CONFINDUSTRIA DIGITALE

Anitec-Assinform

IL DIGITALE IN ITALIA 2021

Previsioni 2021-2024 e Policy

CONFINDUSTRIA DIGITALE

Anitec-Assinform

IL DIGITALE IN ITALIA 2021

Previsioni 2021-2024 e Policy

Novembre 2021

Con la collaborazione di

Net Consulting 3
Empowering your Digital Business

PREMESSA

Questa edizione del Rapporto coincide con una fase particolarmente vitale del nostro settore. Le previsioni ci consegnano un 2021 che dovrebbe chiudere con una crescita del 5,5%. Se le previsioni per l'anno in corso sono ancora vincolate alle dinamiche della pandemia, le prospettive di medio termine vedono una crescita media annua del 5,1% fino al 2024.

Già nell'edizione di luglio abbiamo rilevato come la pandemia abbia imposto un'accelerazione della transizione digitale in ogni settore della nostra società: dall'industria alla Pubblica Amministrazione alle interazioni sociali. Il 2020 ci ha consegnato un Paese che ha più consapevolezza del ruolo strategico della tecnologia e lo si vede anche nella risalita dell'Italia nella graduatoria DESI, l'Indice di digitalizzazione dell'economia e della società, che nell'edizione 2021 vede l'Italia al 20mo posto fra i 27 Stati membri dell'UE, dal 25mo dell'edizione 2020.

Il digitale è oggi il campo su cui si gioca la competizione globale: i grandi blocchi geopolitici – Stati Uniti, Europa, Cina – hanno piani ambiziosi di sviluppo in questo settore (pensiamo all'intelligenza artificiale o alla cybersecurity) che si traducono in investimenti pubblici e privati, e in iniziative di policy finalizzate a definire le nuove regole del gioco. Di contro, il digitale interesserà lo sviluppo di nuovi mercati e farà nascere nuovi player in altre aree del mondo. Ma la competitività di aziende e nazioni si misurerà non più solo in capacità di "produrre valore economico" ma anche in capacità di produrre un nuovo tipo di valore che includa il benessere delle persone, l'impatto sull'ambiente e una maggiore inclusività.

In questo quadro, l'Italia con il Piano Nazionale di Ripresa e Resilienza (PNRR) si gioca oggi la chance di poter recuperare i ritardi accumulati nel tempo e affrontare in maniera sinergica la transizione ambientale ed energetica e quella digitale, sfruttando il ruolo strategico delle nuove tecnologie. Per il nostro mercato, le nuove risorse del PNRR incideranno complessivamente per 29,2 miliardi nel periodo 2021-2024 (nell'ipotesi più ottimistica che il 100% delle risorse messe a disposizione per il Paese venga sbloccato ed effettivamente utilizzato), ovvero tra gli 8 e i 9 miliardi all'anno a partire dal 2022, incrementali rispetto a un mercato "fisiologico" tra i 75 e gli 87 miliardi annui.

Per le imprese, la PA, la scuola e il mondo dei servizi ciò implica affrontare nuove e vecchie sfide e, tra queste, la sicurezza dei dati e la creazione del capitale di conoscenza e delle nuove competenze sono quelle più urgenti e non eludibili.

In questa occasione, abbiamo deciso di approfondire il mercato della cybersecurity. L'accelerazione della trasformazione digitale ha aumentato significativamente l'esposizione di aziende, enti e individui alle minacce cyber, specialmente laddove non si è avuto modo di pianificare con attenzione questo cambio di paradigma. Nel Rapporto vedremo i rischi per l'industria manifatturiera, oggi nel paradigma Industria 4.0, e per le infrastrutture pubbliche a servizio di imprese e cittadini. Vedremo come nuove minacce emergano ogni giorno, con una crescita esponenziale di casi e – conseguentemente – di investimenti in cybersecurity. Proteggere reti, sistemi e dati è una priorità urgente, un imperativo, che richiede un approccio consapevole, sistematico e coeso sia a livello nazionale che a livello europeo.

La digitalizzazione è innovazione, è sicurezza, è competenze, è conoscenza, è condivisione e collaborazione tra pubblico e privato.

Investire e creare un sistema di regole che supportino l'azione del privato e portino il digitale a essere inclusivo e accessibile, riducendo nel contempo le esternalità negative e rendendo palesi le opportunità offerte dal digitale, sarà l'obiettivo per cui ogni attore pubblico e privato dovrà impegnarsi nei prossimi anni per far sì che le nuove tecnologie siano il motore della crescita e dello sviluppo del Paese.

Marco Gay

Presidente Anitec-Assinform

INDICE

LE PREVISIONI 2021-2024 PER IL MERCATO DIGITALE ITALIANO

La situazione economica del Paese sta beneficiando dell'efficacia della campagna vaccinale e del conseguente contenimento della pandemia. L'andamento del PIL mondiale, incluso quello dell'Italia, è in crescita e le previsioni redatte dalle principali istituzioni internazionali confermano questa tendenza anche per il 2022. All'interno di questo scenario, il mercato digitale italiano continua la sua ripresa ed è previsto in crescita al termine dell'anno in corso (+5,5% rispetto al 2020). Tutti i comparti faranno registrare un segno positivo ad eccezione del segmento dei Servizi di Rete. Nei prossimi tre anni (2022-2024) continuerà ad aumentare il volume d'affari del digitale, grazie anche all'impatto positivo delle risorse e delle riforme previste dal Piano Nazionale di Ripresa e Resilienza.

PIL ITALIANO

5,8%
2021

Per il Fondo Monetario Internazionale il PIL italiano crescerà del 5,8% nel 2021 e del 4,2% nel 2022

2022
4,2%

36.069 mln€ **+5,7%**

Nel primo semestre del 2021 il mercato digitale si è attestato a 36.069 milioni di euro (+5,7% rispetto allo stesso periodo del 2020)

1° e 2° SEMESTRE 2021

I comparti Dispositivi e Sistemi, Software e Soluzioni ICT, Servizi ICT, Contenuti e Pubblicità Digitale sono stati in crescita.

