, utilities e bancario, ha dichiarato di adottare un approccio DevSecOps, ovvero di svolgere attività di sviluppo integrando gli aspetti di sicurezza sin dalle prime fasi della scrittura delle applicazioni e non solo nelle battute finali, con benefici in relazione alla velocità di deployment e alla riduzione della probabilità di incidenti di sicurezza. Infine, il 26,3% delle aziende ha indicato l'utilizzo di audit trail per avere una visione cronologica completa di procedure ed eventi di sicurezza.

L'adozione di Operation Technologies (OT) e di piattaforme IoT rappresenta un pilastro fondamentale delle iniziative di digitalizzazione e automazione dei processi operativi. Monitoraggio e controllo di linee produttive, magazzini e altre facility, manutenzione, tracking & tracing e controllo di qualità sono solo alcuni degli ambiti dove piattaforme OT e IoT trovano applicazione. Tutto ciò viene confermato dalle risposte del panel: oltre il 43% dei partecipanti all'indagine riconosce agli ambienti OT e IoT un ruolo rilevante (strategico o comunque importante) e più del 12% ritiene

Figura 5:

Il ruolo degli ambienti OT e IoT e l'adozione della Security by Design nella loro progettazione

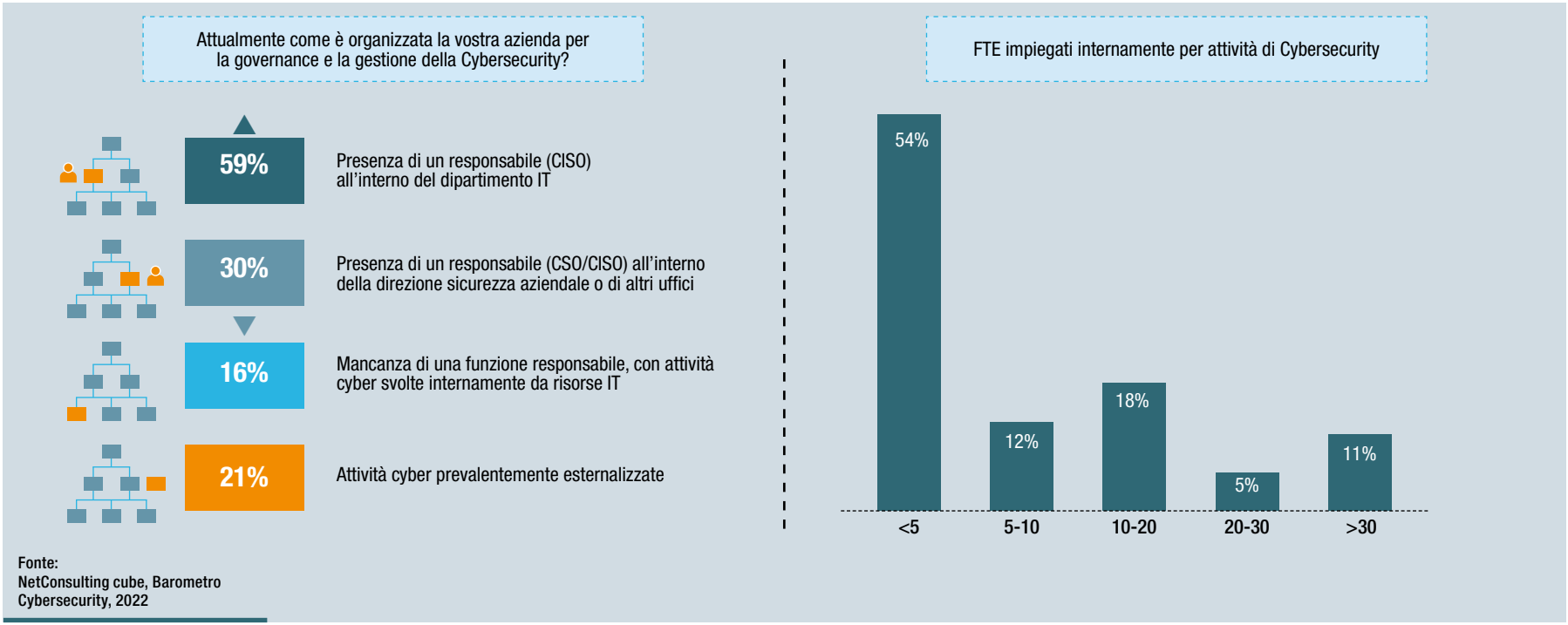


Fonte:
NetConsulting cube, Barometro Cybersecurity, 2022

che il loro utilizzo, oggi marginale, sia destinato a crescere nell'immediato futuro. Industria e utilities, seguiti da retail e assicurazioni, sono i settori caratterizzati da un maggior interesse, più o meno intenso, verso l'adozione di ambienti connessi, mentre banche e Pubblica Amministrazione si distinguono per una minor sensibilità nei confronti di piattaforme OT e IoT.
Solo il 33% circa delle aziende che riconosce agli ambiti OT e IoT un ruolo "almeno marginale", ha dichiarato di applicare principi di Security-by-Design nella loro progettazione e solo il 26% prevede di adottarli entro la fine del 2023 (Fig. 5).
A prevalere sono quindi i casi di imprese che non solo non applicano i principi di Security-by-Design, ma che non prevedono nemmeno di adottarli in futuro. Di conseguenza, dal panel emerge una situazione critica, in quanto ambienti connessi non adeguatamente protetti possono diventare un facile entry point per attacchi alla Cybersecurity, che possono colpire non solo l'ambito delle operation ma anche l'intera azienda.

Figura 6:

Organizzazione adottata per la governance e la gestione della Cybersecurity



Fonte:
NetConsulting cube, Barometro Cybersecurity, 2022

Presenza di team dedicati/ direzione con focus sulla Cybersecurity

Recentemente, il tema della Cybersecurity – complice anche il periodo di incertezza che caratterizza l'ecosistema – ha assunto una maggiore importanza all'interno delle aziende: rappresenta una priorità del piano strategico business o ICT per il 92% del panel ed è oggetto di uno specifico Resiliency Plan (corporate o relativo alla funzione IT) nel 70% delle organizzazioni.

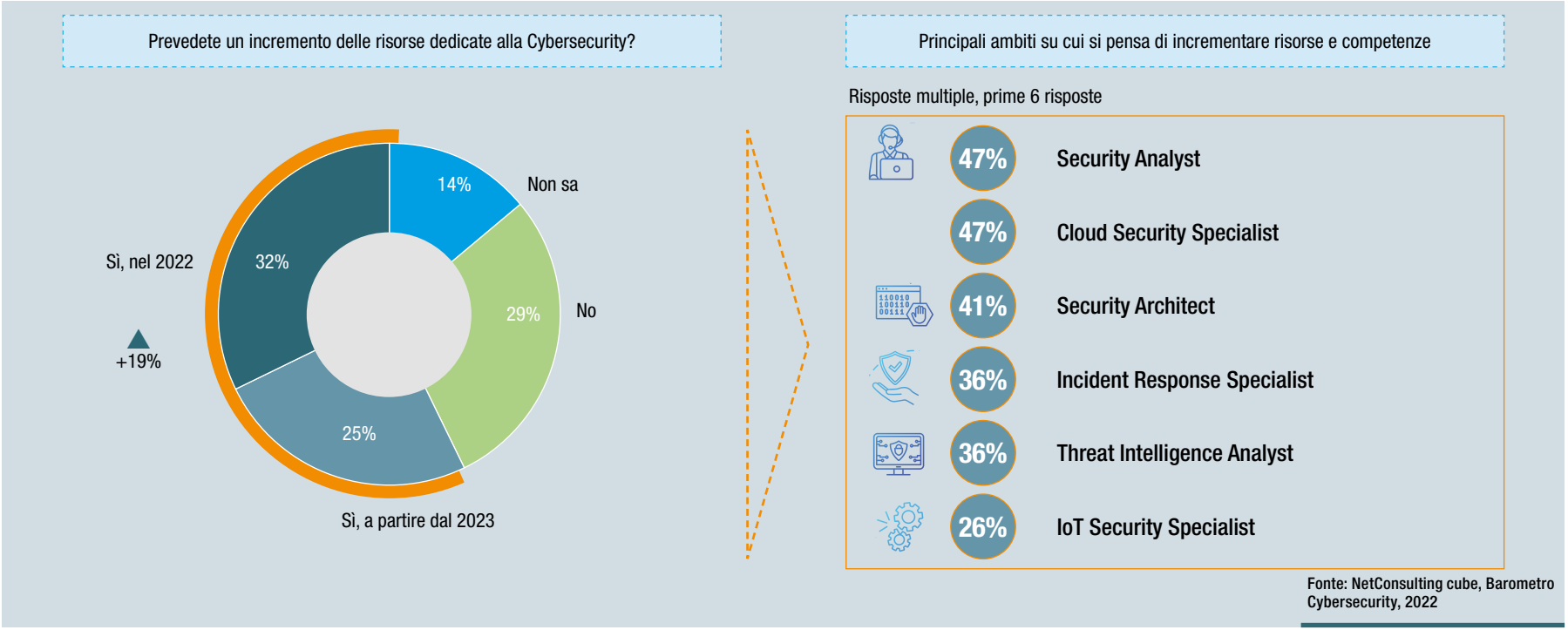
Parallelamente a ciò, si sta assistendo ad una sempre maggiore attenzione alle tematiche di Cybersecurity sul piano organizzativo (Fig. 6).

In particolare, rispetto alle scorse edizioni del Barometro Cybersecurity, si segnala che:

- è in crescita la quota di aziende che ha dichiarato di aver nominato un CISO (Chief Information Security Officer) all'interno della divisione IT, avente la responsabilità della governance e della gestione delle tematiche di sicurezza (59% del panel);
- rimane sostanzialmente inalterata la percentuale

Figura 7:

Priorità in termini di risorse e competenze previste per il 2022



Fonte: NetConsulting cube, Barometro Cybersecurity, 2022

di organizzazioni (30%) che ha indicato la presenza di un responsabile CSO/CISO a capo di una direzione specificatamente dedicata alla sicurezza aziendale, così come la quota di imprese (21%) che esternalizza qualunque attività di gestione della Cybersecurity;
- allo stesso tempo, è in riduzione il numero di organizzazioni (16%) che dichiara l'assenza di una figura di responsabile della Cybersecurity e di svolgere tutte le attività in ambito sicurezza appoggiandosi a risorse IT non specializzate. Si tratta di un buon risultato, in quanto delegare la gestione della sicurezza a profili tecnici ma non specializzati, come CTO (Chief Technology Officer), oppure responsabili Infrastrutture o Networking, può determinare una maggiore vulnerabilità in caso di tentativi di attacco.

In termini di risorse umane, alle attività in ambito Cybersecurity lavorano mediamente meno di 5 full time equivalent (FTE) (54% delle risposte polarizzate soprattutto nei settori della PA e sanità, retail e industria).

Il 30% delle organizzazioni ha indicato l'utilizzo di un numero di FTE compreso tra 5 e 20, mentre la minoranza del panel (16%), si avvale di un numero di risorse superiore ai 20 FTE.

Il numero di risorse dedicate alla Cybersecurity è previsto crescere nel 57% delle imprese che hanno partecipato all'indagine. Nella maggioranza dei casi – concentrati nei settori industria, finanza, utilities e PA – questo aumento avverrà entro la fine dell'anno in corso (Fig. 7).

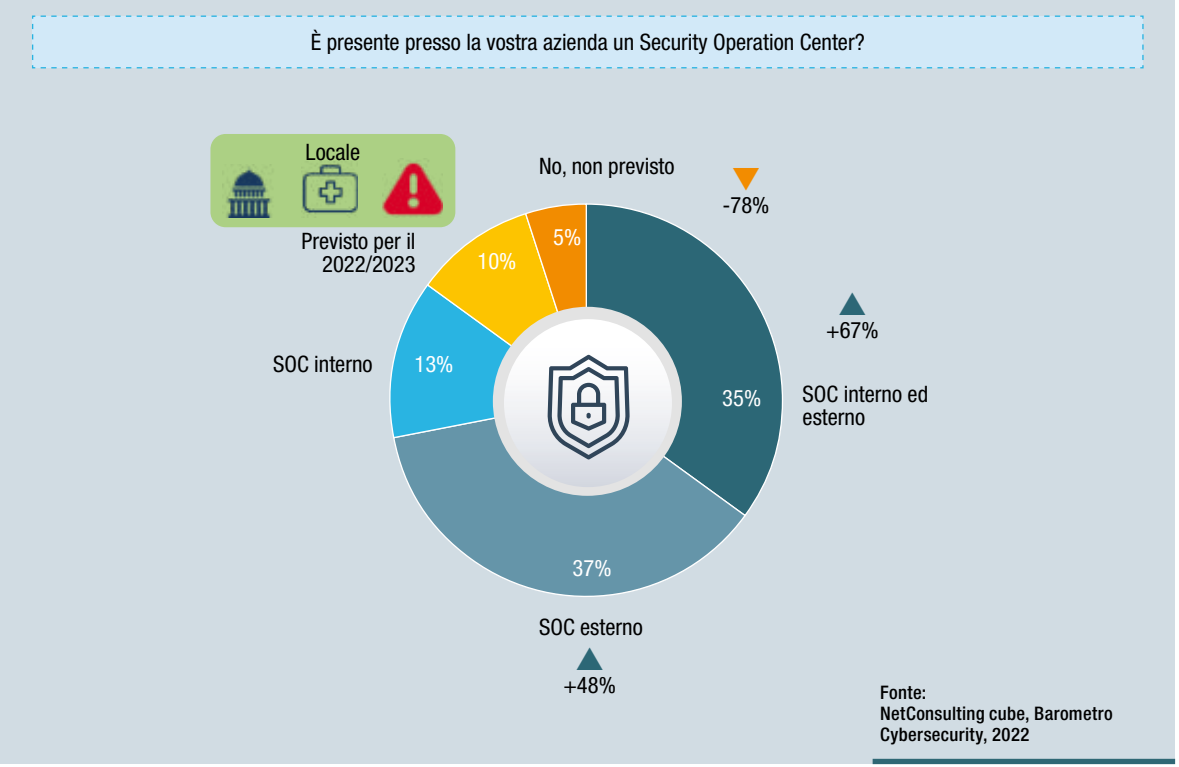
A livello aziendale, vengono ricercate risorse specializzate sia nello svolgimento di specifiche attività in ambito sicurezza sia nella gestione di tematiche di security in settori tecnologici ben determinati:
- le imprese hanno indicato – in prima battuta (47% delle citazioni) – l'esigenza di aumentare il numero di Security Analyst, ovvero di figure in grado di gestire i sistemi aziendali di prevenzione e implementare, aggiornare misure e strumenti di protezione, di identificare intrusioni e raccogliere informazioni a riguardo. Seguono (41% delle citazioni) i Security Architect, ovvero figure che progettano, sviluppano e implementano i principali sistemi di protezione. Infine, tra le figure più ricercate, vanno segnalati gli Incident Response Specialist e i Threat Intelligent Analyst (36% in entrambi i casi), che supportano le aziende, rispettivamente, nel migliorare la capacità di risposta agli incidenti e nell'identificare con precisione le minacce alla sicurezza;
- le imprese che hanno partecipato all'indagine hanno inoltre indicato la necessità di dotarsi di specialisti di sicurezza in ambito Cloud (47% delle citazioni) e IoT (26%, alla luce di una minore diffusione nel panel di ambienti connessi rispetto al Cloud): due contesti tecnologici caratterizzati da rischi per la sicurezza non trascurabili.