Solo i Servizi di Rete hanno fatto registrare una contrazione

CRESCITA MERCATO DIGITALE

2022	5,1%
2023	5,0%
2024	4,9%

Grazie agli investimenti del PNRR, il mercato digitale dovrebbe crescere, secondo lo scenario più ottimistico, di un ulteriore 5,5% nel 2022;

secondo lo scenario meno ottimistico di un ulteriore 2,8%

Nel triennio 2022-2024 i principali driver tecnologici continueranno a essere i Digital Enabler (Cloud Computing, Big Data, AI, IoT, Cybersecurity)

INVESTIMENTI PER TECNOLOGIE E DIGITALIZZAZIONE

PNRR

2022	7,8 mld
2023	9,1 mld
2024	8,9 mld

LE PREVISIONI 2021-2024 PER IL MERCATO DIGITALE ITALIANO

Previsioni per l'economia italiana

Nel corso del 2021 la situazione sanitaria ed economica del Paese è nettamente migliorata, l'obiettivo del Governo di vaccinare almeno l'80% della popolazione si sta avvicinando, generando un contenimento del rischio e dell'impatto di una quarta ondata pandemica.
Il quadro economico ne sta beneficiando: tutti gli Istituti economici prevedono una ripresa dell'economia italiana, anche se lo scenario globale resta incerto. Diversi sono i fattori che alimentano questa situazione di incertezza: possibile frenata della crescita della domanda complessiva mondiale; carenza di materie prime e componenti e forti aumenti dei prezzi dell'energia che potrebbero ostacolare o rendere particolarmente onerosi i piani di produzione delle aziende; eventuale rischio di diffusione di varianti più pericolose di Covid-19 che potrebbero partire dai Paesi più poveri e con un tasso di vaccinati ancora limitato; tensioni finanziarie provenienti in particolare dalla Cina.
Tenendo conto di queste incertezze, le recenti previsioni del Fondo Monetario Internazionale per il 2021 prevedono a livello globale un PIL in crescita del 5,9% e del 4,9% nel 2022. Pesano in particolare gli outlook su alcuni Paesi avanzati in cui le campagne vaccinali non stanno rispettando i programmi. Anche le ultime stime dell'OCSE sono allineate e prevedono un incremento del PIL mondiale del 5,7% nel 2021 e una crescita del 4,5% nel 2022. Sempre secondo l'OCSE, il PIL mondiale ha superato i livelli pre-pandemia, ma permangono molte incertezze in particolare legate alla situazione sanitaria nei Paesi emergenti.
Le consuete previsioni di luglio della Commissione UE hanno previsto per l'Eurozona una crescita del PIL del 4,8% per l'anno in corso e del 4,5% nel 2022. Per l'ultimo trimestre del 2021 l'UE si attende il ritorno del PIL reale ai livelli pre-pandemia. Queste stime tengono in considerazione diversi aspetti: in primo luogo, l'andamento del primo trimestre dell'anno oltre le aspettative; in secondo luogo, l'efficace strategia di contenimento del virus e l'avanzamento delle campagne vaccinali, che ha consentito agli Stati membri dell'UE di riaprire le loro economie con un effettivo beneficio soprattutto per i servizi; infine, una ripresa dei consumi privati e del turismo in tutta l'UE.
A luglio, per l'Italia si stimava una crescita del 5% nel 2021 e del 4,2% nel 2022. A giugno, le previsioni dell'ISTAT ipotizzavano un aumento del PIL del 4,7% nel 2021 e del 4,4% nel 2022 (Tab. 1).

Le previsioni pubblicate a settembre dal Governo italiano evidenziano per il nostro Paese una crescita del PIL per l'anno in corso pari al 6% e del 4,7% nel 2022.
Nella "Nota di aggiornamento del DEF" di fine settembre, presentata dal Presidente del Consiglio Mario Draghi e dal Ministro dell'Economia e delle Finanze Daniele Franco, oltre alla soddisfazione per

Tabella 1:
Previsioni sull'andamento del PIL dell'Italia 2021-2022 elaborate da diverse organizzazioni – variazione % su anno precedente

Fonti	2021	2022
OCSE - settembre	5,9%	4,1%
Commissione Europea - luglio	5,0%	4,2%
FMI - ottobre	5,8%	4,2%
Banca d'Italia - marzo	5,1%	4,4%
ISTAT - giugno	4,7%	4,4%
Governo - settembre	6,0%	4,7%

Fonti: OCSE; Commissione Europea; FMI; Banca d'Italia; Istat; Governo

il contenimento e il controllo della pandemia grazie anche al comportamento responsabile dei cittadini, si pone l'accento sulla fase espansiva che l'Italia affronterà nei prossimi anni grazie al miglioramento del mercato monetario e finanziario, al ritorno della fiducia di imprese e consumatori e al Piano Nazionale di Ripresa e Resilienza (PNRR) che darà slancio a nuovi investimenti e a nuove riforme.

L'Italia ha ricevuto l'anticipo UE su sovvenzioni e prestiti dello strumento per la Ripresa e la Resilienza e ha definito le strutture tecniche di gestione e monitoraggio per la realizzazione del Piano, alcune riforme previste dal cronoprogramma sono già state realizzate, sebbene occorra completare gli investimenti previsti per accedere alla tranche successiva di finanziamenti. Secondo la Nota di aggiornamento, gli incrementi del PIL registrati negli ultimi mesi del 2021 riflettono già i risultati di alcuni stimoli all'innovazione ed all'efficientamento energetico finanziati dal PNRR ma non incorporano ancora il forte impulso agli investimenti pubblici, peraltro già in notevole crescita (quasi del 20% in termini nominali nel 2020 e del 16% nel 2021).

Stando alle previsioni del Governo il superamento del PIL pre-pandemia dovrebbe avvenire nel 2024, mentre per gli ultimi due anni di realizzazione del PNRR (2025 e 2026) si prevede una situazione ben superiore a quella precedente la crisi. Con queste premesse il Governo pensa di attuare una politica espansiva fino al 2024, anche per supportare le logiche occupazionali, per poi orientarsi a ridurre il disavanzo e a ricondurre il rapporto debito/PIL ai livelli pre-crisi entro il 2030.

La Banca d'Italia, nelle previsioni di marzo, ipotizzava una crescita del PIL del 5,1% nel 2021 e del 4,4% nel 2022 sulla base della ripresa del quadro economico mondiale e di contenimento della situazione pandemica. In questo contesto, secondo il Bollettino di luglio, l'Italia gioverebbe della spinta degli investimenti derivanti dal PNRR e di una accelerazione della crescita del PIL in particolare a partire dall'autunno, sempre che il cronoprogramma sia attuato nei tempi e nei modi previsti. In questo scenario il PNRR contribuirebbe nel periodo 2021-2023 alla crescita complessiva per circa 2 punti percentuali.

Sul fronte dell'occupazione, ci si attende per i prossimi trimestri la crescita del numero degli occupati per tornare al di sopra dei livelli pre-crisi entro i primi sei mesi del 2023. L'impatto della rimozione dei provvedimenti di blocco dei licenziamenti sull'occupazione complessiva viene, nelle simulazioni, in larga misura compensato dalle nuove assunzioni. Il tasso di disoccupazione, previsto in aumento nel 2021 (al 10,5%), si ridurrebbe a partire dal 2022.

Le revisioni sulle stime del PIL per l'Italia, pubblicate dal Fondo Monetario Internazionale (FMI) nel mese di ottobre, sono state migliorative: il PIL nel 2021 dovrebbe crescere del 5,8% e nel 2022 del 4,2%. La disoccupazione sarà in aumento (10,3% nel 2021 e 11,6% nel 2022) mentre l'inflazione dovrebbe rimanere sotto controllo.

Anche la Commissione Europea nel mese di luglio ha rivisto al rialzo le stime per il 2021: la crescita per l'Italia sarà del 5%, superiore al 4,2% previsto nella primavera. Per l'Unione Europea si ipotizza un miglioramento sensibile, stimato pari al 4,8% nel 2021 e al 4,5% nel 2022. Ci si attende inoltre che il PIL reale ritorni ai livelli pre-crisi nell'ultimo trimestre del 2021 sia nell'UE che nell'area dell'euro.

Secondo la Commissione UE, consumi ed investimenti dovrebbero trainare la crescita a livello europeo, mentre l'occupazione in questo scenario dovrebbe rafforzarsi.

Occorrerà monitorare attentamente l'andamento dell'inflazione, attesa in crescita nel 2021 per diversi motivi (aumento prezzi energia, carenza materie prime e intermedie di produzione, incremento della domanda di beni di consumo) e che tuttavia dovrebbe attenuarsi nel 2022, a seguito di un assestamento della produzione su livelli superiori e un maggior equilibrio tra domanda ed offerta.

Per il Vicepresidente della Commissione Europea Valdis Dombrovskis, dopo molti mesi l'economia europea è in recupero, con la fiducia dei consumatori e il turismo in netta ripresa, anche se occorre monitorare attentamente la situazione relativa a possibili varianti Covid-19. La crescita è da attribuirsi anche alla ripresa dell'attività economica, ad una strategia vaccinale efficace nei Paesi europei, al ritorno della mobilità nell'area Schengen grazie anche al nuovo certificato vaccinale digitale e al recupero del commercio internazionale.

In questo quadro si prevede che il piano di Ripresa e Resilienza darà un buon supporto alla crescita. Con lo strumento Next Generation EU, di cui il dispositivo per la Ripresa e la Resilienza è il nucleo centrale, l'UE ha messo a disposizione un pacchetto di stimoli all'economia e una dotazione di 806,9 miliardi di euro a favore dei 27 Paesi membri, con lo scopo ultimo di costruire un'Europa futura più ecologica e sostenibile, digitale e resiliente.

A questo proposito si rammenta che il documento relativo al piano di Ripresa e Resilienza riporta un'analisi di impatto delle misure sul PIL italiano, dove vengono quantificati gli effetti diretti del piano e non i possibili benefici di tipo indiretto. Il documento stima, rispetto ad uno scenario base, l'incremento del PIL costante nel periodo di piano: una cifra pari allo 0,5% in più nel 2021 che in modo progressivo arriva al 3,6% in più nel 2026. A questo risultato contribuiscono in modo preponderante due fattori:

- nel breve termine l'effetto di domanda innescato dalle maggiori spese per la costruzione e messa in opera degli investimenti pubblici;
- nel medio periodo l'impatto dei maggiori investimenti sull'aumento nello stock di capitale pubblico con effetti positivi sul PIL.

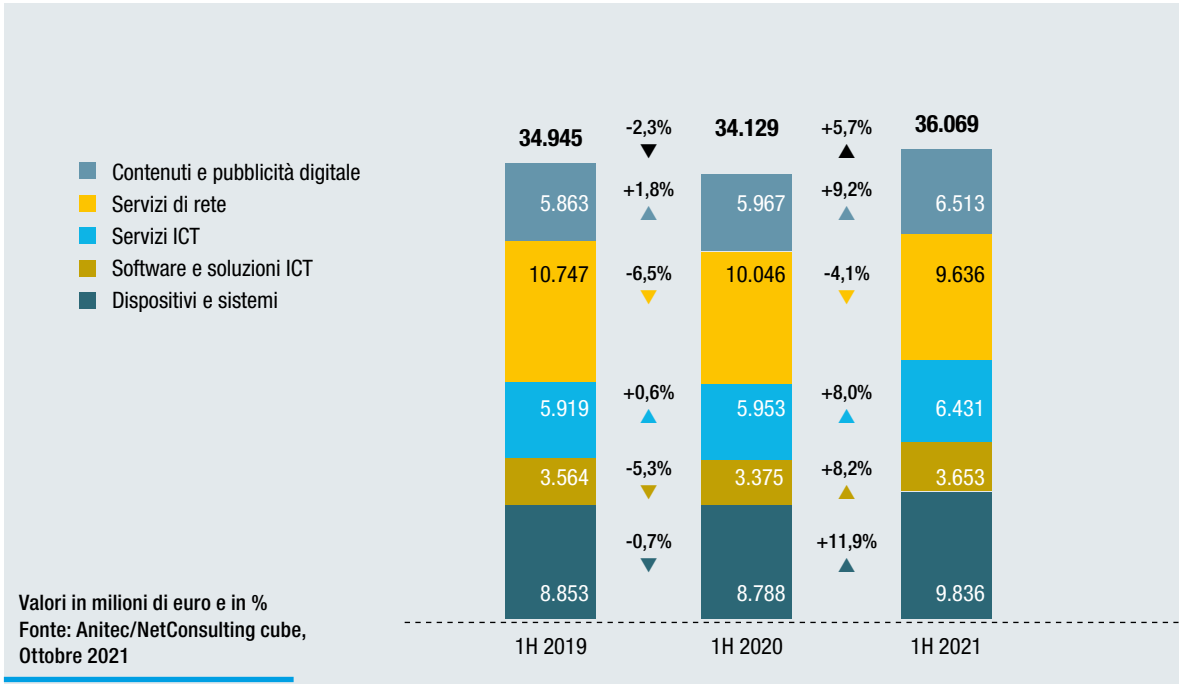
Rispetto allo scenario base, il documento ipotizza anche altri due scenari:

- il primo è uno scenario "medio", in cui vengono finanziati investimenti pubblici tradizionali, ossia investimenti con un'efficacia sul PIL di media intensità;
- il secondo è uno scenario "basso", in cui vengono finanziati investimenti pubblici con una minore efficacia e una minore ricaduta in termini di crescita del PIL potenziale.

Partendo da un dato fisso di incremento dello 0,5% nel 2021, viene ipotizzato un PIL nel 2026 rispettivamente del 2,7% in più nello scenario medio e dell'1,8% in più in quello basso. Secondo le conclusioni del piano, gli scenari dipenderanno dal tipo di investimenti selezionati e realizzati e in modo forse prevalente dal contesto degli stessi, ovvero i tempi di esecuzione, l'efficacia e la sostenibilità degli investimenti pubblici deriveranno in modo sostanziale dal regime di regolamentazione e dalla sua implementazione. Infine, l'efficacia degli investimenti pubblici richiederà un forte coordinamento tra i diversi livelli di governo e di amministrazione.