Adozione di misure di Detection and Response

Una efficace organizzazione in ambito Cybersecurity non è di per sé garanzia di una risposta appropriata ai rischi di attacco cyber. Affinché un'azienda sia in grado di difendersi adeguatamente è necessario che investa anche nell'adozione di strumenti che le per-

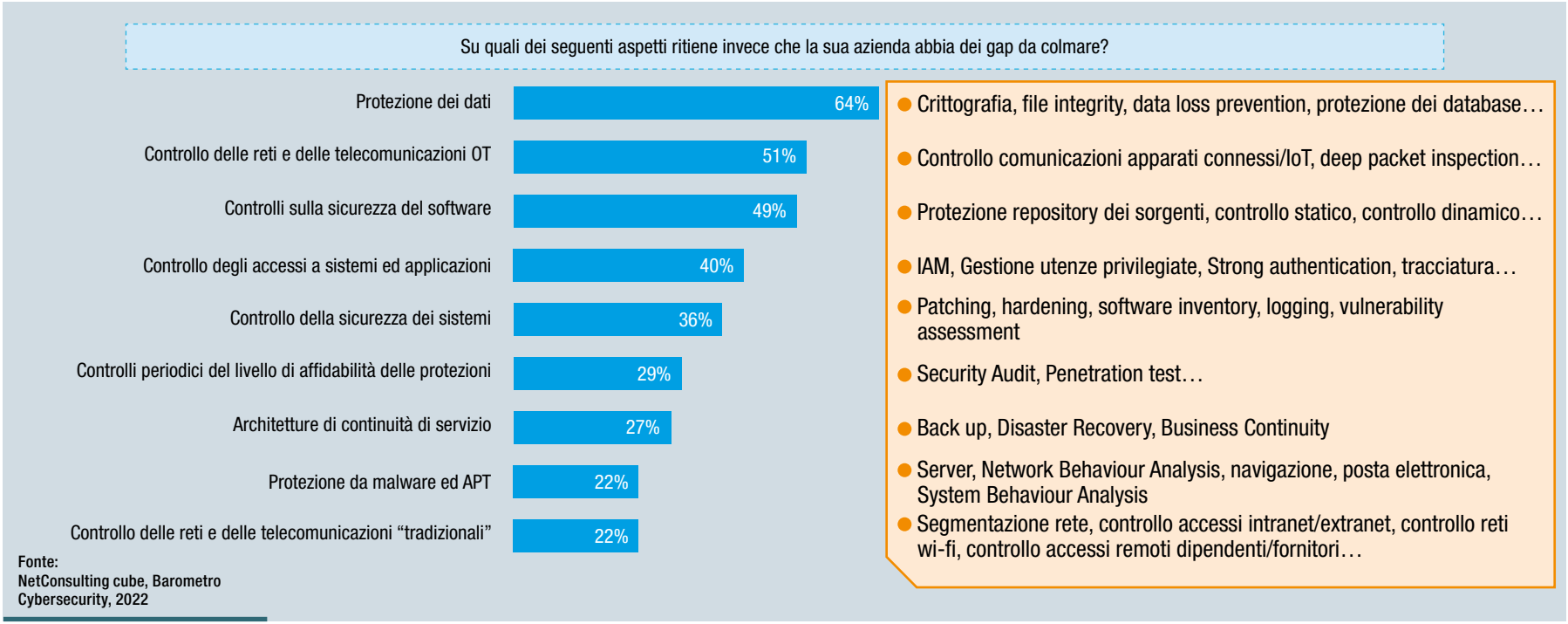
mettano di rilevare e rispondere alle minacce.
L'utilizzo di un SOC (Security Operation Center) riveste, da questo punto di vista, un'importanza fondamentale, considerata la sua missione focalizzata sul monitoraggio delle minacce, sulla gestione delle funzionalità di sicurezza e sull'incremento del livello di protezione delle risorse ICT aziendali.
All'interno del panel che ha preso parte all'edizione 2022 del Barometro Cybersecurity, l'85% delle aziende ha dichiarato di utilizzare un SOC (Fig. 8). A prevalere sono le organizzazioni (37%, in crescita del 48% rispetto alla scorsa edizione del Barometro) che adottano un SOC esterno, usufruendo di Managed Security Services erogati da provider specializzati, con riferimento in particolare a servizi di monitoraggio e proattivi, come ad esempio security assessmen , vulnerability assessment, early warning, etc. Seguono le realtà che utilizzano un SOC interno ed esterno (35% del panel, in crescita del 67% rispetto alla precedente rilevazione). Queste realtà tendono a mantenere al proprio interno le attività di tipo proattivo e di gestione, soprattutto nel caso di infrastrutture critiche, e si rivolgono a provider esterni per i servizi di gestione, fondamentali per avere un quadro sempre aggiornato dei potenziali attacchi.
L'uso esclusivo di un SOC interno è molto poco frequente (13%). Tale scelta è stata effettuata da realtà di grandi dimensioni, che hanno generalmente la capacità di spesa e gli spazi necessari a costruire e mantenere infrastrutture all'avanguardia come i SOC.
Il restante 15% dei casi è polarizzato su aziende che prevedono di utilizzare un SOC entro il 2023. Si tratta per lo più di aziende pubbliche e operanti in ambito sanità che vedranno in questo modo ridursi il divario che le separa dalle altre organizzazioni.
Le aziende che non usano alcun tipo di SOC e che non prevedono di farlo nemmeno in futuro rappresentano una minoranza risicata e, per di più, in forte contrazione rispetto alla scorsa edizione del Barometro.
Alla pericolosità dei tentativi di attacco e delle minacce alla sicurezza contribuiscono, senza dubbio, i gap che caratterizzano i sistemi e gli ambienti tec-

Figura 8:
Presenza di un SOC (Security Operation Center)



nologici di aziende ed enti.
Dalle risposte date nella realizzazione del Barometro Cybersecurity emerge che le aziende ritengono di avere una situazione deficitaria nella protezione dei dati (64% delle citazioni) (Fig. 9). Le maggiori lacune riguardano l'adozione di tecnologie di crittografia, di strumenti per l'integrità dei dati e la prevenzione della loro perdita così come di criteri di data protection. La situazione delle aziende appare, invece, complessivamente migliore in relazione all'utilizzo di soluzioni di back-up & restore e alla segnalazione di eventuali data breach entro le 72 ore, attività portate a termine mediamente nell'80% dei casi.
Tra gli altri ambiti con gap spicca il controllo delle reti negli ambienti OT (51%). In questo frangente, i ritardi da colmare riguardano le comunicazioni tra gli apparati OT/ IoT ed il controllo del traffico che fluisce lungo le reti degli ambienti connessi. Sono lacune che derivano dalla prevalenza di ambienti OT con un'età media avanzata, come quelli utilizzati in impianti di aziende industriali e utilities. È prevedibile che questi gap si ridurranno con la crescita dell'a-

Figura 9:
Principali gap da colmare



Fonte:
NetConsulting cube, Barometro Cybersecurity, 2022

dozione di soluzioni IoT che determineranno una rinnovata attenzione sugli aspetti della sicurezza.
Altre aree di miglioramento sono state indicate in relazione alla sicurezza di applicazioni (49%) e sistemi (36%). In questi casi, le aziende hanno dichiarato di dover migliorare, da un lato, nella protezione dei repository dei codici sorgente e nel controllo statico e dinamico e, dall'altro, nelle attività di patching e vulnerability assessment. Da segnalare, inoltre, sono le lacune riguardanti la gestione di identità e accessi. Un aspetto da rafforzare diventa pertanto l'adozione di strumenti IAM e di soluzioni più avanzate (strong authentication, Zero Trust, etc.).
In relazione ai controlli periodici dell'affidabilità delle protezioni, alla disponibilità di architetture di continuità del servizio, alla protezione da malware e advanced persistent threat e al controllo di reti e telecomunicazioni tradizionali, le risposte del panel suggeriscono la presenza di gap tutto sommato contenuti, vista la frequenza di citazione inferiore al 30% del campione analizzato.
Per ridurre le vulnerabilità e le debolezze che contraddistinguono ambienti e sistemi tecnologici, le aziende e gli enti stanno puntando sull'utilizzo di soluzioni dirette a rilevare possibili attacchi. In quest'ambito, ricoprono un ruolo importante soluzioni di Cybersecurity basate su algoritmi di Machine Learning.
La quota di aziende che sta già usando strumenti di questo tipo è pari al 40%, raddoppiata rispetto alla precedente edizione del Barometro (Fig. 10). Alla luce delle previsioni di un loro utilizzo a breve, dichiarate dal 47% delle aziende, tale percentuale è destinata a crescere ulteriormente.
Allo stato attuale, i casi d'uso principali di soluzioni ML-based riguardano l'ambito SIEM (Security Information and Event Management), a supporto dell'analisi degli eventi e della rilevazione in tempo reale di minacce note e sconosciute da parte dei SOC; la gestione delle frodi; i sistemi di extended detection and response e l'identificazione, correlazione e gestione di incidenti.
L'avvio di iniziative di sicurezza e l'implementazione di soluzioni abilitanti deve basarsi non solo sulla disponibilità di strutture organizzative e team ma anche e soprattutto su adeguate risorse economiche.

Figura 10:
Adozione di strumenti avanzati di analisi: Machine Learning

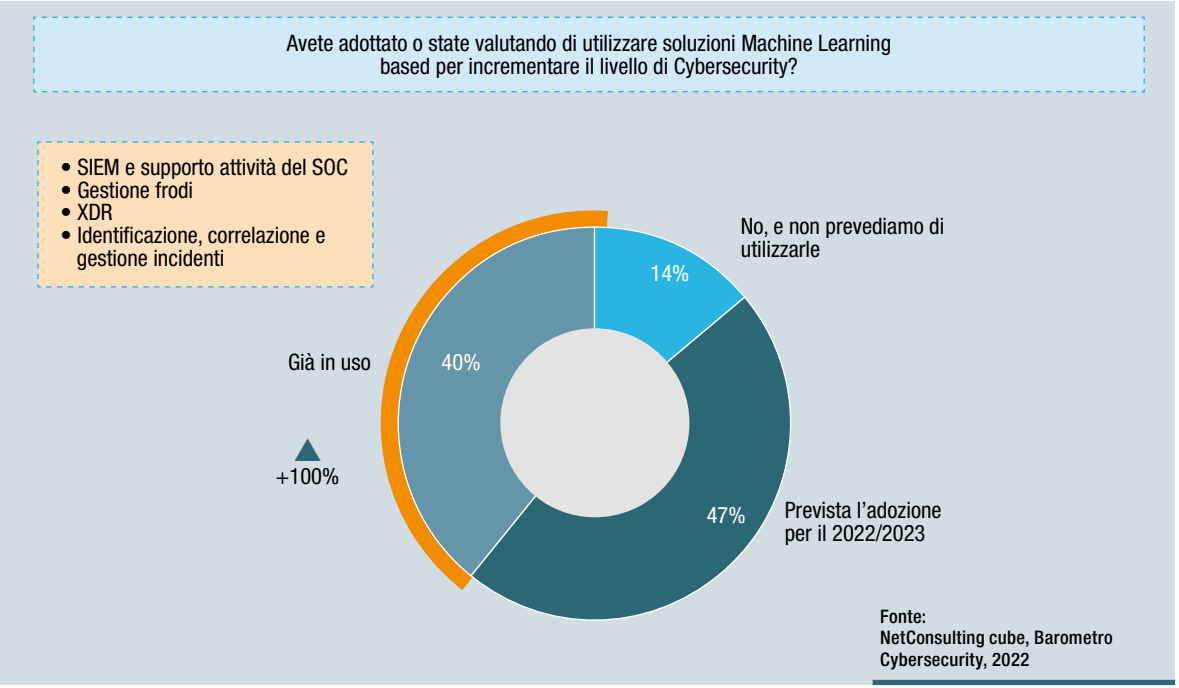
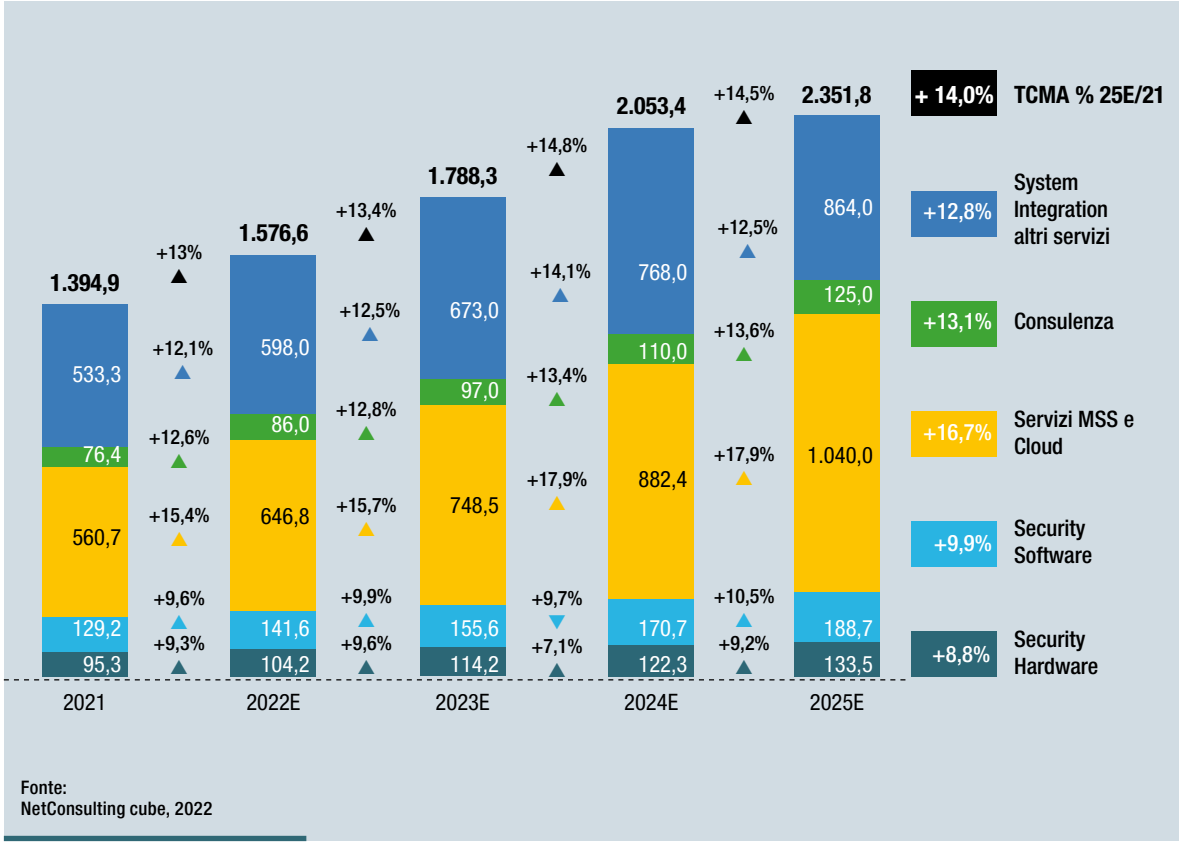


Figura 11:

Il mercato della Cybersecurity in Italia, 2021-2025E

Il trend del mercato Cybersecurity, 2021-2025

La crescita del mercato Cybersecurity proseguirà anche nei prossimi anni con dinamiche in progressivo miglioramento e un TCMA del 14% nel periodo 2021-2025.



Fonte:
NetConsulting cube, 2022

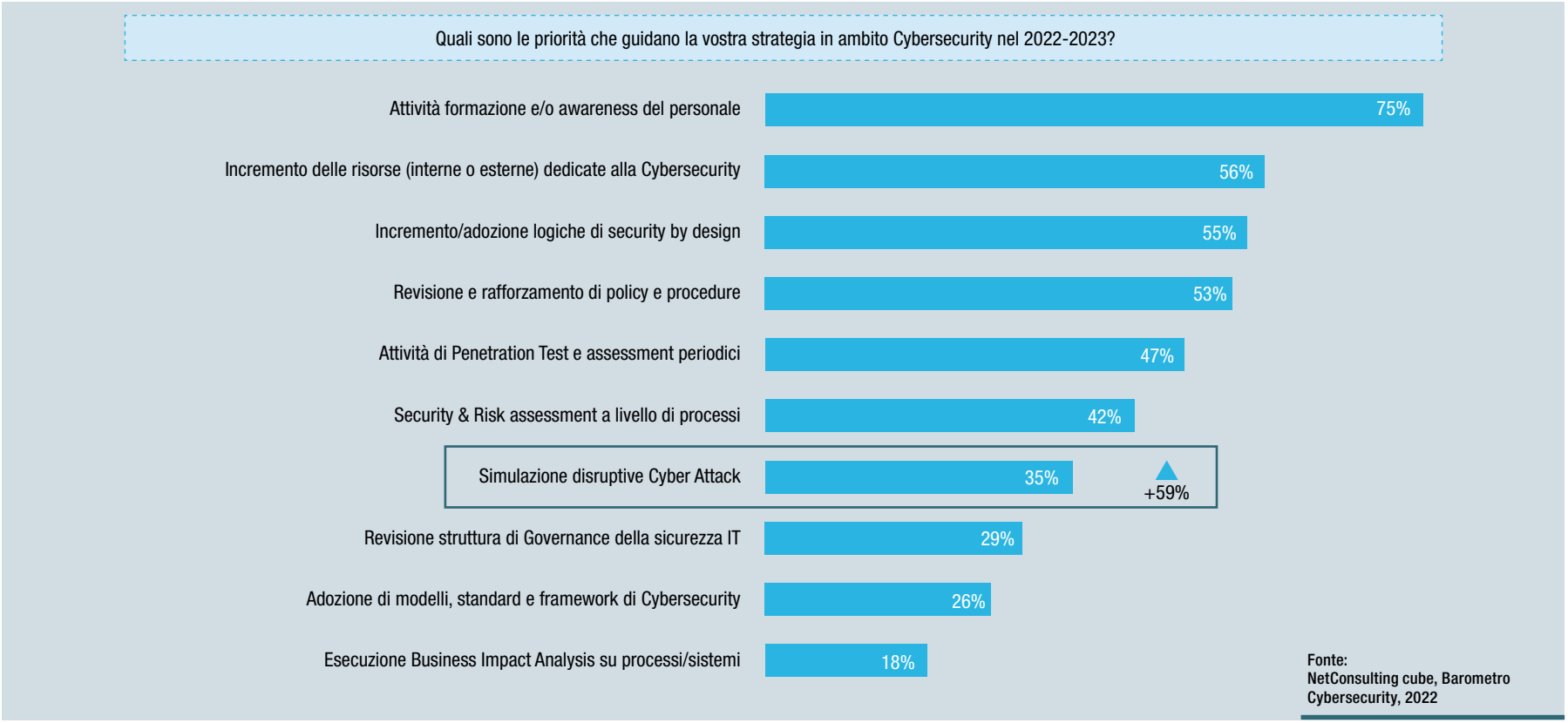
A fine 2022 la spesa dovrebbe raggiungere i 1.576 milioni di euro, con una crescita del 13,5%, continuando così a rappresentare uno dei principali driver del mercato digitale (Fig. 11).