Figura 1:

Il mercato digitale in Italia nel primo semestre, 2019-2021



Valori in milioni di euro e in %
Fonte: Anitec/NetConsulting cube, Ottobre 2021

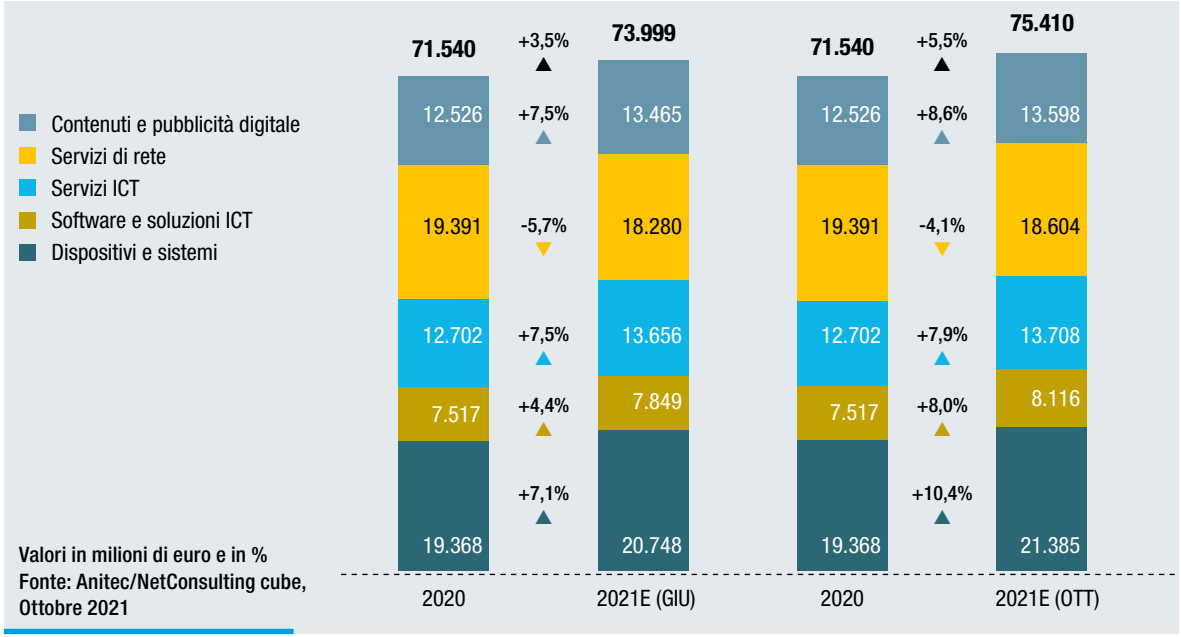
Dal punto di vista operativo, relativamente al PNRR, in estate l'Italia ha ricevuto 24,9 miliardi di euro di prefinanziamenti, pari al 13% di quanto stanziato complessivamente per il nostro Paese.

Andamento complessivo del mercato digitale nel primo semestre 2021

In linea con lo scenario economico, il mercato digitale in Italia nel primo semestre 2021 è stato caratterizzato da una ripartenza degli investimenti ICT, che avevano invece fatto registrare una contrazione nel primo semestre dello scorso anno a causa dell'emergenza pandemica.
Gli investimenti e la spesa in tecnologie digitali hanno dimostrato di esercitare un ruolo determinante nella ripresa economica del Paese.
Il mercato digitale nel primo semestre del 2021 si è attestato a 36.069 milioni di euro, con un incremento del 5,7% rispetto allo stesso periodo dell'anno precedente (Fig. 1). Il primo semestre del 2020 aveva invece visto un decremento sui primi sei mesi del 2019 (-2,3%).
Il comparto dei **Dispositivi e Sistemi** ha avuto un incremento importante (+11,9%), portandosi a 9.836 milioni di euro. In questo segmento di mercato si segnalano le crescite dei PC Laptop (+23,5%), dei Tablet (+20,7%) e degli apparecchi TV (+21,7%). Buona anche la performance degli Smartphone nel primo semestre (+19,8%).
Il comparto dei **Software e Soluzioni ICT** ha segnato un incremento dell'8,2%, arrivando a 3.653

milioni di euro, dovuto ad un aumento della spesa per acquisti di software middleware, nei segmenti dell'information management, della sicurezza e della collaboration, e di software applicativo.
Il valore del mercato dei **Servizi ICT** è stato, nel primo semestre 2021, di 6.431 milioni di euro, in aumento dell'8% rispetto allo stesso periodo dello scorso anno. In tale contesto si segnala la continua e costante crescita del mercato cloud (+23,7% nel primo semestre 2021) e di tutti i comparti dello sviluppo e manutenzione delle applicazioni e della system integration che avevano subito le maggiori contrazioni nello stesso periodo dello scorso anno.
I **Servizi di Rete** hanno registrato un valore di mercato nel primo semestre 2021 pari a 9.636 milioni di euro, evidenziando un'ulteriore contrazione (-4,1%). In tale contesto si segnala una diminuzione, più contenuta rispetto allo scorso anno, dei servizi di rete fissa (-1,6%), ma un decremento maggiormente importante (-6,4%) dei servizi di rete mobile.
Il segmento dei **Contenuti e Pubblicità Digitale** ha chiuso il primo semestre del 2021 con un mercato di 6.513 milioni di euro e una crescita del 9,2%.
Particolarmente positivi i mercati del digital advertising (+11,5%), delle applicazioni mobile (+9,8%) e del gaming online.
La crescita del mercato digitale nel primo semestre 2021 conferma la sempre maggiore rilevanza di questo comparto nel gestire e sostenere la crescita economica in generale e delle imprese in particolare.

Figura 2:
Il mercato digitale in Italia nel 2021



Valori in milioni di euro e in %
Fonte: Anitec/NetConsulting cube, Ottobre 2021

Andamento complessivo del mercato digitale nel 2021

Le dinamiche nella seconda metà del 2021, pur confermando un trend positivo, sono influenzate dalla carenza di materie prime e dei chip nonché da un generale aumento dei costi indiretti quale quello dei trasporti di merci ad alta tecnologia.
In generale, nell'anno in corso, tutti i comparti sono comunque previsti in crescita e con un trend in miglioramento rispetto alle previsioni dello scorso giugno. L'unica eccezione è rappresentata dal segmento dei Servizi di Rete, per il quale si stima il proseguimento del calo già osservato negli anni scorsi (Fig. 2).
Tra le maggiori differenze rispetto alle previsioni di giugno si evidenziano:

- un aumento dei Dispositivi e Sistemi grazie alla crescita maggiormente sostenuta nei segmenti degli apparecchi TV, che beneficiano dello switch off delle vecchie frequenze del digitale terrestre, dei personal computer, per effetto dell'esigenza di rinnovare il parco installato, rimasto fermo per un anno, così come i device mobili, quali smartphone, tablet e smartwatch;
- una crescita ulteriore del segmento software per effetto del processo di accelerazione della digitalizzazione in tutti i comparti;
- una previsione in aumento dei contenuti digitali a causa soprattutto delle maggiori crescite registrate nel segmento del Digital Advertising.

Tutti gli altri segmenti di mercato (Servizi ICT e Servizi di Rete) risultano sostanzialmente confermati agli stessi livelli di crescita previsti a giugno.

Previsioni del mercato digitale e dei comparti tecnologici: 2021-2024

Le previsioni sul mercato digitale nel prossimo triennio sono molto condizionate non solo dall'entità di una ripresa economica endogena, ma anche dalla consistenza dei progetti finanziati dal PNRR destinati alla trasformazione digitale della Pubblica Amministrazione e del sistema produttivo, per i quali non è però ancora possibile prevedere completamente gli effetti.

Sulla base di queste considerazioni, nel 2022 si prevede un ulteriore apprezzabile aumento del mercato digitale italiano, con una crescita complessiva del 5,1%, a 79.286 milioni di euro, quasi 4 miliardi di euro in più rispetto al 2021. Per il biennio 2023-2024 la previsione è di una conferma della crescita (+5,5% nel 2023 e +4,9% nel 2024), con un mercato nel 2024 che si prevede attestarsi intorno agli 87 miliardi di euro (Fig. 3).

Nel triennio 2022-2024 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.

La conferma dei progetti di modernizzazione infrastrutturale avrà un impatto positivo sul segmento dei **Dispositivi e Sistemi**. Nel 2022, si prevede un ulteriore aumento degli acquisti nei segmenti degli apparecchi TV (+20,4%) per quanto concerne il consumer, dei server high end e X86 e delle stampanti nel segmento

Figura 3:
Il mercato digitale in Italia, previsioni 2021-2024

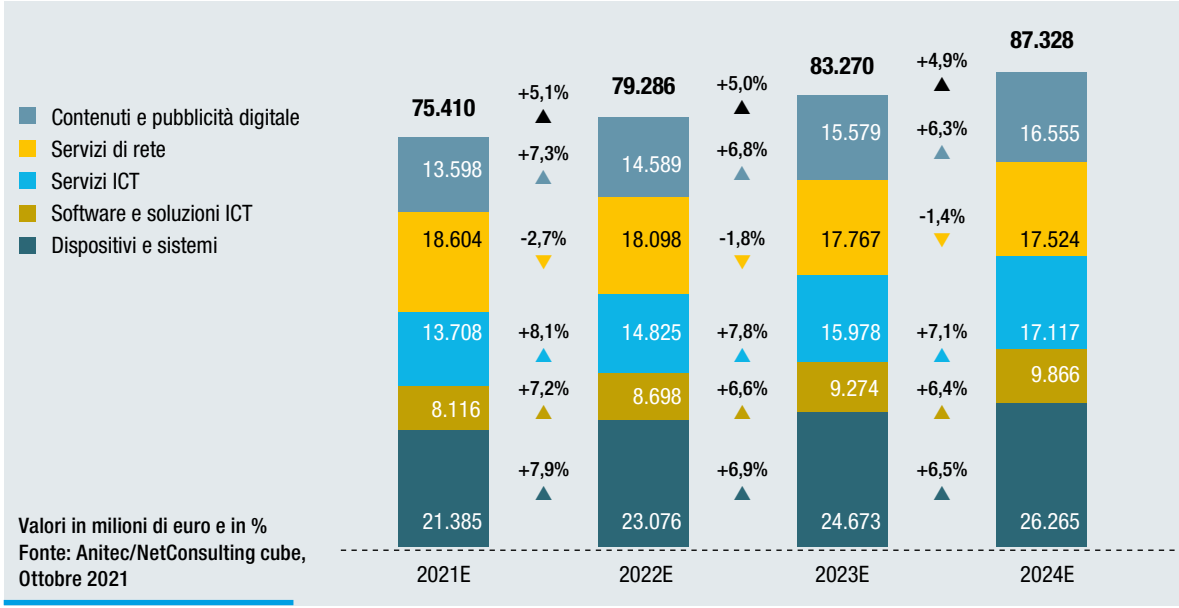
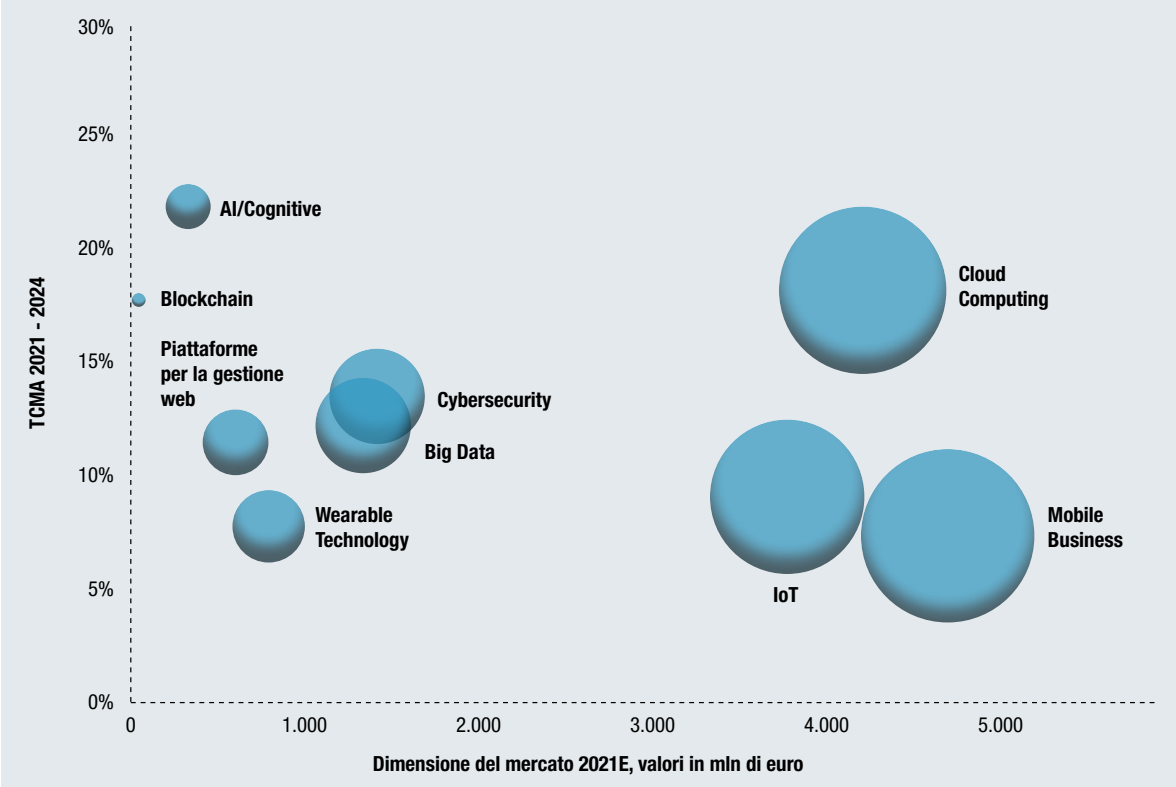