La crescita è rilevante in tutti i segmenti del mercato, sebbene la componente con maggiore incidenza e con la dinamica più positiva sia indubbiamente quella dei Managed Security Services (MSS), in cui rientrano i servizi di Cloud Security, con un aumento previsto per il 2022 del 15,4% e un TCMA del 16,7% nel periodo considerato. La domanda di MSS è sostenuta dall'esigenza di sopperire alla carenza di risorse e competenze, che rappresenta una criticità per gran parte delle aziende, e dal ricorso a servizi di SOC esterno 24X7 per monitorare e difendere un perimetro sempre più esteso. Questo trend è rafforzato, da una parte, dalla crescente adozione del Cloud e, dall'altra, dalla costante crescita degli apparati connessi, che vanno adeguatamente protetti e monitorati.

Il secondo segmento, sempre in ordine di rilevanza sul mercato, è quello della System Integration e altri servizi, che si prevede crescerà del 12,1% nel 2022, raggiungendo quasi i 600 milioni di euro. I servizi sono correlati alla maggiore adozione di soluzioni per la governance di identità e accessi, che vanno rafforzate per gestire in modo sicuro la transizione al modello di lavoro ibrido. Nell'ambito degli investimenti indirizzati all'implementazione di soluzioni software è prevista anche una crescita dell'Endpoint Detection & Response e delle soluzioni di SIEM per poter monitorare il perimetro esteso, che sempre più va al di là di quello della singola azienda. Formazione e rafforzamento dell'awareness sono anch'essi driver importanti che sosterranno la mag-

giore domanda di servizi, così come l'adozione di politiche di security by design, finalizzate a garantire la sicurezza end-to-end nello sviluppo di nuovi servizi digitali, su cui molte aziende concentreranno i propri investimenti nei prossimi anni (Fig. 12).
La consulenza, pur crescendo a ritmi importanti (TCMA +13,1%), rappresenta una quota marginale del mercato complessivo, con un valore pari a 86 milioni di euro. I servizi maggiormente richiesti riguardano Risk e Vulnerability Assessment, che consentono di ottenere una piena consapevolezza degli ambiti maggiormente esposti e del relativo impatto in termini di rischio. In aumento, come negli anni precedenti, anche la consulenza indirizzata a risolvere le situazioni di criticità conseguenti ad attacchi.

Figura 12:
Le principali priorità in ambito Cybersecurity



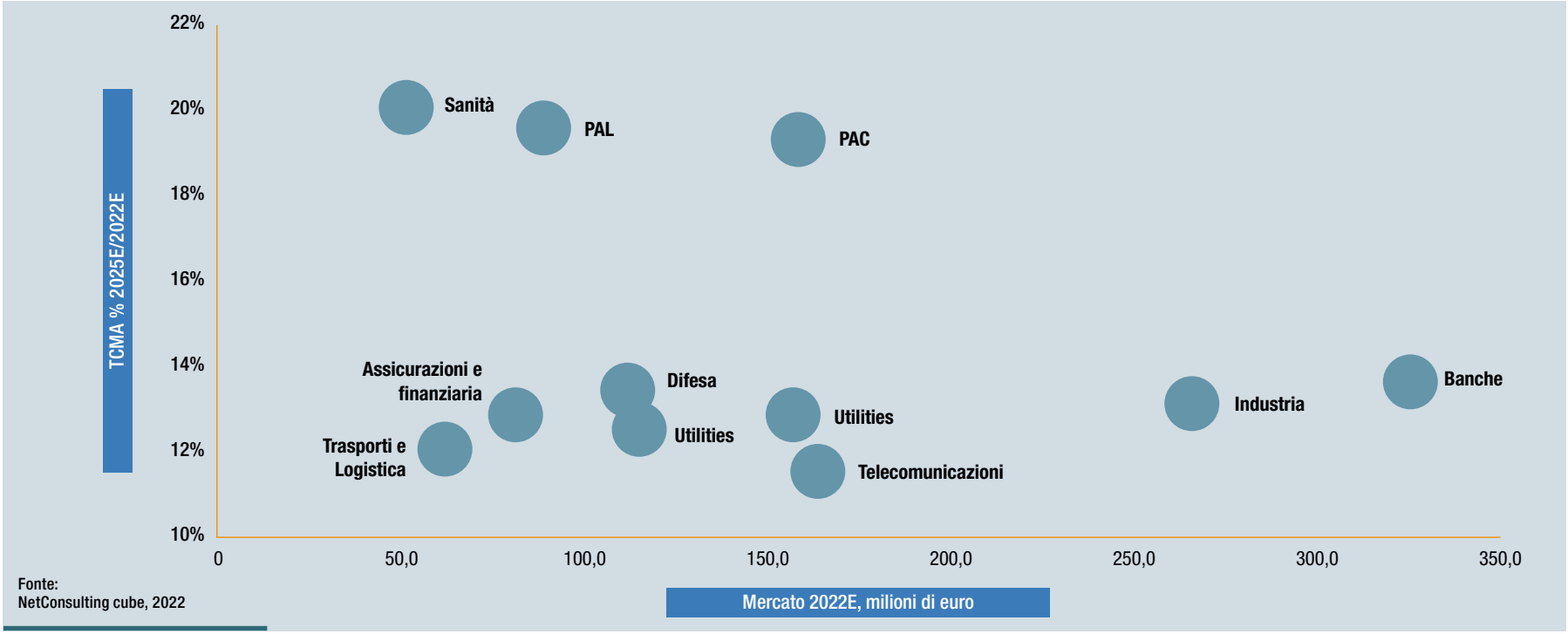
Fonte:
NetConsulting cube, Barometro Cybersecurity, 2022

La spesa in Cybersecurity nei settori dell'economia

La domanda di servizi e soluzioni di Cybersecurity è in crescita in tutti i settori, sebbene sia da evidenziare come la Pubblica Amministrazione, centrale e locale, insieme alla sanità, rappresentino gli ambiti in cui si prevede un incremento maggiore, trainato dall'esigenza di supportare la transizione digitale di enti e aziende sanitarie con misure e dotazioni adeguate sul fronte della Cybersecurity.

L'aumento previsto, che si attesta in termini di TCMA tra il 19% della PAC e della PAL, e il 20% della sanità, è determinato principalmente dall'esigenza di colmare un ritardo accumulato negli anni e ormai non più sostenibile (Fig. 13). La crescita del mercato riceverà inoltre una forte spinta dal PNRR, che prevede investimenti per 623 milioni di euro indirizzati verso molteplici interventi, tra cui la creazione ed il rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese e dei presidi di front-line per la gestione degli alert e degli eventi a rischio verso la PA e le imprese di interesse na-

Figura 13:
L'andamento della spesa Cybersecurity nei settori, 2022E-2025E



Fonte:
NetConsulting cube, 2022

zionale. Nel corso del 2022, per supportare questo cambio di passo, la Consip ha attivato Accordi quadro e indetto bandi per complessivi 714 milioni di euro, tra cui l'attivazione del Lotto 2 "Servizi di compliance e controllo" e, successivamente, del Lotto 1 dell'Accordo quadro "Servizi di sicurezza da remoto" – valore totale di 468 milioni di euro – che offre alle Amministrazioni un insieme articolato di servizi di sicurezza erogati "da remoto" (presso il fornitore) per la protezione di infrastrutture, applicazioni e dati.

Il nuovo contratto si affianca a quello già attivo da marzo che ha per oggetto servizi di sicurezza "on premise" per la protezione dei dati e delle applicazioni in uso alle PA, attraverso i quali le amministrazioni possono acquisire prodotti per la gestione degli eventi di sicurezza e degli accessi, per la protezione dei canali email, web e dati.

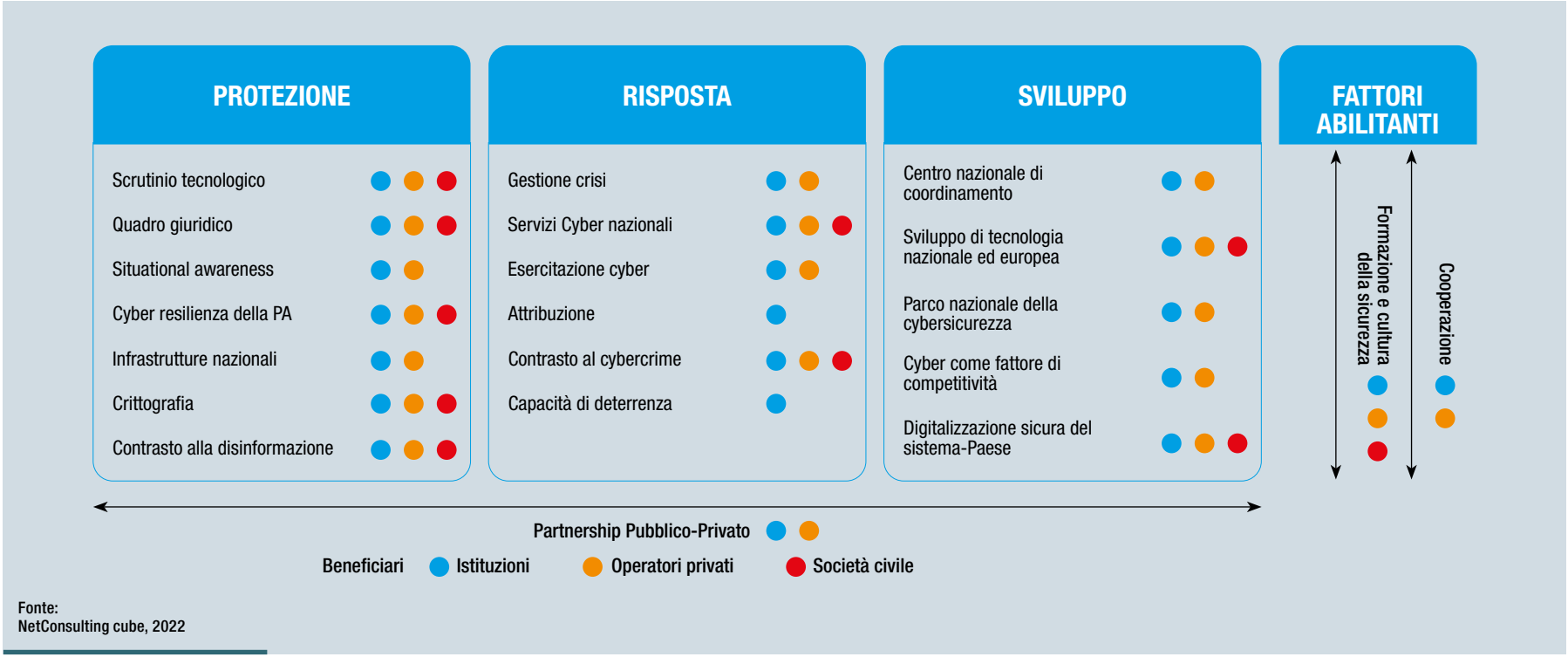
Nei settori privati la crescita prevista, sebbene più contenuta, è comunque significativa. I top spender sono le aziende del settore bancario, che complessivamente raggiungerà all'incirca i 324 milioni di euro nel 2022 (TCMA +13,2%). Le banche sono più mature dal punto di vista organizzativo e della governance e stanziano verso la Cybersecurity importanti budget. Security by design, rafforzamento della sicurezza negli ambienti Cloud, data protection e miglioramento della sicurezza nel digital workspace sono gli ambiti principali di investimento in questo settore.

A seguire l'industria, che ha visto una crescita significativa degli attacchi indirizzati verso le aziende leader di alcune filiere, e che si prevede raggiungerà i 264 milioni di euro e una crescita media annua del 13,1%. Le aziende industriali si focalizzeranno sul rafforzamento della sicurezza sugli endpoint e sull'estensione delle soluzioni di Disaster recovery e back up and restore, per poter affrontare al meglio gli attacchi ransomware e DDoS. Un ambito molto critico continua ad essere rappresentato dalla Supply chain e dall'Industrial IoT, dove al crescere del numero dei dispositivi connessi aumenta sia l'esigenza di mapparne le interconnessioni che la ricerca di strumenti adeguati che consentano di individuare tempestivamente vulnerabilità e relativi rischi di compromissione.

Tra gli altri settori più maturi si segnalano le tele-

comunicazioni, la difesa e le utilities, con una spesa che raggiungerà rispettivamente i 164 milioni di euro, i 111 milioni e i 116 milioni di euro. In questi settori, ad eccezione della difesa che rappresenta un comparto a sé stante, rientrano soggetti che forniscono servizi essenziali che già da diverso tempo hanno intrapreso strategie volte a potenziare le misure di sicurezza.
Il settore Retail e servizi rappresenta un ambito molto eterogeneo e frammentato con una spesa media in Cybersecurity assai contenuta, pur raggiungendo complessivamente un valore pari a 156 milioni di euro, con una crescita superiore al 12%; un dato che però risulta ancora insufficiente se si pensa ai gap da colmare.
Infine, i comparti delle assicurazioni e dei trasporti e della logistica evidenziano una spesa in aumento ma inferiore in termini assoluti, segnalando così un approccio di non piena consapevolezza verso i temi Cyber.

Figura 14:
Obiettivi della strategia di cybersicurezza nazionale



Fonte:
NetConsulting cube, 2022

La strategia di cybersicurezza nazionale

Nell'ambito degli obiettivi del PNRR, che prevedono il rafforzamento dei presidi front-line, rendendo più solide le capacità di valutazione e audit della sicurezza delle applicazioni e degli apparati elettronici e definendo l'architettura dell'intero ecosistema della cybersecurity nazionale (M1C1-6), il Comitato interministeriale per la cybersicurezza ha approvato la strategia nazionale di cybersicurezza 2022-2026. Si prevede, inoltre, per aumentare il livello di protezione della Pubblica Amministrazione dai rischi posti dalla criminalità informatica, l'avvio e l'attivazione dei laboratori di screening e certificazione della Cybersecurity (M1C1-7); l'Agenzia per la cybersicurezza ha avviato le procedure di reclutamento del personale ed è in corso la definizione degli accordi con i ministeri della Difesa e dell'Interno per l'integrazione dei rispettivi centri di valutazione.
Per implementare la presente strategia e affrontare le molteplici sfide in ambito Cybersecurity, al di là degli strumenti finanziari già assegnati alle Amministrazioni con competenza in materia cyber, potranno anche essere messi a disposizione appositi fondi previsti di anno in anno dalle leggi finanziarie, per supportare specifici progetti di interesse. A tale fine sarà riservata una quota, pari all'1,2%, degli investimenti nazionali lordi su base annuale. Saranno previsti anche sgravi fiscali per le aziende o l'introduzione di aree nazionali a tassazione agevolata per la costituzione, ad esempio, di un "parco nazionale della cybersicurezza" e dei relativi "hub" delocalizzati sull'intero territorio nazionale.

Per fronteggiare al meglio le sfide sono stati individuati tre obiettivi fondamentali – Protezione, Risposta e Sviluppo – con le relative misure, per consentire la concreta attuazione della strategia, raggruppate per aree tematiche e declinabili sia dal punto di vista organizzativo e di policy che prettamente operativo (Fig. 14).
L'obiettivo della Protezione sarà raggiunto mediante l'istituzione dei Centri di Valutazione e Certificazione, l'evoluzione del quadro giuridico e normativo, la

capacità di comprendere lo scenario cyber, la cyberesilienza della PA, la difesa delle infrastrutture critiche, la crittografia e il contrasto alla disinformazione.

Un tema sicuramente strategico riguarda il potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione, per realizzare una trasformazione digitale sicura e resiliente. A tal fine, la transizione verso il Cloud della Pubblica Amministrazione, sia verso tecnologie di Public Cloud che mediante la creazione di un Polo Strategico Nazionale (PSN), rappresenta il principale fattore per garantire adeguate garanzie di autonomia tecnologica del Paese. Tale transizione dovrà essere guidata e controllata da una metodologia di gestione del rischio basata sulla classificazione dei dati e dei servizi della Pubblica Amministrazione (ordinari, critici e strategici). Al riguardo saranno altresì coordinati interventi di potenziamento delle capacità di identificazione, monitoraggio e controllo del rischio cyber nella PA.

L'obiettivo di Risposta si articola in un sistema di gestione di crisi cibernetica nazionale – assicurato dal Nucleo per la Cybersicurezza (NCS) – e transnazionale, fondato su procedure di collaborazione consolidate e supportate da costanti flussi informativi e da elementi di conoscenza condivisi anche grazie a reti e infrastrutture nazionali e transnazionali, tali da coinvolgere le Amministrazioni e gli operatori privati interessati.

Nelle azioni previste rientra anche la realizzazione di Hyper SOC, ovvero un sistema di raccolta, correlazione e analisi di eventi di interesse da Security Operation Center, nonché dagli Internet Service Provider (ISP) mediante apposite convenzioni, al fine di individuare tempestivamente eventuali "pattern" di attacco complessi che potrebbero rappresentare minacce emergenti.

Altre azioni previste sono:

- la modalità di notifica unitaria degli incidenti di sicurezza cibernetica al Computer Security Incident Response Team (CSIRT), per rendere più efficace la capacità di reazione e di allarme tempestivo;
- la risposta agli incidenti attraverso la realizzazione di una rete di CSIRT/Computer Emergency Response Team (CERT) settoriali federati con lo CSIRT Italia per la condivisione di procedure, informazioni e supporto nella reazione alle minacce emergenti e agli incidenti;
- la realizzazione di un Information Sharing and Analysis Center (ISAC) centrale presso l'Agenzia, integrabile con una rete di ISAC settoriali sviluppati mediante iniziative pubblico-private, che possa potenziare la diffusione e l'applicazione di best practice di settore, linee guida, avvisi di sicurezza e raccomandazioni;
- la qualificazione di aziende in materia di incident response, in grado di fornire supporto allo CSIRT Italia nel caso in cui dovesse verificarsi una moltitudine di incidenti cyber di natura sistemica.

L'obiettivo Sviluppo si basa infine sul potenziamento consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze del mercato. La costellazione di centri di eccellenza e imprese che compongono, assieme all'accademia, il tessuto della ricerca e dello sviluppo è infatti un patrimonio essenziale per il nostro Paese, con importanti potenzialità di espansione. A tale scopo un ruolo

centrale sarà svolto dal Centro Nazionale di Coordinamento (NCC) che, in stretto raccordo con il Centro Europeo di Competenza per la Cybersicurezza in ambito industriale, tecnologico e della ricerca (ECCC), è chiamato a supportare lo sviluppo dell'autonomia strategico-tecnologica e digitale dell'Unione Europea e del nostro Paese. L'obiettivo finale è la creazione di un'industria tecnologica europea competitiva, capace di poter conquistare autonomia rispetto agli operatori extra europei.
La strategia prevede inoltre la realizzazione di un "parco nazionale della cybersicurezza" che consenta di mettere a sistema competenze e risorse provenienti dal pubblico, dall'industria e dal mondo accademico e della ricerca, fornendo tutte le infrastrutture tecnologiche necessarie allo svolgimento di attività di ricerca e sviluppo nell'ambito della cybersecurity e delle tecnologie digitali quali, a titolo di esempio, l'intelligenza artificiale, il quantum computing, la crittografica e la robotica.
Formazione specialistica, promozione della cultura della sicurezza cibernetica, al fine di aumentare la consapevolezza del settore pubblico e privato e della società civile sui rischi e le minacce cyber, e infine la collaborazione, anche attraverso forme di partenariato pubblico-privato, rappresentano elementi fondamentali per poter conseguire gli obiettivi delineati nella strategia nazionale di Cybersecurity.

Note:
1. Fonte: Rapporto Clusit 2022.
2. Fonte: Rapporto Clusit 2022.

CYBERSECURITY IN OSPEDALE

di Gianluca Cesare
Chief Information Officer,
Humanitas

Il settore sanitario pubblico e privato è tra i più colpiti da attacchi informatici: secondo il **Data Breach Investigations Report 2021 di Verizon**, che ha analizzato 79.635 incidenti e 5.258 violazioni (*data breach*) conclamate in 88 Paesi in un anno, gli attacchi informatici "ransomware" (ovvero i virus che prendono in ostaggio PC e smartphone criptando i relativi dati e chiedendo di pagare un riscatto per decriptarli) contro il settore sanitario sono passati **dal 17% al 24%**. Gli attacchi al settore hanno principalmente una **motivazione di tipo economico** (91%), sebbene comincino ad emergere anche altre finalità, quali ad esempio lo **spionaggio industriale**.

Principalmente **gli incidenti di sicurezza compromettono dati sanitari** (55%) e dati personali dei soggetti interessati (66%). Aspetto non meno importante, il settore sanitario risulta l'unico in cui **le violazioni sono causate da un alto valore di fattori/agenti interni** (39%) oltre che da agenti esterni (61%), anche a causa di pratiche poco idonee nel trattamento dei dati critici sanitari, per limitata consapevolezza o sottovalutazione della necessità di adottare appropriate cautele e misure di sicurezza.

Nel biennio 21-22 negli ospedali, gli attacchi Cyber sono cresciuti enormemente, con volume di affari per i "Banditi Digitali" che nell'ultimo anno ha raggiunto i 20 miliardi di euro in riscatti e tuttora in forte crescita!

Tra i casi internazionali più noti si ricordano quello al sistema sanitario britannico nel 2019 (603 strutture bloccate, 92 milioni di sterline di danni e 20mila cancellazioni) e quello al sistema sanitario irlandese nel 2021 (80% dei computer bloccati e nessun dato clinico accessibile, 5 milioni di pazienti danneggiati, danno di 100 milioni di euro e riscatto richiesto di 20 milioni). L'attacco alla sanità irlandese è stato perpetrato da "Conti", lo stesso gruppo di hacker che ha colpito 16 volte la sanità USA. Nel 2021 in Italia sono state attaccate con successo le strutture sanitarie di Ospedale San Giovanni di Roma, aziende ospedaliere della Regione Lombardia, aziende ospedaliere della Regione Toscana, ASL Roma 3, ASL di Padova, Regione Lazio (con impatto sul piano di somministrazione delle vaccinazioni anti-Covid) e Comune di Brescia.

Contesto normativo

Nonostante il contesto normativo sia piuttosto chiaro e definito attraverso la Direttiva europea NIS 2016/11448 e NIS 2 del 2021 recepita dai singoli Governi, almeno in Italia rimangono ancora da definire alcuni elementi delle modalità attuative. Attraverso il Cybersecurity Act 2019, la Legge 18/2019 ed i successivi DPCM del 2021 è stata recepita la Direttiva europea, quale base dell'inquadramento normativo, definendo gli organi competenti (ACN, CSIRT, CVCN) e le organizzazioni che sono parte del cosiddetto perimetro di Cybersicurezza Nazionale, in particolare per quelle che sono definite "OSE" ovvero **Organizzazioni Erogatrici di Servizi Essenziali, tra cui è inquadrata la Sanità, con chiari obblighi di legge.**

I principali adempimenti richiesti dal D.L. 105/2019 e dai sopracitati DPCM sono obblighi di informazione, per permettere allo Stato di utilizzare efficacemente i propri poteri di controllo e intervento in caso sopraggiungano ragioni di sicurezza nazionale, e misure per mantenere elevati livelli di sicurezza:

- **comunicazione del perimetro di sicurezza:** dai soggetti coinvolti alle reti/sistemi/servizi informatici (architettura e componenti), all'organizzazione di Cybersicurezza interna all'ospedale (include la revisione organizzativa e dei processi);
- **comunicazione degli incidenti di sicurezza** aventi impatto su reti, sistemi e servizi informatici, entro un'ora dal momento in cui se ne viene a conoscenza per incidenti più gravi e sei ore per i meno gravi;
- **costituzione del CVCN** (Centro di Valutazione e Certificazione Nazionale). Per la certificazione di acquisti di beni e servizi e delle qualifiche degli incaricati dell'organizzazione, validazione tecnica e collaudo delle soluzioni di Cybersicurezza interna e validazione acquisti in perimetro. Al momento non è stato ancora pubblicato il DPCM relativo alla creazione di una rete di laboratori pubblico-privata per coadiuvare le attività del CVCN (Centro di Valutazione e Certificazione Nazionale);
- **introduzione di un nuovo reato, con varie soglie e penali per i mancati adempimenti degli obblighi di comunicazione e notifica** di incidenti, infrastrutture, misure tecniche e misure di sicurezza, nonché l'impiego di prodotti e servizi non certificati e la mancata collaborazione per l'effettuazione delle attività di test e delle attività di ispezione e verifica.

Tipologie di rischio cyber nel settore sanitario

L'utilizzo pervasivo dell'ICT all'interno dei processi operativi ospedalieri espone a rischi di attacchi informatici sempre più frequenti e sofisticati.
La disponibilità di informazioni tempestive e accurate, processate attraverso l'utilizzo di sistemi informativi evoluti e affidabili, implica anche una maggiore vulnerabilità degli Ospedali **alle minacce informatiche messe in atto da attori interni e/o esterni malevoli** pur a fronte di **regolamentazioni stringenti** che hanno ricadute dirette sul sistema di protezione e sicurezza delle informazioni di cui le strutture sanitarie sono tenute a dotarsi.[1]
L'anello debole continua ad essere la posta elettronica, attraverso la quale vengono effettuati attacchi ransomware, che sono raddoppiati rispetto al 2020, e campagne di phishing (la vittima è ingannata per convincerla a fornire informazioni personali, dati finanziari o codici di accesso), che rappresentano il 91% degli attacchi con riscatto e il 61% di tutte

le violazioni. Altro elemento di vulnerabilità è l'utilizzo diffuso di **dispositivi biomedicali connessi in rete**, ma abilitati da sistemi operativi e database obsoleti con politiche di gestione degli accessi logici poco robuste, che diventano facile punto di ingresso per chi vuole comprometterne il funzionamento e/o acquisire informazioni dei pazienti.

In un contesto complesso e significativamente regolamentato come quello sanitario, i **principali rischi** cui le aziende ospedaliere sono esposte includono:

- **furto di proprietà intellettuale**, su segreti industriali derivanti da ricerche mediche commissionate dalla struttura sanitaria e i cui risultati risiedono sui server aziendali e/o sui dispositivi dei ricercatori;
- **danni di natura reputazionale**, per screditare di fronte all'opinione pubblica l'operato dell'azienda ospedaliera;
- **furto di identità**, con l'accesso illecito ai record che contengono le informazioni personali dei pazienti valutati a un prezzo unitario di circa 500 dollari sul mercato nero, secondo una ricerca del Ponemon Institute;[2]
- **danni alla salute dei pazienti**, compromettendo il corretto funzionamento di dispositivi di diagnostica e somministrazione di cure mediche o modificando in maniera non autorizzata le informazioni mediche dei pazienti nel fascicolo sanitario generando procedure e terapie non coerenti con i veri sintomi da curare;
- **danni di natura operativa**, compromettendo il funzionamento dei sistemi informativi aziendali a supporto dei processi operativi (Denial of Service del sistema di accettazione) e/o dei dispositivi di diagnostica;
- **rischio di incorrere in sanzioni regolamentari** per non ottemperanza alle normative di riferimento (General Data Protection Regulation Europeo ed Direttiva NIS 2).

Di fatto, direttamente o indirettamente, ciascuna delle tipologie di rischio sopra esposte ha un **impatto di natura economica** sulla struttura sanitaria, in termini di perdita di ricavi (per diminuzione di prestazioni sanitarie erogate e di pazienti allontanatisi per sfiducia o per danni diretti ad essi cagionati) e/o aumento di costi (per *recovery* dei dati oggetto di attacco).

Organizzazione della Cybersecurity negli ospedali

Nell'ottica di garantire al minimo la postura di Cybersicurezza di un ospedale, occorre che la struttura sia vista come un presidio non solo dei Sistemi Informativi in quanto erogatori del servizio informatico, ma anche dei più alti vertici aziendali (Direzione Sanitaria e Direzione Generale). Essenziale, in questo senso, per le strutture ospedaliere è l'adozione di un vero e proprio Cyber Security Master Plan.

Un valido riferimento è offerto dal **Framework Internazionale per la Gestione di Infrastrutture Critiche del National Institute of Standards and Technology (NIST)**,[3] dall'utilizzo diffuso in USA e fondato su un approccio olistico di 5 Core Functions (Identify, Protect, Detect, Respond, Recover) per indirizzare i requisiti minimi di Cybersecurity per le infrastrutture critiche.

Questo *framework* può essere declinato per i processi ospedalieri secondo gli interventi definiti per ciascuna delle cinque Core Function nella tabella seguente.

Principali interventi suddivisi sulle 5 Core Function NIST

Core Function	Descrizione	Area di intervento	Principali interventi
Identity	Attività finalizzate allo sviluppo delle capability organizzative e di governo per **identificare e gestire** i cyber risk	Organizzazione	Costituzione di un board per la continuità di erogazione ospedaliera in caso di attacco Hacker e definizione del PdCO Piano di Continuità Ospedaliera Introdurre la figura/funzione (Chief Information Security Officer) preposta alla gestione della Cyber Security
		Cyber Risk Management	Definizione e implementazione di un processo di Cyber Risk Management inclusivo della fase di Cyber Risk Assessment
		Policy & Procedure	Formalizzazione di un set di politiche e procedure di sicurezza sulle seguenti tematiche: • Access Management • Patch & Vulnerability Management • Change & Configuration Management • Network Security • Log Management • Data Classification • Mobile Security incluso tema del Bring Your Own Device (BYOD) • Backup & Restore • Physical Security
		Asset Management	Censimento del parco HW/SW aziendale utilizzando appositi strumenti di Asset Discovery & Management
		Cyber Security Training & Awareness	Definizione e implementazione di un programma di formazione in modalità e-learning sulla sicurezza delle informazioni a tutto il personale; Campagne di comunicazione mirate ai dipendenti e a tutti gli utenti del sistema informativo aziendale, almeno trimestrali, aventi lo scopo di sensibilizzare l'utenza sul tema della protezione dei propri asset da e-mail di phishing, di Business compromise, man in the middle, DDOS, …
		Supply Chain Risk	Definizione di un set di controlli sulle terze parti (security baseline) e di un piano di verifiche progressivo sui fornitori critici in ottica Cybersecurity, da integrare nel processo complessivo di Cyber Risk Management

Protect	Attività finalizzate al disegno e all'implementazione di misure di sicurezza in grado di **prevenire** gli attacchi Cyber	Identity & Access Management	Definizione e implementazione di un processo di review delle utenze e dei profili autorizzativi sui principali sistemi applicativi, incluse le utenze di amministrazione di sistema
		Vulnerability Management	Effettuazione di attività periodiche (cadenza almeno annuale) di Vulnerability Assessment (VA) e Penetration Testing (PT)
		Physical & Environmental Security	Revisione delle misure di sicurezza fisica e ambientale dei Data Center
		Upgrade tecnologico	Aggiornamento dell'infrastruttura tecnologica ICT (client, server, apparati di rete) e di sicurezza (firewall, antivirus/ antispam, IPS/IDS). Tale task abilita la sicurezza complessiva delle informazioni garantendo l'enforcement delle policy definite
Detect	Attività finalizzate al disegno e all'implementazione di misure di sicurezza in grado di **rilevare** tempestivamente gli attacchi informatici	Security Operation Center (SOC) / Security Event Monitoring	Definizione puntuale del perimetro dei servizi in carico al SOC ad attività di threat intelligence e behavioural analysis
		Threat Management	
Respond	Attività finalizzate a disegno e implementazione di misure di sicurezza in grado di **rispondere** agli attacchi informatici	Security Incident Response Planning	Definizione e implementazione da parte della Direzione Aziendale di un processo di gestione degli incidenti di sicurezza di concerto con i Sistemi Informativi, il SOC
Recover	Attività finalizzate al disegno e all'implementazione di misure di sicurezza in grado di **ripristinare** un processo e/o un servizio a seguito di attacchi informatici	Disaster Recovery/ Business Continuity & Crisis Management	Disegno di un Disaster Recovery Plan (DRP) preliminare all'implementazione degli interventi tecnici necessari a garantire la continuità operativa in tempi non critici per il business a seguito di failure dei sistemi Implementazione delle misure tecniche previste nel piano di Disaster Recovery Disegno di un Business Continuity Plan (che integri il DRP) effettuando preliminarmente una Business Impact Analysis (BIA)

Conclusioni

La sanità è uno dei principali settori oggetto di attenzione da parte degli Hacker, al pari delle organizzazioni finanziarie e delle banche, poiché, pur non disponendo direttamente di fondi e non gestendo rilevanti transazioni economiche, per via di una sempre più alta digitalizzazione dei processi di cura dei pazienti, dispone di informazioni personali e sensibili dei pazienti in formato digitale "Medical Records" che hanno un controvalore economico nel cosiddetto "Darkweb".

Organizzazioni criminali vendono e acquistano Medical Records (MR) nel Darkweb ad un controvalore di circa 500 dollari per MR. Altre organizzazioni non sono interessate ai dati ma a attacchi mirati a organizzazioni sanitarie in quanto infrastrutture critiche di una nazione, così come peraltro individuato dal quadro normativo di riferimento. Nei prossimi tre-cinque anni la Cybersicurezza sarà prioritaria negli investimenti per i Sistemi Informativi ospedalieri. Ma è anche necessario che gli operatori che lavorano in Sanità (Healthcare Provider Operators) definiscano la propria organizzazione di Cybersecurity ispirandosi ad un framework valido di riferimento (reso disponibile anche in ambito internazionale) che ne assicuri il completo allineamento con il contesto normativo nazionale.