Figura 4:

Dimensioni e trend dei Digital Enabler, previsioni 2021-2024



business. Sono previsti andamenti positivi anche nei comparti dei sistemi di comunicazione e dei sistemi specializzati, per l'esigenza di potenziare le reti e rinnovare i sistemi in alcuni settori, primo tra tutti quello sanitario. Per quanto riguarda i device mobili, è previsto, sempre nel 2022, un ulteriore aumento per gli smartphone (+10,9%) e una sostanziale conferma della crescita di PC Laptop (+9,4%) e Tablet (+9,2%).
Con il riavvio dei progetti applicativi e di digital transformation anche i comparti del **Software e Soluzioni ICT** e dei **Servizi ICT** sono previsti in forte ripresa. In particolare, nel 2022 e per quanto concerne il comparto Software si prospetta un andamento positivo essenzialmente nelle aree del software di sistema, grazie alle maggiori vendite di server e agli aggiornamenti verso il nuovo sistema operativo Windows 11 Pro, del software middleware e del software applicativo, in funzione di maggiori acquisti in piattaforme e-commerce e di gestione web e di soluzioni IoT relative all'industria 4.0.
I **Servizi ICT** beneficeranno di una crescita dei progetti di sviluppo applicativo e di system integration, sulla spinta dei progetti di digitalizzazione e di re-platforming di applicazioni nonché di conteinerizzazione per sostenere la migrazione al cloud, che proseguirà la sua crescita, considerata la centralità che assume nei piani di trasformazione digitale. Un deciso aumento faranno registrare anche i servizi di Consulenza ICT (+4,9%). Il rilancio degli investimenti in Digital Advertising farà da traino alla crescita del mercato dei **Contenuti e Pubblicità Digitale**, che dovrebbe raggiungere nel 2022 i 14.589 milioni di euro (+7,3%) nel 2022, i 15.579 milioni (+6,8%) nel 2023 e i 16.555 milioni (+6,3%) nel 2024.

Previsioni per i Digital Enabler: 2021-2024

Nel triennio 2022-2024, i principali driver tecnologici continueranno a essere i Digital Enabler – trasversali a tutti i comparti merceologici dell'ICT e che permettono il continuo sviluppo di nuove soluzioni – che già negli ultimi anni hanno dato un forte impulso al mercato digitale (Fig. 4).

Più in particolare:

- continuerà in misura sempre maggiore l'utilizzo di servizi di **Cloud Computing**, che è diventato oramai una scelta alla base dell'evoluzione dei sistemi informativi delle medie e grandi aziende e per le piattaforme dei servizi online. Il mercato cloud si prevede possa raggiungere quasi i 7 miliardi di euro nel 2024 con una crescita media annua nel 2021-2024 del 18%;
- un forte impulso continuerà a venire dal mercato dei **Big Data**, con investimenti che coprono tutta la filiera del dato, che si prevede possa raggiungere i 2 miliardi nel 2024, con una crescita media annua nel periodo 2022-2024 del 12%;
- a questa visione è connessa anche la crescita degli strumenti e dei sistemi di **Intelligenza Artificiale** (o AI), che già nei prossimi anni inizierà a essere implementata su una scala più ampia a supporto dei piani strategici, delle operazioni commerciali e di marketing, dell'ottimizzazione della produzione. Per tale mercato è prevista una crescita media annua del 22% negli anni 2022-2024;
- l'**IoT**, che ha sofferto la crisi indotta dalla pandemia nel 2020, tornerà a crescere nei prossimi anni anche grazie alla spinta delle misure inserite nel PNRR per quanto concerne soprattutto la componente relativa all'Industrial IoT;
- un marcato sviluppo caratterizzerà ancora la **Cybersecurity**, a cui viene dedicato un capitolo in questo rapporto. Con la crescita della digitalizzazione e delle attività in rete, le minacce sono sempre più in aumento e diventano più sofisticate, mettendo a rischio la sicurezza di dati e sistemi e la continuità operativa. Questo indurrà le aziende a incrementare gli investimenti in Cybersecurity.

Previsioni per settori d'utenza: 2021-2024

Le previsioni di ripresa del mercato digitale in Italia evidenziano anche per il periodo 2022-2024 una maggiore dinamicità della componente business (aziende e amministrazioni) rispetto a quella consumer (famiglie) (Fig. 5).