La **Cybersicurezza** non è quindi esclusivamente un presidio tecnologico ma il riferimento di un **modello gestionale organizzativo da adottare**, che coinvolge l'intera azienda ospedaliera, dai vertici sino a tutti gli operatori, in qualità di attori dei processi / servizi digitali, e ai pazienti stessi, in quanto fruitori di essi.

Nella consapevolezza che il raggiungimento di un livello di sicurezza totale è molto arduo, poiché comporterebbe un impegno estremamente rilevante in termini organizzativi, operativi e finanziari, è indispensabile comunque commisurare gli impegni al grado di rischio accettabile che un ospedale ritiene di voler assumere.

Note:

1. Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, General Data Protection Regulation (GDPR) europeo, NIS e NIS 2.
2. Ponemon Institute, The State of Cybersecurity in Healthcare Organizations in 2016.
3. Framework for Improving Critical Infrastructure Cybersecurity - National Institute of Standards and Technology (NIST), versione 1.1, Aprile 2018.

CYBERSICUREZZA: IL CASO ENEL

di Francesco Paolo Landolfo
Head of Cyber Security Strategy, Reporting, Risk Analysis and Awareness, Enel

La transizione energetica richiede alle utility di evolvere e diventare orchestratori di un sistema complesso, caratterizzato da molteplici attori e asset distribuiti. Le tecnologie digitali permettono di gestire questo nuovo paradigma, migliorando l'efficienza e l'efficacia dei processi di business. In Enel, a guidare la trasformazione digitale è l'unità Global Digital Solutions, che, insieme a tutte le Linee di Business e Funzioni di Holding, indirizza le scelte strategiche, definisce i percorsi di sviluppo e ne garantisce l'attuazione. Dal 2015 lavoriamo per semplificare la nostra mappa applicativa attraverso lo sviluppo di tecnologie digitali globali, utilizzabili trasversalmente lungo l'intera catena del valore, e promuoviamo lo sviluppo e l'adozione di modelli operativi a piattaforma nell'intera organizzazione, abilitati dalla completa migrazione sul Cloud avvenuta nel 2019. Il Cloud, infatti, rappresenta un abilitatore strategico fondamentale che consente l'utilizzo efficiente di risorse informatiche, sia infrastrutturali sia applicative, permettendo di supportare efficacemente le direzioni strategiche di business del Gruppo.

In questa era di trasformazione digitale, la Cybersecurity ha assunto un ruolo fondamentale per garantire l'operatività delle imprese. Le tipologie di attacchi informatici sono cambiate drasticamente negli ultimi anni: il numero è cresciuto in modo esponenziale, così come il loro grado di sofisticazione e impatto. Ad evolvere è anche la **rilevanza dei soggetti verso i quali gli attacchi sono diretti**, che risultano essere società, istituzioni o organizzazioni di rilievo e fornitrici di servizi critici ed essenziali. Inoltre, la pandemia da Covid-19 ha portato a un ulteriore incremento degli eventi di sicurezza in tutto il mondo, anche considerando la necessità di operare in modalità di lavoro agile e di fare uso di reti domestiche.

Il Gruppo Enel, in linea con le esigenze del settore industriale energetico e in coerenza con la sua strategia di digitalizzazione, ha pertanto adottato una **visione sistemica dei temi della Cybersecurity**, nonché una strategia globale di analisi, prevenzione e gestione degli eventi di sicurezza informatica. Il percorso della sicurezza informatica a supporto della trasformazione digitale del Gruppo si basa sulla definizione, valorizzazione e adozione di un modello di governance, infrastrutture e servizi di sicurezza, al fine di sfruttare al meglio le opportunità disponibili, anche coadiuvate da tecnologie all'avanguardia, per aumentare la resilienza informatica di infrastrutture e applicazioni. Da settembre 2016, all'interno di Global Digital Solutions è stata costituita **l'unità di Cyber Security**, a diretto riporto del Chief Information Officer (CIO), e il cui responsabile ricopre il ruolo di Chief Information Security Officer (CISO) del Gruppo. L'unità è impegnata a garantire la governance, la direzione e il controllo delle tematiche di sicurezza informatica, la definizione della strategia, delle policy e delle linee guida, in conformità con le normative nazionali e internazionali, il supporto di ingegneria per la protezione degli ambienti del Gruppo, il monitoraggio della "risk posture" mediante controlli basati su processi e tecnologia, e ancora il presidio e l'implementazione dei requisiti di *compliance* derivanti da normative in tema di Cybersecurity, unitamente all'adozione delle soluzioni tecniche e all'adozione di procedure volte alla mitigazione di possibili debolezze rilevate. Per garantire il giusto presidio delle tematiche di sicurezza informatica a livello executive, è stato istituito il **Cyber Security Committee**, presieduto dal CEO di Gruppo e composto dalle sue prime linee. Questo organismo approva la strategia di sicurezza informatica e controlla periodicamente i progressi della sua attuazione. Inoltre, l'unità Cyber Security lavora in **sinergia** con le **Linee di Business** e con le **unità tecniche** responsabili della progettazione e gestione del ciclo di vita di sistemi ed applicazioni digitali, grazie al concepimento di specifiche figure che consentono l'integrazione quotidiana nei processi: lato business tramite i **Cyber Security Risk Manager** e lato tecnico tramite i **Cyber Security Response Manager**. In questo modo, tutte le aree partecipano attivamente all'attuazione della strategia di sicurezza informatica attraverso un piano operativo integrato e allineato agli obiettivi del Gruppo.

In Enel, elemento cruciale della gestione del rischio Cyber è il **Cyber Security Framework** (nel seguito "Framework"), policy di Gruppo definita e adottata fin dal 2017, che indirizza i principi e i processi operativi che sono a supporto di una strategia globale di analisi, prevenzione e gestione dei rischi. Tale Framework, che recepisce i principali standard internazionali e le migliori pratiche di settore, è trasversalmente applicabile al più tradizionale settore dell'Information Technology (IT, dal Cloud al Data Center e al cellulare), così come agli ambienti di Operational Technology (OT, tutto ciò che riguarda il settore industriale, come il telecontrollo degli impianti), e dell'Internet of Things (IoT, l'estensione della comunicazione e dell'intelligenza digitale al mondo degli oggetti). Il Framework:

- definisce puntualmente **8 processi** per la **piena gestione della sicurezza informatica** in tutte le aree del Gruppo;
- è strutturato in processi pienamente applicabili a tutti i **contesti operativi e tecnologici** del Gruppo;
- definisce **ruoli e responsabilità** attuando il pieno coinvolgimento delle aree di business, costituendosi solida base per la **piena fusione di tecnologie, processi e persone**.

Inoltre, il Framework dettaglia i responsabili e le responsabilità di ogni processo e sotto processo (tramite apposite matrici RACI) assicurando il posizionamento corretto delle decisioni strategiche nell'organigramma societario e il rispetto delle prescrizioni di sviluppo sicuro attraverso due approcci e principi di cardinale importanza:

- **approccio risk-based** che pone la valutazione del rischio come prerequisito per le decisioni strategiche e per lo sviluppo e il mantenimento sicuro di tutti gli asset dell'organizzazione;

- **principio di cyber-security-by-design** che mira a garantire l'adozione dei principi di sicurezza informatica sin dall'inizio e durante l'intero ciclo di vita delle soluzioni, servizi e infrastrutture IT / OT / IoT.

Contestualmente alla definizione del Framework, con l'obiettivo di abilitare in maniera strutturata ed efficace l'approccio "risk-based" appena menzionato, nel 2017 è stata definita anche la **metodologia di Cyber Security Risk Management**, anch'essa applicabile a tutti gli ambienti IT, OT e IoT, che racchiude tutte le fasi necessarie per effettuare l'analisi dei rischi e definire il relativo piano di mitigazione, in coerenza con gli obiettivi stabiliti.

Tutti i progetti, i programmi e le iniziative di Cybersecurity mirano a evitare, mitigare o porre rimedio ai rischi di sicurezza informatica per l'intero Gruppo. Di conseguenza, tutte le attività, gestite con un approccio "risk-based" e secondo il principio di "security by design", generano un processo di *due diligence* continuo che include anche attività di *self assurance*.

In termini di innovazione e digitale, il Gruppo Enel promuove un approccio di **Open Innovation**, tramite la funzione di **Innovability®**, per affrontare le sfide della transizione energetica: l'innovazione rappresenta infatti lo strumento per raggiungere l'obiettivo di essere sostenibili. Gli Innovability® manager sono presenti in ogni funzione di Staff e Business Line del Gruppo, portando quindi l'innovazione ovunque e garantendo all'azienda la capacità di rinnovarsi ed adattarsi al contesto in cui opera. Il Gruppo, in applicazione del modello di Open Innovability®, lavora con un ecosistema di più di 500.000 persone, composto da startup – con cui siamo connessi tramite i nostri **10 Innovation Hub** e **22 Lab** – partner industriali, piccole e medie imprese ("PMI"), centri di ricerca, università e imprenditori, anche attraverso l'utilizzo di piattaforme di *crowdsourcing*, come openinnovability.com. La piattaforma è dedicata al mondo degli innovatori e alle persone in Azienda che desiderano contribuire allo sviluppo del business con soluzioni innovative e sostenibili, trasformando le proposte in progetti concreti in grado di risolvere sfide ispirate a specifiche esigenze aziendali. Le soluzioni presentate riguardano l'intera catena del valore: dalla generazione alla distribuzione dell'energia, fino ai mercati. La piattaforma, inoltre, offre anche uno spazio a chiunque abbia progetti innovativi legati al business, anche se le proposte non rispondono ad alcuna specifica challenge attiva.

In generale, grazie all'approccio Open Innovability® più di 25.000 proposte sono state valutate, sono state attivate 700+ collaborazioni (di cui 545 con startup) e, tramite 1200 progetti attivati. Sono state scalate 300+ innovazioni.

La costante applicazione della strategia sicurezza informatica, oltre all'attuazione dei processi appena descritti, ha anche previsto l'adozione di specifiche misure di protezione, consapevoli del fatto che il rischio Cyber non è solo un problema della singola azienda, ma è un rischio di portata ecosistemica e come tale va affrontato favorendo una costante cooperazione tra tutti gli *stakeholder* interessati: enti istituzionali, accademie e, non ultimo, l'intera *supply chain*.

CYBERSICUREZZA: IL CASO ITALGAS

di Alessandro Menna
Chief Security Officer, Italgas

Seppure il panorama dei rischi che insistono sulle infrastrutture energetiche del Paese sia in continua evoluzione, la minaccia rappresentata dagli incidenti Cyber ha assunto una rilevanza sempre maggiore nel corso degli ultimi anni, arrivando a scalare rapidamente le classifiche dei principali rischi per le organizzazioni del settore, sia quelle più grandi che quelle di dimensioni medie e piccole. Il rischio di attacchi cibernetici alle infrastrutture critiche di un Paese ha assunto ormai un ruolo tanto rilevante da entrare frequentemente nelle discussioni dei Consigli di Amministrazione, nei Comitati di Controllo ed in tutti i processi di business, di innovazione tecnologica e di trasformazione in cui siano coinvolte tecnologie informatiche.

È sempre più condiviso (finalmente) l'approccio "security by design" in cui l'innovazione tecnologica e la trasformazione digitale dell'organizzazione trovano nella sicurezza informatica e delle informazioni un pilastro fondamentale ed un fattore di vantaggio competitivo, diversamente dal passato, quando gli investimenti in sicurezza erano spesso considerati come "perdite operative" necessarie e, come tali, dovevano essere contenute entro limiti percentuali della spesa IT.

In questi ultimi anni **le infrastrutture energetiche**, ed in particolare quella della distribuzione del gas, hanno affrontato un rapido processo di digitalizzazione il cui scopo è stato quello di **evolvere verso reti intelligenti**. Nel settore del gas, la disponibilità di intelligenza distribuita su tutta la rete, dallo Smart Meter presso il consumatore finale, fino ai City Gate di collegamento alla rete di trasporto nazionale, passando per le centinaia di impianti intermedi di regolazione e monitoraggio del gas, ha consentito di raggiungere la flessibilità necessaria a poter gestire flussi bidirezionali nella rete; ha consentito di ottenere una visibilità totale, ed aggiornata in tempo reale, sullo stato dell'infrastruttura, aumentando i livelli di sicurezza, la capacità di individuazione tempestiva di anomalie e di intervento rapido ed efficace di manutenzione, anche adottando tecniche preventive, mediante l'impiego di algoritmi di intelligenza artificiale.

Le caratteristiche delle reti digitali abilitano la possibilità di gestire diverse tipologie di gas: oltre al tradizionale metano, possono oggi essere gestite miscele di gas con contenuto di idrogeno variabile e gas sintetici, oltre al biometano, facendo della rete di distribuzione di Italgas un asset fondamentale a supporto della transizione energetica nazionale.
Se da un lato, quindi, la digitalizzazione delle infrastrutture energetiche è un fattore fondamentale a supporto sia della competitività delle organizzazioni del settore sia della strategia di transizione energetica del Paese, dall'altro deve essere accompagnato da una crescita delle capacità di protezione informatica altrettanto solida.
Alcune organizzazioni attive nel settore delle energie sono oggi annoverabili tra i cosiddetti "Digital Master", disponendo di infrastrutture digitali avanzate, di processi di gestione delle operations totalmente ridisegnati sulla base della disponibilità delle tecnologie IT, di elevati livelli di flessibilità organizzativa e velocità di innovazione grazie, in particolare, all'utilizzo del Cloud.
In questo contesto, **la minaccia di incidenti Cyber è in grado di impattare trasversalmente rispetto a rischi tradizionali** quali l'interruzione della continuità operativa (inclusa quella della supply chain), la capacità di gestire efficacemente eventi esterni di sicurezza sul territorio (tra cui gli eventi naturali), la perdita di reputazione dell'organizzazione e dei propri fornitori.
È per questo motivo che Italgas sta facendo evolvere il proprio sistema di sicurezza **da un approccio di tipo reattivo ad un modello di protezione attiva**, in grado di coinvolgere e correlare tutti gli eventi aziendali provenienti da differenti domini ed ambiti con l'obiettivo di prevenire, riconoscere e mitigare potenziali incidenti di sicurezza partendo da semplici segnali ed evidenze.
La resilienza quale valore cardine e guida dell'organizzazione non riguarda soltanto la prevenzione dei rischi ed il corretto ripristino dell'operatività ma rappresenta la capacità di anticipare, di rispondere e adattarsi ai cambiamenti improvvisi ed alle situazioni di crisi, tra cui quelle cibernetiche.
Il Gruppo ha quindi avviato un percorso di innovazione del proprio modello di sicurezza, sviluppando un approccio che permetta di gestire in maniera del tutto integrata differenti livelli di informazione, ed in particolare:

- il livello dei dati digitali e delle infrastrutture informatiche (il cosiddetto Dominio logico), relativo a tutti i presidi tecnico-organizzativi che tramite gli strumenti ed i servizi di Cybersecurity sono volti a salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni, con riferimento a sistemi, applicazioni, piattaforme, reti informatiche, dati e processi necessari alla loro gestione;
- il livello degli asset materiali e del personale (il cosiddetto Dominio fisico), ovvero l'insieme di misure, controlli e soluzioni il cui scopo, tramite le attività di gestione integrata degli allarmi provenienti dai vari sistemi presenti sul territorio, è garantire l'adeguata protezione delle persone e delle infrastrutture (sedi e siti operativi) del Gruppo;
- il livello delle informazioni (il cosiddetto Dominio informativo), relativo a tutti i presidi che, tramite servizi di Early Warning, attività di Intelligence ed analisi socio-ambientali, mirano a raccogliere, gestire e distribuire informazioni ed istruzioni per la tutela del patrimonio, della reputazione dell'organizzazione e per la sicurezza del personale.

L'obiettivo è **convergere verso il Sistema Integrato di Sicurezza** in grado di interfacciare piattaforme di gestione della sicurezza multi-dominio, applicazioni, servizi e processi operativi con la finalità di gestire in modalità integrata vulnerabilità, minacce ed eventi di sicurezza e garantire una visione quantitativa e dinamica del rischio per indirizzare e facilitare i processi decisionali.
Esempio concreto di questa visione della sicurezza è il nuovo centro Italgas denominato ISC^3 (Integrated Security Cloud Command Center) ospitato all'interno della sede di Torino, Headquarter di Italgas Reti.

CONCLUSIONI

Il mercato del digitale si conferma anche quest'anno un segmento dell'economia molto dinamico: l'ICT "trascina" infatti la crescita dell'economia almeno dal 2015. Oltre all'impatto che l'adozione delle tecnologie ICT ha sull'organizzazione delle imprese, queste tecnologie stanno attivando nuovi modelli di business, nuovi concorrenti e nuovi mercati, e trasformando modalità di produzione e processi, con la diffusione di fenomeni come la robotizzazione, l'automazione e l'intelligenza artificiale.
Il 2022 può rappresentare l'inizio di un nuovo ciclo positivo per il mercato digitale, che vede le tecnologie ICT al centro di cambiamenti dirompenti: diffusa è l'aspettativa che esse possano avere un doppio effetto positivo, non solo sull'economia ma anche sull'ambiente. La sfida dei prossimi mesi, anche per il nuovo Governo, sarà governare accelerazione tecnologica, sostenibilità e aggiornamento delle competenze al fine di gestire e ottimizzare le opportunità offerte dal PNRR.

DIGITALE, ECONOMIA, AMBIENTE E RISCHI CIBERNETICI GLOBALI

Cinque condizioni di contesto per determinare meccanismi di interazione "virtuosi"

CONCLUSIONI

L'ICT "trascina" la crescita dell'economia almeno dal 2015

Il mercato del digitale si conferma anche quest'anno un segmento dell'economia molto dinamico, con performance superiori all'intera economia in diversi ambiti, dal valore aggiunto, agli addetti, alla crescita del numero di imprese attive e indicatori come intensità di R&S o produttività. Questa evoluzione è più positiva di quella dell'intera economia ormai da qualche anno.

Dal confronto della serie storica della crescita annua del mercato ICT e del PIL a prezzi di mercato o correnti e a prezzi costanti (Fig. 1) è evidente che l'ICT "trascina" la crescita dell'economia almeno dal 2015, quando muovevano i primi passi il Mercato Unico Europeo del Digitale e il Piano Industria 4.0 (poi trasformato in Impresa 4.0 e quindi Transizione 4.0), mentre sul mercato si affacciavano le principali tecnologie abilitanti del digitale, dal Cloud ai Big Data, all'IoT e alle soluzioni avanzate di Cybersicurezza.

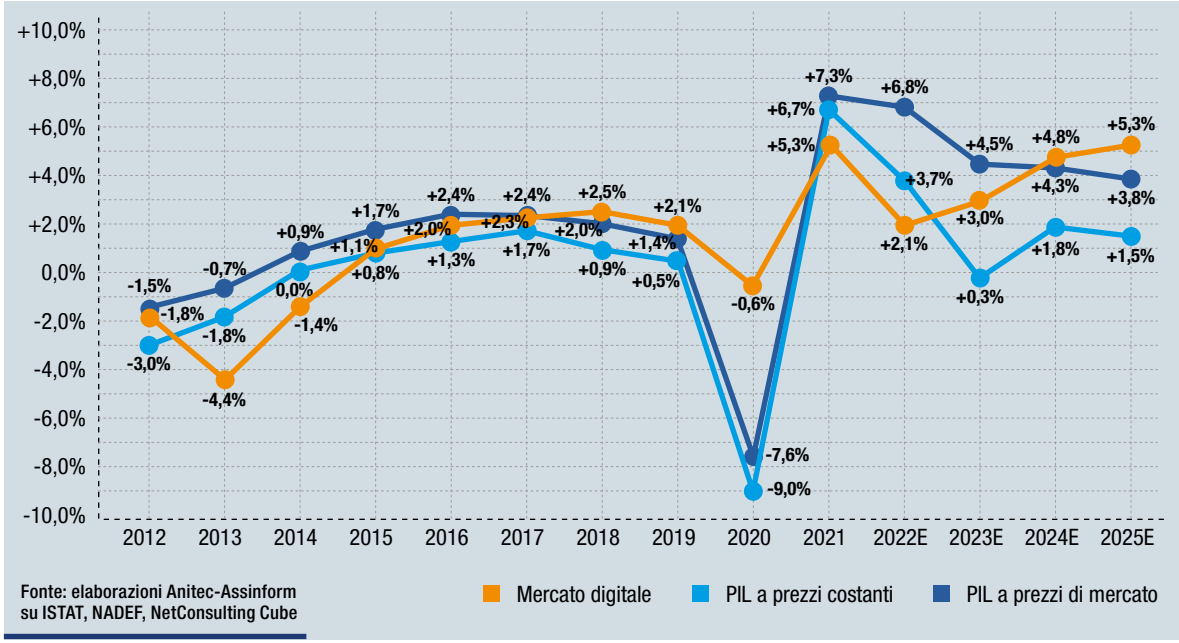
Questa dinamica si è mantenuta più positiva per l'ICT anche durante gli anni della pandemia di Covid-19, con un settore del digitale nettamente meno colpito rispetto a manifatturiero e servizi in generale. Questo si è tradotto in una dinamica pressoché piatta (-0,6%) per il nostro settore nel 2020 contro una caduta del -7,6% del PIL.

Dal punto di vista competitivo, accelerata dalle sfide aperte dalla pandemia, si afferma ormai in maniera diffusa in tutti i settori la consapevolezza che i **Digital Enabler e le tecnologie ICT determinano il potere competitivo nell'economia della conoscenza.** Diventa evidente l'impatto dell'adozione diffusa del digitale sull'organizzazione di imprese, ospedali ed enti pubblici, che, per affrontare il Covid facendo leva sul digitale, hanno realizzato in pochi mesi cambiamenti organizzativi e operativi radicali, che in passato richiedevano anni.

Oltre all'impatto che l'adozione delle tecnologie ICT

Figura 1:

Crescita annua mercato digitale e PIL, 2012-2025E



Fonte: elaborazioni Anitec-Assinform su ISTAT, NADEF, NetConsulting Cube

ha sull'organizzazione delle imprese, diventa fondamentale il **ruolo abilitante di queste tecnologie nel creare nuovi modelli di business, nuovi concorrenti e nuovi mercati, come pure nel trasformare produzione e processi**, con la diffusione di nuovi fenomeni come la robotizzazione, l'automazione e l'intelligenza artificiale, e aprono la strada alla frammentazione internazionale delle catene di approvvigionamento. La pandemia è un catalizzatore unico di queste tendenze, rivelando il potenziale delle tecnologie alla base del digitale per mitigare l'impatto delle restrizioni imposte.

Di conseguenza, mentre il 2020 vede un arresto della crescita per il mercato ICT a fronte di un crollo dell'economia, nel 2021 l'"effetto rimbalzo" per l'ICT è meno forte e la sua crescita si assesta a un livello inferiore a quella del PIL (a prezzi correnti per la prima volta dal 2017, a prezzi costanti per la prima volta dal 2015).

Mentre l'effetto rimbalzo su ICT e PIL si protrae, **nel 2022 uno scenario completamente nuovo si apre per il digitale**, in cui si vede convergere sia dal punto di vista competitivo che dal punto di vista normativo e politico una nuova visione strategica che mette la trasformazione digitale al centro dell'evoluzione economica del futuro prossimo.

Vediamo pertanto **un ricorso importante che può costituire di nuovo l'inizio di un ciclo positivo per il nostro settore come è avvenuto nel 2015.**

L'inizio del ciclo positivo nel 2015 era associato a uno scenario in cui le tecnologie ICT, soprattutto attraverso i Digital Enabler, consentono la crescita economica sia direttamente, ampliando la portata di tecnologie come Internet e banda larga, facilitando l'interazione tra gli attori economici e innalzando la produttività, sia indirettamente abilitando nuove strategie, nuovi processi e modelli di business e anche nuove filiere.

Il 2022 può rappresentare l'inizio di un nuovo ciclo positivo per il mercato digitale, che vede le tecnologie ICT di nuovo al centro di **cambiamenti dirompenti di una portata ancora maggiore rispetto a quelli avviati nel 2015: l'impatto del digitale sulla crescita economica sarà sempre più interconnesso agli effetti sull'ambiente da un lato e ai rischi cibernetici di scala sempre maggiore dall'altro.**

Così come il digitale ha rimodellato il mondo negli ultimi decenni, diffusa è ora l'aspettativa che le nuove tecnologie ICT abbiano un doppio effetto positivo, non solo sull'economia ma anche sull'ambiente (come risultante netta tra l'impronta generata e il contributo alla riduzione dell'inquinamento).

Dal punto di vista normativo e politico a livello dell'UE e a livello nazionale, la risposta alle sfide del Covid-19, come il Recovery Plan for Europe e il **PNRR** in Italia, pone le tecnologie ICT al centro di una visione decennale ambiziosa per una trasformazione digitale di successo entro il 2030. Lo strumento della Next Generation EU mira a rendere l'economia più sostenibile, resiliente e meglio preparata per il futuro. Le tecnologie per la trasformazione digitale sono necessità fondamentali per raggiungere questo obiettivo.

Tradotto in previsioni per il mercato ICT nel contesto più generale delle previsioni economiche nazionali, questo scenario genererà **un nuovo ciclo che nella sua fase iniziale (almeno) avrà di dinamiche di crescita più positive per il mercato ICT rispetto all'intera economia. A differenza del ciclo 2015-2020, le dinamiche di mercato nel nuovo scenario che emergerà dal 2022 saranno tuttavia sempre più legate a fattori che influenzano la stessa interazione tra trasformazione digitale, economia, ambiente e nuovi rischi globali di natura cibernetica.**

Per questo la nostra visione è tutt'altro che deterministica, anzi. Nell'esplorare e valutare le **relazioni di interazione sempre più strette e complesse tra digitale, economia, ambiente e rischi cibernetici globali** abbiamo individuato almeno **cinque condizioni di contesto** senza le quali i meccanismi di interazione tra questi livelli da "virtuosi" potrebbero rapidamente invertirsi e diventare di segno opposto.

NON SI PUÒ PRESCINDERE DA LIVELLI DI PRODUTTIVITÀ SOSTENIBILI PER LA CRESCITA DELL'ECONOMIA

A sostegno di occupazione e crescita il disegno di legge di bilancio per il 2023 prevede un taglio limitato del cuneo fiscale per i lavoratori dipendenti a basso reddito e decontribuzione delle assunzioni di donne e giovani under 36, degli over 50 e dei percettori di reddito di cittadinanza. Si tratta di interventi dalla portata limitata che potranno anche mitigare parzialmente la recessione economica attesa per il 2023 ma sono sicuramente lontani dal rappresentare vere misure di incentivo per favorire la crescita dell'economia e dell'occupazione. Se si guarda a quanto prodotto dai tre anni di decontribuzione sperimentata dal "job acts", ad esempio, risulta che a beneficiarne è stata soprattutto l'occupazione delle classi di età mature, piuttosto che i giovani, cioè il lavoratore sperimentato con formazione "on the job", facendo emergere gli evidenti problemi di

occupabilità alla radice della elevata disoccupazione tra i giovani. Ma su questo torneremo nel punto successivo.

Resta invece totalmente non affrontato il problema vero della nostra economia: la produttività.

Questo è oltremodo preoccupante.

La velocità alla quale ogni economia può crescere nel tempo dipende in gran parte da due elementi: la crescita della popolazione e il ritmo di aumento della produttività. Se la produttività aumenta, significa che stiamo raggiungendo risultati migliori nella nostra attività. Le idee innovative e le nuove tecnologie sono al centro di questo processo. La popolazione non cresce tanto quanto in passato. La società deve quindi divenire più produttiva per consentire all'economia di crescere di più.

Qual è il ruolo delle tecnologie digitali nell'aumentare la produttività delle imprese?

La crescente importanza dell'impatto delle tecnologie digitali sul sistema economico italiano è evidente da molti anni come dimostra uno studio del MISE del 2010 sugli investimenti in ICT attraverso l'analisi dei moltiplicatori della produzione e della domanda calcolati sulle matrici Input Output rilasciate dall'Istat per gli anni 1995, 2000, 2005. I risultati di questo studio mostrano che l'ICT dà al sistema produttivo un impulso moltiplicativo molto più elevato rispetto al settore non ICT e si conferma, dunque, un settore chiave per perseguire obiettivi di crescita economica.[1] Questo impatto inoltre potrebbe anche sottostimare il contributo totale dell'economia digitale alla produzione e alla crescita economica poiché le tecnologie ICT sono un input che aumenta la produttività fornendo alle imprese maggiori economie di scala, resilienza organizzativa, flessibilità e accelerazione operativa, capacità di personalizzazione dell'offerta e di adattamento ai cambiamenti esterni.

Tuttavia ormai da decenni si osservano in Europa dinamiche aggregate della produttività del lavoro non positive e molto eterogenee da Paese a Paese. La produttività aggregata del lavoro in Europa – misurata come valore aggiunto reale per dipendente – è diminuita durante la crisi finanziaria globale (2007-09), quasi ha ristagnato durante la crisi del debito sovrano (2012-13) per poi riprendersi (2013-16). In Italia la variazione è stata negativa nei primi due periodi e si è solo ripresa dopo.[2]

Oltre ai tassi di adozione tecnologica, le riforme

istituzionali e strutturali a sostegno dell'innovazione e gli investimenti in capitale umano sono fattori con un grande impatto sugli sviluppi della produttività e le loro diverse dinamiche tra i Paesi. Inoltre, nei periodi di rapido cambiamento tecnologico come quello attuale è più diffusa la carenza di competenze associate alle nuove tecnologie e un loro crescente disallineamento.
La pandemia di Covid-19 e la relativa accelerazione nella digitalizzazione ha dato ulteriore impulso ai guadagni di produttività anche se con una portata ancora incerta essendo dipendente dallo sviluppo di istituzioni, infrastrutture, competenze, metodi di produzione e competenze strategiche.
Nel nuovo scenario che sta per aprirsi, se i rischi recessivi saranno opportunamente mitigati da vere politiche industriali e la crescita economica si materializzerà, nuovi e molteplici fattori influenzeranno il rapporto tra tecnologie digitali, economia e ambiente. Il collegamento tra i vari sistemi economici sarà sempre più complesso con filiere sempre più localizzate upstream e globalizzate downstream.
Per affrontare positivamente la recessione dei prossimi anni servirà una vera politica industriale focalizzata sulla produttività con obiettivi che rispecchino il contesto di questo nuovo scenario in cui digitale, economia e ambiente sono strettamente interconnessi.
Anche la contabilizzazione dell'impatto dell'innovazione digitale e ambientale andrà rivista perché se mantenuta su un singolo sistema (o una singola filiera economica) potrà portare a stime distorte. Per misurare l'impatto degli incentivi alla digitalizzazione servirà pertanto una **definizione multidimensionale della produttività** in cui poter considerare le diverse fasi produttive e le interazioni fondamentali tra "produttività dei fattori" (digitale, lavoro, capitale, etc.) e "produttività ambientale" (o anche più semplicemente "impronta ambientale").
La buona notizia è che abbiamo lo strumento, il PNRR; e le risorse finanziarie (almeno per i finanziamenti previsti fino al 2022). Il nostro auspicio è che quanto già avviato dal Ministero dell'innovazione per l'attuazione delle iniziative sul digitale previste nel PNRR continui a essere una priorità anche per il nuovo Governo ed eventualmente essere potenziato e ampliato attraverso una forte collaborazione tra chi, nell'Esecutivo, ne ha ereditato le deleghe.
In particolare vediamo l'urgenza maggiore su questi quattro assi:

- **competenze digitali specialistiche** per favorire aumenti della produttività per ora lavorata e dell'occupazione giovanile;
- **transizione 4.0** per favorire aumenti della produttività dei fattori di produzione attraverso incentivi per il continuo aggiornamento delle tecnologie digitali disponibili;
- rapida attuazione del nuovo **Codice dei contratti pubblici**, per accelerare l'attuazione dell'agenda digitale della Pubblica Amministrazione;
- **Cybersicurezza** per i rischi cibernetici a cui le infrastrutture strategiche nazionali pubbliche e private sono sempre più esposte.

PIÙ COMPETENZE DIGITALI SPECIALISTICHE RENDONO POSSIBILI AUMENTI DELLA PRODUTTIVITÀ PER ORA LAVORATA E DELL'OCCUPAZIONE GIOVANILE

Produttività del lavoro e occupabilità sono sempre più interconnesse nell'economia digitale.
Non è un caso se il divario di competitività con le altre economie a noi più vicine non è spiegato in termini di differenziali nel costo del lavoro (anzi penalizzanti per i lavoratori italiani) ma piuttosto di produttività del lavoro, ovvero il valore di ciò che si produce in un'ora di lavoro. **Il prodotto per ora lavorata è pari in Italia a 42,5 euro, contro il 52,1 euro in Germania e 57,5 in Francia.**[3] Tale divario origina dalla fine degli anni '90 quando la crescita potenziale della nostra economia è rallentata in termini di qualità innovativa, combinando bassi salari, bassa produttività, depauperamento del capitale umano, maggior interventismo burocratico. I settori tradizionali del manifatturiero e dei servizi hanno investito poco in innovazione e i settori più innovativi – a parte qualche eccezione come aerospazio e biotech – pur presenti, non sono decollati rapidamente come negli altri Paesi. Ne è risultato che il divario di produttività per ora lavorata con Germania e Francia è peggiorato e il gap è ora solo in minima parte sanabile con gli sgravi sul costo del lavoro previsti nella legge di bilancio in fase di approvazione.
Dei segnali incoraggianti arrivano dalle nostre analisi condotte in collaborazione con InfoCamere, sulle Startup e PMI innovative iscritte alla sezione speciale del Registro delle Imprese. Startup e PMI innovative "digitali", ovvero che utilizzano le tecnologie digitali in modo intensivo per migliorare i processi ma anche per creare nuovi prodotti e servizi digita-

li, nel 2021 hanno registrato un valore aggiunto per addetto pari a 41.200 euro, contro 36.800 euro del resto delle Startup e PMI innovative registrate.