Figura 5:
La domanda digitale per settore di utenza, previsioni 2021-2024

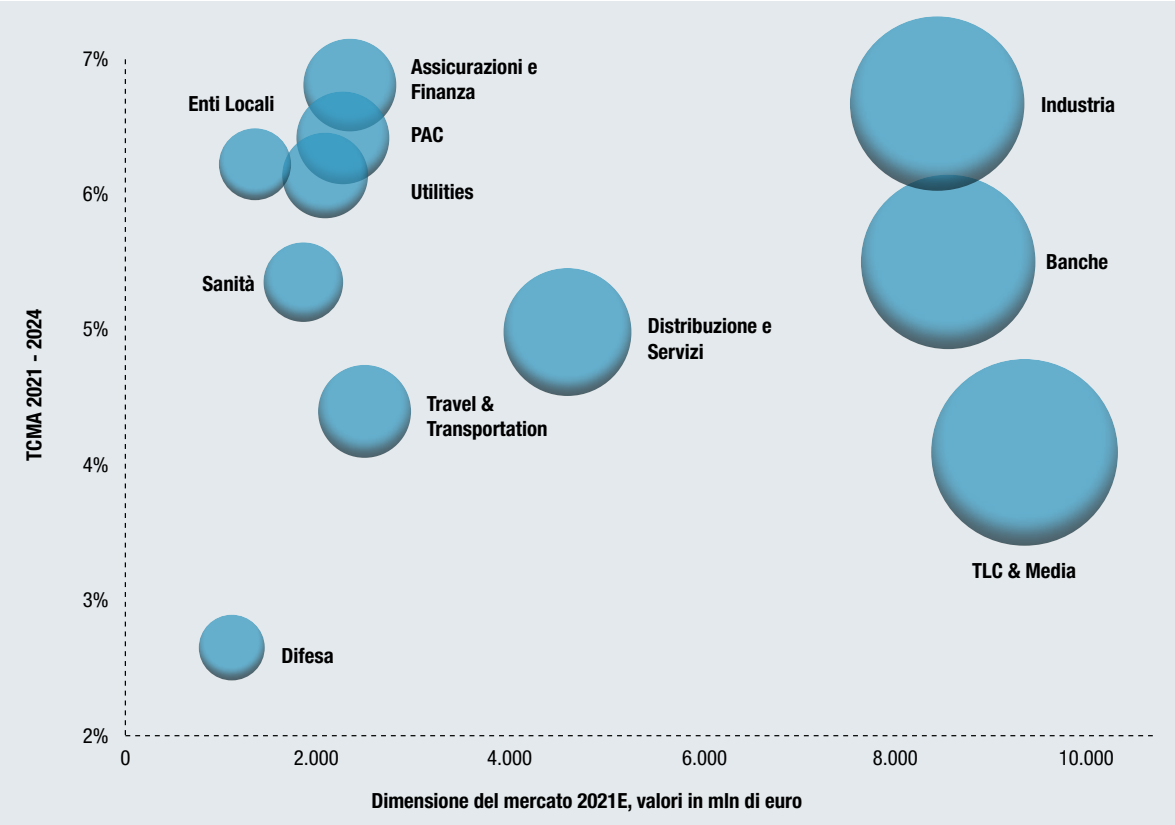


Tabella 2:

Il mercato digitale in Italia per settore economico, 2020-2024E

Valori in milioni di euro
Fonte: NetConsulting cube, Ottobre 2021

Dati in mln€	2020	2021E	2022E	2023E	2024E	21E/20	22E/21E	23E/22E	24E/23E	TCMA 20/24
Industria	7.909,1	8.366,7	8.895,0	9.472,5	10.161,4	5,8%	6,3%	6,5%	7,3%	6,5%
Banche	7.989,3	8.478,5	8.952,5	9.462,9	9.959,6	6,1%	5,6%	5,7%	5,2%	5,7%
Assicurazioni e finanza	2.159,1	2.301,2	2.467,4	2.638,7	2.806,5	6,6%	7,2%	6,9%	6,4%	6,8%
PAC	2.060,0	2.229,5	2.412,6	2.562,6	2.689,2	8,2%	8,2%	6,2%	4,9%	6,9%
Difesa	1.041,8	1.082,1	1.114,1	1.143,7	1.171,2	3,9%	3,0%	2,7%	2,4%	3,0%
Enti locali	1.246,2	1.333,6	1.421,4	1.511,6	1.599,6	7,0%	6,6%	6,3%	5,8%	6,4%
Sanità	1.706,4	1.819,6	1.923,1	2.027,7	2.129,3	6,6%	5,7%	5,4%	5,0%	5,7%
Utilities	1.924,2	2.049,8	2.183,4	2.320,0	2.453,3	6,5%	6,5%	6,3%	5,7%	6,3%
Telecomunicazioni & Media	8.815,3	9.302,7	9.709,8	10.110,0	10.494,0	5,5%	4,4%	4,1%	3,8%	4,5%
Distribuzione e Servizi	4.301,0	4.555,4	4.796,5	5.038,5	5.272,9	5,9%	5,3%	5,0%	4,7%	5,2%
Travel & Transportation	2.360,6	2.460,7	2.567,4	2.686,6	2.801,5	4,2%	4,3%	4,6%	4,3%	4,4%
Consumer	29.991,5	31.430,6	32.843,2	34.295,6	35.789,4	4,8%	4,5%	4,4%	4,4%	4,5%
Totale Mercato Digitale	**71.504,5**	**75.410,6**	**79.286,3**	**83.270,4**	**87.327,9**	**5,5%**	**5,1%**	**5,0%**	**4,9%**	**5,1%**

In ambito business, gli investimenti si concentrano in particolare sulla digitalizzazione della relazione con il cliente/cittadino e in generale sull'ammodernamento dei sistemi relativi ai processi core e su Data Management and Analytics. Dal punto di vista infrastrutturale, si osserva una propensione crescente all'adozione del cloud oltre a progetti di modernizzazione architetturale e applicativa. Si iniziano ad inglobare negli obiettivi di trasformazione digitale le linee di investimento previste nel PNRR, con intensità differenziata in base ai settori (Tab. 2).

Nell'**Industria** si prevede una domanda digitale in crescita del 5,8% nel 2021, a 8.366 milioni di euro, e del 6,3% nel 2022, a 8.895 milioni. La domanda in progetti e investimenti digitali è prevista particolarmente dinamica in particolare in ambito Cybersecurity, Fabbrica 4.0 e Data Analytics. Soprattutto la Cybersecurity è ormai un tema trasversale rispetto al sistema di R&D e produzione, alla supply chain e agli ambienti IT/OT.

In alcuni comparti industriali si mantiene elevata l'attenzione sul tema della supply chain, che deve essere sempre più agile e flessibile, mentre in ambito dati si osservano progetti relativi ai software per la raccolta, l'integrazione e l'archiviazione dei dati e all'introduzione di data lake. Cresce anche l'attenzione verso il cliente, con un incremento dei progetti in ambito CRM e verso il digital customer.

Per le **Banche**, la previsione è di una domanda digitale in crescita del 6,1% nel 2021 a 8.478 milioni di euro e del 5,6% nel 2022 per un mercato di 8.952 milioni. Il settore ha dimostrato una intensa resilienza nel periodo della pandemia, puntando sul digitale per garantire continuità di servizio alla clientela, attraverso i servizi già presenti sui canali online e la creazione di nuovi. Questo trend risulta accelerato dal proseguimento del processo di riduzione delle filiali, che ha subito un'ulteriore accelerazione a causa della situazione sanitaria. I progetti di innovazione digitale si sono concentrati principalmente nell'adozione o nel rinnovo di piattaforme di internet e, ancor più, di mobile banking. Oltre all'evoluzione del modello di relazione con il cliente in logica digitale, la Cybersecurity è un altro ambito prioritario di progetti digitali, seguito da Data Platform e Data Strategy, in particolare attraverso progetti di Data Governance intesi a sviluppare Business Glossary e Data Catalog. Anche la modernizzazione applicativa rappresenta una priorità per quelle banche che hanno intrapreso programmi di rinnovo delle applicazioni e di revisione architetturale finalizzati ad adeguare i sistemi di back

end alla maggiore velocità di risposta richiesta dai canali digitali.