Occorre pertanto **promuovere le produzioni e le filiere tecnologicamente più avanzate nei processi o anche "digital native" dove maggiore è il valore prodotto per ora lavorata. Il paradosso centrale è che anche a volerlo non abbiamo abbastanza esperti di digitalizzazione per fare crescere e diffondere l'innovazione.**

Insieme alla produttività per ora lavorata, l'altro fattore chiave da sostenere per la crescita economica è dunque **l'occupabilità**, soprattutto quella giovanile e femminile.

Il problema è proprio nell'offerta di giovani candidati pronti a entrare sul mercato del lavoro. Sottolineiamo: "pronti", "operativi". Questa offerta è inferiore alla domanda. I candidati disponibili non hanno le competenze necessarie per svolgere i "nuovi" lavori che emergono nell'economia digitale.

Il problema è di livello (troppo pochi laureati) e di indirizzi di formazione (troppo pochi diplomati e laureati STEM) nonché di aggiornamento in linea con la rapida evoluzione delle tecnologie digitali.

Nel nostro ambito associativo vediamo soprattutto il caso delle competenze specialistiche dell'ICT: abbiamo contato 89mila posizioni di lavoro offerte sul web nel 2021 di cui 57mila anche per candidati non laureati o con formazione informale.[4] Di queste web vacancy circa 32mila sono sul job di "Developer"'.

Secondo uno scenario conservativo, l'Osservatorio per il 2019 ha stimato un fabbisogno di 14.400 laureati e 8.800 diplomati contro un'offerta di 9.300 laureati e 17.200 diplomati. Il gap risultante è quindi di una **carenza di 5.100 unità per i laureati** pari al 35% del fabbisogno e un **surplus di circa 8.400 unità**, ovvero il 95% in più di quanto necessario, **per i diplomati** che però richiedono percorsi formativi ulteriori per diventare "operativi". Secondo uno scenario espansivo, il gap potrebbe arrivare a una carenza di 17.200 unità per i laureati e un avanzo di 900 unità per i diplomati.

Se fare formazione al lavoro in modo rigoroso e continuo e trasversale è indispensabile e genera contestualmente benessere per la società e produttività per l'economia, **fare formazione al lavoro in ambito ICT è cruciale dal punto di vista strategico per il Paese e per le imprese.** Eppure, mai l'Italia si è dotata di un sistema di formazione diffusa al lavoro in generale né tantomeno per le competenze digitali avanzate. Costruirlo significa che, insieme alle risorse economiche da dedicare in modo non episodico, deve essere identificata una **strategia di lungo periodo che integri i processi di riqualificazione con quelli di orientamento e accompagnamento al lavoro, che coordini i percorsi di istruzione tecnica e i percorsi di formazione permanente e che mantenga allineate e complementari le politiche formative pubbliche con quelle aziendali.** Questa strategia deve essere corredata da piani di implementazione specifici (per territori, per caratteristiche delle persone e delle imprese coinvolte, etc.) che identifichino le responsabilità degli attori pubblici e di quelli privati (a partire dalle imprese dotate di sistemi di formazione professionalizzanti) e che specifichino fasi e strumenti standardizzati, indispensabili per il monitoraggio dei risultati formativi e per la loro portabilità nelle transizioni lavorative delle persone.

È comunque possibile un **sistema di formazione diffusa per le competenze avanzate ICT** così delineato in Italia? Sicuramente **è possibile, ma serve monitorare e affrontare le criticità con consapevolezza e pragmaticità.** Le criticità più importanti sono a livello di:

- *scuole di impresa:* ridotta dimensione e connessa limitata diffusione di sistemi di formazione professionalizzanti, ridotta diffusione di programmi di formazione aziendali in condivisione nelle filiere;
- *enti di formazione:* mercato frammentato e opaco, miriade di piccolissimi soggetti accreditati negli albi regionali, con scala di azione irrisoria in termini di ore formative erogate, senza il patrimonio di competenze metodologiche necessarie alla costruzione di corsi lunghi di formazione per e al lavoro;
- *sistema fondazioni ITS:* numeri esigui di studenti, percorsi lunghi (annuali e biennali) e solo per un target giovane, presenza selettiva delle imprese grandi e centrali nelle fondazioni.

Nel Dipartimento per la Trasformazione Digitale è stato avviato il progetto "Scuola diffusa", che intende creare un'iniziativa di formazione su ampia scala per "mettere a sistema" le iniziative di formazione delle aziende ICT fornendo un punto di accesso unico ai percorsi di sviluppo delle competenze specialistiche ICT più richieste dal mercato. Anitec-Assinform contribuisce attivamente al progetto.

Nel 2022 Anitec-Assinform ha contribuito attivamente a "Scuola diffusa" con due iniziative:

- **il positioning paper "La formazione delle competenze avanzate ICT: Linee guida per una Scuola diffusa"**[5] che, sulla base di una estesa analisi della letteratura e di approfonditi studi empirici dell'ambito ICT in Italia, propone delle linee

guida di progettazione e di implementazione di un sistema di formazione diffusa per le professioni ICT, nonché misure di policy a supporto della sua fattibilità;

- **il portale "Formati con noi"**[6] come strumento di conoscenza per chiunque voglia diventare un professionista del settore ICT, attraverso una panoramica aggiornata dei programmi di formazione per competenze specialistiche ICT erogati dalle imprese associate insieme alle opportunità di lavoro da loro messe a disposizione e la profilazione delle professioni ICT più ricercate dal mercato, con relative abilità e requisiti formativi richiesti.

Ma il nostro impegno non si ferma qui e resterà tra le nostre priorità nell'attesa di vedere un riequilibrio tra domanda e offerta di professionisti ICT.

Per quanto riguarda le iniziative di **finanziamento della formazione** auspichiamo modifiche nel corso dell'esame in Parlamento della legge di bilancio 2023 affinché sia rinnovato il **credito di imposta nella formazione 4.0** al momento non previsto malgrado il recente aumento nell'utilizzo dello strumento. Marginale anche l'impegno sulla formazione professionale, con il rifinanziamento del Fondo sociale per occupazione e formazione, incrementato di 100 milioni di euro annui a partire dal prossimo anno e l'istituzione del "Fondo per accrescere il livello professionale nel turismo" per 21 milioni di euro nel periodo 2023-2025.

Con riguardo alla formazione continua auspichiamo anche che il rifinanziamento del **Fondo Nuove Competenze** nell'ambito del PNRR permetterà ai datori di lavoro di effettuare attività di formazione per il personale focalizzate sulle competenze ICT a maggiore domanda soprattutto per le professioni emergenti in ambito front-end e back-end development, data science, IoT/IA secondo i requisiti definiti nell'ambito dell'**e-Competence Framework 4.0 recepito in Italia nel 2021** attraverso la normazione UNI.

UN AGGIORNAMENTO SOSTANZIALE DI QUANTITÀ E PERIMETRO DI FINANZIAMENTO DEGLI STRUMENTI PER L'INNOVAZIONE DELLE IMPRESE POTRÀ RIPORTARE IN ITALIA PEZZI IMPORTANTI DELLE CATENE DEL VALORE GLOBALE

Insieme alla produttività del lavoro vogliamo considerare cruciale anche la **produttività degli investimenti tecnologici.** Su questo l'industria manifatturiera ha sfide importanti davanti a sé. Le potenzialità dell'innovazione tecnologica sono emerse in tutta la loro rilevanza negli ultimi due anni e sono molteplici le questioni che devono essere affrontate con urgenza per progettare tanto il futuro delle fabbriche quanto la digitalizzazione dell'intera relazione con i clienti. In più le tecnologie non solo rendono più efficienti i processi e chi li esegue, ma arrivano a gestire più autonomamente sequenze di processo sempre più complesse fino all'interazione m-to-m e all'abilitazione di nuove attività sia a monte che a valle della catena di produzione.

I rapidi cambiamenti apportati ai modelli di business dalla pandemia hanno reso le imprese sempre più sensibili alla necessità di adottare piattaforme Cloud e tecnologie collaborative, migliorare la qualità dei dati, ottimizzare il portafoglio prodotti/componenti. Di questi sviluppi stanno beneficiando in particolare la gestione del processo di sviluppo prodotto e della catena di fornitura, alla ricerca di livelli sempre maggiori di resilienza in un contesto di progressiva rilocalizzazione di alcune fasi produttive. Questo vuol dire che **le imprese italiane non possono non innovare se vogliono restare competitive nelle supply chain globali.**

Ma stanno anche emergendo due grandi nemici del rinnovamento tecnologico: **l'incertezza** associata al clima attuale e al conflitto in Ucraina, l'impatto dei **costi della burocrazia** che può generare perdite di produttività che vanificano i vantaggi dei finanziamenti.

Contro questi nemici, continueremo a supportare i tre progetti previsti nella componente C2 "Digitalizzazione, innovazione e competitività del sistema produttivo" del PNRR:

- **transizione 4.0** (13.381 milioni di euro) per promuovere la trasformazione digitale dei processi produttivi e sostenere gli investimenti in beni strumentali materiali tecnologicamente avanzati e in beni immateriali nella fase di ripresa post-pandemica;
- competitività e resilienza delle **filiere produttive** (750 milioni di euro);
- investimento nel sistema di **proprietà industriale** (30 milioni di euro di cui 16 per brevetti, 7,5 per progetti di proof of concept e 8,5 per potenziamento degli Uffici di trasferimento tecnologico.

In ambito **filiere produttive** auspichiamo il massimo impatto dei 500 milioni di euro (a valere sul Fondo nazionale complementare al PNRR) appena destinati a finanziare progetti di ricerca e sviluppo nell'ambito del secondo sportello dedicato agli **Accordi per l'innovazione**, con agevolazioni per le imprese di qualsiasi dimensione, in ambito industriale, agroindustriale, artigiano o di servizi all'industria nonché attive nella ricerca.

Per il **Piano Transizione 4.0**, che entra nel suo sesto anno di vita, apprezziamo l'orizzonte di medio termine che dà stabilità alla misura, ma confermiamo l'auspicio che le aliquote non saranno più che dimezzate[7] e non finirà il credito d'imposta per l'ac-

quisto di beni strumentali ordinari sia materiali che software, come previsto nel piano dal 2023. Temiamo forti riduzioni negli investimenti per questi minori crediti di imposta che aggraveranno le perdite in innovazione delle PMI che già mettiamo in conto per la "chiusura" per mancato rifinanziamento della Nuova Sabatini.

Sul piano attuativo auspichiamo che il Governo proceda al più presto con l'apertura di un tavolo di confronto con imprese ed esperti. È evidente che le merceologie elencate nei due allegati non sono più aggiornate, mentre gli stessi beni oggetto di investimento nel 2016-17 sono ormai soggetti a sostituzione e nuove tecnologie arrivate sul mercato in tempi più recenti mancano all'appello.

Stride infine **la limitatezza e la lentezza delle procedure di accesso alle risorse dedicate a Intelligenza artificiale, IoT e Blockchain** rispetto al loro rapido sviluppo e alla loro portata innovativa. Il "Fondo per lo sviluppo di tecnologie e applicazioni di Intelligenza Artificiale, Blockchain e Internet Of Things" è stato istituito dalla legge di bilancio 2019, che ha stabilito una dotazione complessiva pari a 45 milioni di euro (25 milioni per IA, e 10 ciascuno su Blockchain e IoT). Il decreto interministeriale 6 dicembre 2021 ha definito come saranno utilizzate le risorse mentre il decreto direttoriale 24 giugno 2022 quando e come presentare le domande di agevolazione e come verranno erogati gli incentivi. Sono finanziabili progetti di ricerca e sviluppo, nonché di innovazione dell'organizzazione e di processo, "anche mediante il paradigma del metaverso", per un minimo di 500mila euro e un massimo di due milioni di euro ciascuno. Il 60% delle risorse è riservato a proposte da PMI e reti di imprese, il 34% ai territori del Mezzogiorno. **Poche risorse su tre ambiti tecnologici strategici, distribuite a pioggia, rischiano di non generare l'impatto voluto.**

È NECESSARIO FAR EVOLVERE LA MODALITÀ DI ESECUZIONE DEI BANDI DEL PNRR VALORIZZANDO LA CONCERTAZIONE TRA GLI ATTORI DELLA DOMANDA E I PARTNER TECNOLOGICI FINALIZZATA AL RISULTATO

La revisione del Codice dei contratti pubblici, per aggiornarlo e armonizzarlo rispetto alla normativa europea, è uno degli obiettivi più impegnativi fissati dal PNRR sul fronte delle riforme. L'adozione di una nuova legge sugli appalti dovrà consentire l'efficace messa a terra degli investimenti, con tempi e modi che permettano di non vanificare i processi evolutivi e di sviluppo che la spesa pubblica ha il compito di guidare, soprattutto per quanto attiene alla trasformazione digitale, transizione ecologica e superamento delle disparità geografiche, di genere e generazionali.

Lo schema di decreto legislativo contenente la bozza di revisione è stato consegnato al Governo dall'apposita commissione creata nel Consiglio di Stato lo scorso ottobre. Inizia così il conto alla rovescia per l'esecutivo in vista del 31 marzo (entrata in vigore del decreto legislativo attuativo della delega per la revisione), del giugno 2023 (entrata in vigore di tutte le leggi, regolamenti e provvedimenti attuativi) e del dicembre 2023 (pieno funzionamento del sistema nazionale di e-procurement). In questi prossimi step non è escluso che il testo possa subire ulteriori modifiche.

Accogliamo con soddisfazione il nuovo testo che si presenta come il **primo Testo Unico della materia e come il primo Codice "autoapplicativo"** e ci auguriamo che questo possa permetterne una rapida implementazione. Non solo. Innovativi e impattanti sono i nuovi principi generali fissati nei primi articoli, che costituiscono espressamente i criteri interpretativi di tutto il nuovo Codice. In particolare il **"Principio del risultato"** per il quale «le stazioni appaltanti e gli enti concedenti perseguono il risultato dell'affidamento del contratto e della sua esecuzione con la massima tempestività e il migliore rapporto possibile tra qualità e prezzo, nel rispetto dei principi di legalità, trasparenza e concorrenza. La concorrenza tra gli operatori economici è funzionale a conseguire il miglior risultato possibile nell'affidare ed eseguire i contratti».

Molto importanti e funzionali al ruolo strategico del nostro settore sono anche:

- il rafforzamento e la promozione delle procedure di **partenariato pubblico-privato e di project financing** per l'attrazione di investitori istituzionali ed esteri nella realizzazione di opere pubbliche;
- il rafforzamento delle prescrizioni e della **promozione dell'utilizzo delle tecnologie verdi e digitali al fine di garantire la centralità di questi processi** nell'ambito dei contratti e degli interventi afferenti alla Pubblica Amministrazione;
- la **semplificazione delle procedure destinate alla realizzazione di investimenti in tecnologie verdi e digitali**, nonché in innovazione e ricerca; ciò anche al fine di conseguire gli obiettivi dell'Agenda 2030 per lo sviluppo sostenibile, in tal modo incrementando il grado di ecosostenibilità degli investimenti pubblici e delle attività economiche secondo i criteri del regolamento (UE)

2020/852 del giugno 2020.

In questo nuovo contesto crediamo che sia ormai **imprescindibile una collaborazione sempre più stretta tra gli attori della domanda pubblica e i partner tecnologici in tutte le fasi del contratto pubblico**, dalla progettazione del bando alla selezione ed esecuzione del progetto, come già avviene in altri Paesi UE, come la Francia. Il criterio di aggiornamento della valutazione economica di progetto è un progresso importante, ma non va separato dall'intero contesto delle nuove progettualità in ambito digitale e ambientale, in base alle quali non è più possibile per l'ente pubblico lavorare "in autonomia" o secondo modalità "bidirezionali domanda-offerta", se si vogliono raggiungere i risultati attesi. Questo perché i progetti dei prossimi anni si caratterizzeranno in misura sempre più rilevante per una innovazione molto rapida, requisiti di competenza digitale avanzata a diversi livelli, controllo e soprattutto prevenzione del rischio cibernetico, business plan progettuali sempre più complessi, interazione di variabili di natura diversa e non più solo economiche, ma anche ambientali e sociali.

UNA CHIARA CONSAPEVOLEZZA DEI RISCHI CYBER GLOBALI E DEL RUOLO EMERGENTE DELL'INTELLIGENZA ARTIFICIALE GUIDERÀ LE SCELTE IN AMBITO CYBERSICUREZZA

L'evoluzione dell' iniziativa pubblica sulla sicurezza cibernetica sta avvenendo su due livelli:

- **la protezione delle infrastrutture critiche unitamente al controllo delle rotte e del trasporto dei dati.** In questo ambito è stata fondamentale l'estensione del perimetro di sicurezza nazionale cibernetica ai soggetti, pubblici e privati che (attraverso reti, sistemi informativi e servizi informatici) esercitano 223 funzioni essenziali dello Stato, ed erogano servizi essenziali per il mantenimento di attività civili, sociali o economiche strategiche;
- **lo sviluppo dell'Intelligenza artificiale**, seconda chiave della competizione globale del futuro. Insieme a Big Data, tecnologie quantistiche, tecnologie spaziali ed ipersoniche, e tecnologie del potenziamento umano, l'IA è considerata una delle principali Emerging Distruptive Technolgies, (EDT), destabilizzanti per lo scenario di sicurezza della NATO. Su questi fronti il mantenimento della superiorità tecnologica dell'Occidente è visto di cruciale importanza.

Dei 623 milioni di euro previsti dal PNRR per la Cybersicurezza,[8] **170 sono già stati assegnati per progetti previsti nel 2021 e 190,4 per progetti nel 2022.** Lo stato di attuazione della roadmap vede la finalizzazione dell'architettura dell'ecosistema, la messa in esecuzione dei primi servizi e l'approvazione finale del Piano Nazionale che renderanno così pienamente operativa l'Agenzia Nazionale per la Cybersecurity entro fine anno, unitamente all'avviamento entro dicembre della rete dei laboratori di screening e certificazione e il reclutamento delle competenze necessarie.

Fondamentale nei prossimi mesi sarà lo **sviluppo di partnership pubblico-private.** Il nostro settore è pronto per una **collaborazione sempre più forte con la nuova Agenzia** per avviare rapidamente gli appositi strumenti di cooperazione (fondazioni o società) che vedrà il nostro settore tra i maggiori contributori alla costruzione dello scudo cyber del Paese, attraverso la progettualità internazionale, la formazione delle competenze e lo sviluppo delle tecnologie. Vogliamo richiamare l'importanza di una vera e propria "istituzionalizzazione" di questo dialogo tra la struttura ed il comparto industriale, in modo che gli operatori in possesso delle dovute certificazioni possano essere coinvolti "in automatico", come avviene per i gruppi di lavoro internazionali. Nel mondo delle Startup e PMI innovative cresce la presenza e il valore delle nuove imprese attive in ambito Cybersicurezza. Per questo potrebbe anche essere utile **dedicare alle aziende della Cybersicurezza uno status di Zona Economica Speciale**, consentita e prevista dalla UE, per spingerle con vantaggi fiscali ad insediarsi in distretti o parchi tecnologici.

Per concludere…

Abbiamo visto che molti cambiamenti di direzione e di marcia per il digitale si affacciano sul nuovo scenario economico e competitivo dei prossimi anni e molte tendenze del passato non saranno più così scontate.

Tra i principali capovolgimenti vediamo che:

- ricadute positive o negative di digitale, ambiente e Cybersicurezza sono gestibili solo se gestite a livello dei meccanismi di interazione tra loro e per affrontarle serve un grande lavoro di collaborazione tra policy maker, industria e ricerca;
- i potenziali impatti a breve di regolamenti ambientali stringenti, che potrebbero reindirizzare gli investimenti delle imprese dal digitale alla tecnologia verde, possono generare risvolti positivi in una visione più sistemica che vede più benefici che concorrenza di interessi dall'interazione tra tecnologie digitali e tecnologie verdi;

- la crescita della produttività del lavoro è un fattore chiave per la vita di un Paese e la sua crescita economica, in particolare in una situazione in cui recessione e incertezza non permettono di aumentare le ore lavorate per dipendente e l'azzeramento della crescita demografica limita anche la crescita della forza lavoro;
- serve più digitalizzazione per raggiungere livelli maggiori di produttività per ora lavorata e quindi per addetto;
- la tecnologia da sola non basta: l'innovazione tecnologica deve innestarsi all'interno di un progetto di innovazione organizzativa e di revisione dei processi. Il motore di questa transizione sono le persone che devono esprimere competenze sempre più qualificate. Ma non abbiamo sufficiente forza lavoro con queste competenze, né per portare avanti più rapidamente questi progetti né per ottimizzare l'utilizzo delle nuove tecnologie digitali;
- più accelera l'innovazione tecnologica più non vale la relazione biunivoca, "minor costo del lavoro più occupazione". Il problema non è di domanda da parte delle aziende o di costo del lavoro, ma di carenza di offerta, ovvero di competenze specialistiche ICT aggiornate o del tutto nuove e di percorsi formativi "sistematizzati";
- questo ritardo nella digitalizzazione è effetto ma anche causa – in parte – di un livello di disoccupazione giovanile e femminile nel Paese tra i più elevati in Europa. Le opportunità occupazionali, soprattutto dei giovani, sono molto legate alla diffusione dei processi innovativi e di digitalizzazione. Il ricorso alla componente giovanile è infatti per sua natura più frequente per i progetti di innovazione digitale e tecnologica, in quanto richiedono competenze e qualità personali di apprendimento e di flessibilità più facilmente possedute dalle nuove generazioni;
- la caratteristica di questi ultimi anni è la velocità: tanto la creazione di tecnologia digitale che l'adozione di essa ha visto una forte accelerazione. Non si vede altrettanto nei guadagni di produttività derivanti da questo sviluppo, sia in Italia che in Europa. Questo perché la tecnologia si diffonde a velocità diverse per settore e nello stesso settore per tipologia di impresa con propensioni diverse all'innovazione o competenze diverse a disposizione. Anche le incertezze legate all'attuale conflitto rallentano la crescita della produttività, con l'aumento del costo degli investimenti e la diminuzione dei benefici percepiti o attesi;
- man mano che la confidenzialità, la disponibilità e l'integrità dei dati divengono più rilevanti per la ricchezza del Paese e la sicurezza nazionale, più urgente diventa rafforzare la sicurezza cibernetica. La tutela e la promozione del vantaggio tecnologico, nel quadro di un nuovo equilibrio geopolitico, diventa altrettanto, se non più importante, della potenza militare ed economica.

Mai come in questo momento di grande preoccupazione sui segnali recessivi dell'economia e di grande incertezza per il perdurare del conflitto in Ucraina, **i governi possono influenzare** con la loro visione e le loro decisioni **il futuro competitivo e la crescita delle economie nazionali.** Per favorire aumenti di produttività e crescita economica **serve che mantengano sostenuti gli investimenti in tecnologie digitali e rendano il lavoro più efficiente** grazie alla formazione di competenze ICT e digitali avanzate. E serve che continuino a promuovere la formazione di nuove competenze, la **ricerca e sviluppo**, e l'avvio di **attività imprenditoriali innovative** e ad elevata intensità tecnologica.

La sfida dei prossimi mesi sarà governare accelerazione tecnologica, sostenibilità e aggiornamento delle competenze al fine di gestire e ottimizzare le opportunità offerte dal PNRR. Su questa visione e queste decisioni si decide il futuro della nostra economia.

Note:

1. Claudio Di Carlo ed Elisabetta Santarelli, *Contributo dell'ICT alla crescita economica in Italia: un'analisi Input Output*, Dipartimento delle Comunicazioni, MISE 2010.
2. *Key factors behind productivity trends in EU countries*, European Central Bank Occasional Paper, December 2021, www.ecb.europa.eu/pub/pdf/scpops/ecb.op268~73e6860c62.it.pdf.
3. Fonte: Eurostat.
4. Fonte: Osservatorio delle Competenze Digitali 2021.
5. www.anitec-assinform.it/pubblicazioni/policy-paper/la-formazione-delle-competenze-avanzate-ict-linee-guida-per-una-scuola-diffusa.kl.
6. www.anitec-assinform.it/cosa-facciamo/iniziative-e-progetti/formati-con-noi/progetto/formati-con-noi.kl.
7. Per gli investimenti in beni materiali 4.0 (dal 40% al 20% per investimenti fino a 2,5 milioni, dal 20% al 10% per investimenti da 2,5 a 10 milioni e dal 10% al 5% per investimenti da 10 a 20 milioni) mentre per i software 4.0 si passa dalla superaliquota al 50% introdotta con il decreto aiuti al 20% per il 2023.
8. Con l'obiettivo di rafforzare l'ecosistema digitale nazionale potenziando sia le capacità di monitoraggio, prevenzione e risposta a rischi ed eventi Cyber che le capacità di valutazione e certificazione delle necessarie tecnologie Cyber.

PROFILO ANITEC-ASSINFORM

Anitec-Assinform è l'Associazione Italiana per l'Information and Communication Technology (ICT). Con sedi a Milano e Roma e oltre 700 associati – fra soci diretti e indiretti attraverso le Associazioni Territoriali di Confindustria. Un settore che nel suo insieme fattura oltre 21 mld ed occupa circa 70.000 addetti. È l'espressione di unione delle aziende dell'high-tech digitale, operanti in Italia, di ogni dimensione e specializzazione:
dai produttori di software, sistemi e apparecchiature ai fornitori di soluzioni applicative e di reti, fino ai fornitori di servizi a valore aggiunto e contenuti connessi all'uso dell'ICT ed allo sviluppo dell'innovazione Digitale.
È portavoce nazionale del settore ICT, motore dell'Innovazione dei processi aziendali e della pubblica amministrazione, elemento di sviluppo industriale competitivo, supporto indispensabile alla cittadinanza attiva.
Anitec-Assinform aderisce a Confindustria, è socio fondatore della Federazione Confindustria Digitale, la Federazione di categoria che promuove lo sviluppo e la società digitale in Italia ed è socio italiano e membro dell'Executive Board di DigitalEurope,
l'Associazione Europea dell'Industria ICT con sede a Bruxelles.
L'Associazione garantisce un'ampia gamma di servizi e attività; si fa portavoce delle necessità e delle esigenze delle imprese dell'ICT in diversi ambiti: legislativo (nazionale e comunitario), economico e di business, promozionale, formativo.
Sul fronte della rappresentanza, Anitec-Assinform è il canale privilegiato di dialogo fra le principali forze economiche, politiche ed istituzionali e del mondo digitale.

ANITEC-ASSINFORM - ASSOCIAZIONE ITALIANA PER L'INFORMATION TECHNOLOGY
Sede legale e uffici di Milano: Via San Maurilio, 21 – 20123 Milano
Tel. 02 0063 28 01 - Fax. 02 0063 28 24
Uffici Roma: Via Barberini, 11 - 00187 Roma
Tel. 0645417522
www.anitec-assinform.it - segreteria@anitec-assinform.it

AZIENDE ASSOCIATE ANITEC-ASSINFORM

3M Italia - Sistemi Informativi per la Salute
Accenture Spa
Adamantic Srl
ADS Automated Data Systems Spa
Advanced Micro Devices
Aitek Spa
Algowatt Spa
AlmavivA Spa
Amazon Italia Service Srl
Apkappa Srl
Apparound Italia Srl
Apple Italia Srl
Array System Srl
Atik Srl
Atomike Srl
Atos Italia Spa
Auriga Srl
Autec Srl
Axway Srl
Banksealer
Blulink Srl
BMC Software Srl
BT Italia
BTO Research
C.A.T.A. Informatica
Cadan Srl
Cefriel S.C.a R.L.
Certego Srl
Cisco
Cloud Europe Srl
Colin & Partners
Commvault Systems Italia Srl
Computer Care Srl
Computer Gross Spa
Confindustria Ancona
Confindustria Bari E Barletta-Andria-Trani
Confindustria Canavese
Confindustria Genova
Confindustria Trento
Consorzio Netcomm
Copying Srl
Corvallis Srl
CPI Srl
CyberArk Software Italy Srl
Cykel Software
Dassault Systemes Italia Srl
Data 4 Services Italy Spa
Data Masters Srl
Datacore Software
Db Elettronica Telecomunicazioni Spa
Dell Spa
Develhope
Digiquest Solutions
Digital Magics Spa
Dilium Srl
DVR Italia Srl
DXC Technology Italia
Ecoh Media Srl
Edicom Srl
El.Ca Elettronic System Srl
Elettromedia Srl
Emme Esse Spa
Epson Italia Spa
Equinix Italia Srl
Eris Srl
Esri Italia Spa
Euronet Srl
Eustema Spa
Experis Srl
Exprivia Spa
Facebook Italy Srl
FacilityLive OpCo Srl
Fasternet Srl
Fibernet Srl
Fitre Spa

Flow Factory Srl
FN & Partners Srl
Focus Group Srl
Fondazione Asphi
Formatech Srl
Fracarro Radioindustrie Srl
Futurenext Srl
Google Italy Srl
GPI Spa
Gruppo Industriale VESIT Spa - Società Unipersonale
Gruppo Pragma Srl
GVS Srl
Heta Lab Srl
Hewlett Packard Enterprise
Hiperforming Research Srl
Hitachi Vantara
Hp Italy Srl
IBM Italia Spa
ICT Consulting Spa
ICT Logistica Spa
ID Technology
Ids Georadar Srl
IFM Srl
iGenius Srl
INAZ Srl
InfoCamere SCpA
Informatica
Injenia Srl
Inmatica Spa
Insiel Spa
Intel Corporation Italia SpA
iSimply Learning Srl
IT Finance Srl
Italtel Spa
Itinera Srl Unipersonale
J Fin Servizi finanziari Srl
Juniper Networks Italy Srl
JVCKENWOOD Italia Spa
Kaspersky
Kelyon srl
Keysight Technologies Italy Srl
Kibernetes Srl
Laser Srl
Leading Kite Srl
Lenovo (Italy) Srl
Leonardo Spa
LG Electronics Italia Spa
Liguria Digitale Spa
Links Management & Technology Spa
Livemote Srl
Logic Sistemi Srl
Lumia Srl
Lutech Spa
Maggioli Spa
Mare Engineering Spa
Maticmind Spa
Maxfone Srl
Mediafarm Srl
Mediterraneo Lab 4.0 Srl
Mega Italia Media Spa
Meliconi Spa
Message Spa
Microsoft Srl
Microsys Srl
Mida
Midland Europe
Miller & Partners Srl
Minsait (An Indra Company)
Mostaza Srl
Motorola Solutions Italia Srl
Movenda Spa
Mychicjungle Srl
MYLIA – The Adecco Group
Nami Lab Srl
Nana Bianca Srl
Neulos Visiotech Srl
Nodopiano Sas
Nokia Solutions and Networks Spa
Nolan Norton Italia Srl
NTT Italia Spa
Ocra Srl
Olivetti Spa
Open 1 Srl

Opinno Italia
Oracle Italia
Orange Business Services
PagoPa Spa
Panasonic Italia Spa
Pentastudio Srl
Philip Morris Italia Srl
Pipecare Srl
Planet Idea Srl
Polo Navacchio Spa
Present Spa
Proclesis Srl
Projectfarm Srl
Protom Group S.p.a
Proxel Srl
QiBit - Divisione Ict di Gigroup Spa
Qualcomm Inc.
Qualta Spa
Quid Informatica Spa
Red Hat Srl
Reply Spa
R-Store SpA
Safra Srl
Saiet Telecomunicazioni Srl
Samsung Electronics Italia Spa
Schneider Electric Spa
SecLab Srl
Secure Network Srl
Sesa Spa
SIDI Srl
Sinapto Srl
Sisal Spa
Siscom Spa
Sit Srls
Sogei — Società Generale d'Informatica Spa
Sony Europe BV
Sorint.Lab
Strong Italia Srl
Synapsis Srl
Talents Venture
Tecnologica Srl
TELE System Digital Srl
The Next Srl
TikTok Italy S.R.L.
TIM Spa
Tinn Srl
TJ Point Srl
Tp Vision Italy Srl
Transaction Network Services Srl
Trend Micro
Tsp Association
Tvn Srl
Umana Spa
Unione Industriale Di Torino — Gruppo I.C.T.
Unisapiens
Var Group Spa
Var Group Srl
Var4Advisor Srl
Velocar Srl
Vem sistemi Spa
Veritas Italy Srl
Versya Srl
VMware Italy Srl
Westpole Spa
While True Srl
Xiaomi Technology Italy Srl
Zucchetti Centro Sistemi

REALIZZATO E PUBBLICATO DA ANITEC-ASSINFORM.

CONTENUTI A CURA DI NETCONSULTING CUBE:

- Le previsioni 2022-2025 per il mercato digitale italiano
- Cybersecurity e transizione digitale

CONTENUTI A CURA DI ANITEC-ASSINFORM:

- Conclusioni

Revisione editoriale: Filippo Cavazzoni
Coordinamento: Luisa Bordoni
Grafica e impaginazione: Studio Zanoni sas - Milano
Pubblicato in versione elettronica – Novembre 2022
Chiusura testi - Novembre 2022

CONFINDUSTRIA DIGITALE

Anitec-Assinform

Anitec-Assinform
www.anitec-assinform.it
segreteria@anitec-assinform.it
tel. 02 00632801

Confindustria Digitale
www.confindustriadigitale.it
segreteria@confindustriadigitale.it
tel. 06 45417541