Per il settore **Assicurazioni e Finanza** la domanda digitale nel 2021 è prevista in crescita del 6,6% (per un valore pari a 2.301 milioni di euro), che si rafforzerà ulteriormente nel 2022 raggiungendo un incremento del 7,2% nel 2022, portandosi a 2.467 milioni. Anche in questo settore, nelle attività di vendita si intensifica l'ibridazione tra canali tradizionali e digitali, mentre il digitale permea sempre di più le aree marketing, back office e customer care. Nell'ambito dello sviluppo di prodotti, in particolare nelle polizze salute, la tecnologia, si pensi all'IoT, al 5G e ai wearables, viene sempre più adottata. Tra i principali investimenti in digitale, nelle agende delle compagnie di assicurazioni si trovano le soluzioni per il digital customer, la modernizzazione applicativa, sia per effetto della maggiore propensione al cloud, sia come evoluzione delle applicazioni, spesso custom, in uso. Tra le tecnologie più innovative, oltre all'applicazione dei sistemi di automazione nell'area sinistri per velocizzarne la gestione, si assiste ad un incremento di attenzione verso l'Intelligenza Artificiale (applicata su larga scala in tutto l'ambito di gestione sinistri e di stima del rischio per ogni cliente), la Blockchain e le Container Platform, queste ultime utilizzate in particolare per lo sviluppo di applicazioni cloud native.

Per la **Pubblica Amministrazione Centrale** si prevede una domanda digitale in crescita dell'8,2% sia nel 2021 che nel 2022, per un valore di mercato rispettivamente di 2.295 e 2.412 milioni di euro. Nel 2021 la PAC è il settore che realizza le migliori performance in termini di dinamica del mercato digitale.

Nella **Pubblica Amministrazione Locale** ci si attende una crescita del 7% nel 2021, a 1.333 milioni di euro, e del 6,6% nel 2022, a 1.421 milioni.

La sfida per la Pubblica Amministrazione Centrale e Locale rimane quella di essere sempre più digitale rispetto ai cittadini e alle imprese e di riuscire a realizzare riforme e investimenti previsti nel PNRR per portare l'amministrazione pubblica a diventare il perno del cambiamento in chiave digitale del sistema Paese e delle sue infrastrutture. Inoltre, sempre più strategico è il tema dell'integrazione di dati e applicazioni, per accrescere efficienza ed efficacia nell'erogazione dei servizi al cittadino. La Strategia Cloud

Italia, lanciata dal Dipartimento della Transizione digitale in collaborazione con l'Agenzia di Cybersicurezza nazionale, guiderà la transizione della Pubblica Amministrazione verso il principio cloud first, favorendo l'adozione prioritaria da parte della Pubblica Amministrazione di strumenti e tecnologie di tipo cloud nello sviluppo di nuovi servizi e nell'acquisizione di software.
Un ruolo fondamentale sarà ricoperto, come descritto nei paragrafi successivi, dai fondi del PNRR per l'ammodernamento e la digitalizzazione della Pubblica Amministrazione.
Nella **Difesa**, la domanda digitale registrerà una crescita del 3,9% nel 2021, per un valore di 1.082 milioni di euro, e del 3% nel 2022, assestandosi a 1.114 milioni di euro. Anche in questo caso la Cybersecurity rappresenterà il driver di una quota consistente di investimenti, considerata anche la necessità di adeguarsi a quanto previsto dal Piano di Resilienza Nazionale e dal Perimetro di Sicurezza Cibernetico.
Per il settore della **Sanità** si stima per il 2021 una crescita della domanda digitale del 6,6%, a 1.819 milioni di euro, e per il 2022 del 5,7%, a 1.923 milioni. Anche in ambito sanitario la trasformazione digitale risulta trainata dal PNRR e in particolare dalle disposizioni previste nella missione 6 con le due componenti di sanità territoriale e di ricerca e digitalizzazione. Il ripensamento della sanità su base territoriale, la cui esigenza è stata sottolineata dalla pandemia, prevede il disegno e la riorganizzazione del sistema della salute secondo la logica della prossimità, dove i luoghi della cura sono organizzati secondo i livelli di intensità. Questa riorganizzazione porta con sé un'elevata attenzione verso la Telemedicina per la riorganizzazione dei servizi sanitari, la modernizzazione applicativa sia dei sistemi informativi amministrativi che ospedalieri, l'importanza dell'integrazione e dell'interoperabilità dei sistemi, la strategicità della data architecture e della data strategy per rendere disponibile e utilizzabile il dato sanitario.
La spesa digitale nel settore delle **Utility** è prevista in crescita per entrambi gli anni del 6,5%, per un mercato digitale che vale 2.049 milioni di euro nel 2021 e 2.183 milioni nel 2022.
Il programma European Green Deal e gli obiettivi inseriti nel PNRR puntano a rendere l'Europa e l'Italia più sostenibili e "verdi", anche nel maggiore utilizzo di energie rinnovabili. L'impulso a investire in digitale è molto elevato, sia relativamente alle soluzioni innovative in ambito produttivo, sia alle infrastrutture di rete e trasporto come le smart grid.
I progetti riguardano da un lato le relazioni sempre più digitali con i clienti e i prospect che coinvolgono sistemi di CRM as a service o il miglioramento del customer engagement, dall'altro la razionalizzazione del back office con la ricerca di maggiori efficienze nella gestione dei processi, anche grazie all'utilizzo di soluzioni di RPA e Intelligent Automation. Molti progetti di digitalizzazione che prevedono un'accelerazione sono legati al mondo dati, ad esempio l'implementazione di soluzioni di Advanced Analytics, inclusi algoritmi di Intelligenza Artificiale e Machine/Deep Learning, che risulta correlata alla realizzazione di data lake unificati e sistemi per la gestione e l'archiviazione di grandi moli di dati. Infine, si assiste a una vivacità delle iniziative relative a Business Intelligence e Reporting.
Il settore **Telecomunicazioni e Media** evidenzia una domanda digitale in crescita del 5,5% nel 2021, per un mercato di 9.302 milioni di euro, e del 4,4% nel 2022 (9.709 milioni di euro).

I progetti di digitalizzazione vedono come principale area di investimento quella legata alle soluzioni digitali per i clienti, orientando l'attenzione a soluzioni sempre più personalizzate (campagne marketing profilate, programmi di engagement & loyalty, politiche di pricing customizzate). Importanti sono gli investimenti in Cybersecurity, mentre la realizzazione di data lake unificati e sistemi per la gestione e l'archiviazione e integrazione di grandi moli di dati rappresenta la base per conoscere in modo approfondito i propri clienti e personalizzare le azioni di marketing e distribuzione. In ambito dati, rilevanti sono i progetti per l'adozione di strumenti di Advanced Analytics, AI e Machine Learning. Sempre significativa è anche l'attenzione a progetti di modernizzazione applicativa.

Il settore **Distribuzione e Servizi** registra una stima di crescita del mercato digitale del 5,9% nel 2021, per un valore di 4.555 milioni di euro, e del 5,3% nel 2022, pari a 4.796 milioni.

L'intero settore ha risentito in modo marcato della situazione pandemica con diverse chiusure di punti vendita fisici, il ricorso al canale e-commerce non solo come risposta alle chiusure ma anche come canale prediletto dal cliente per evitare assembramenti e il cambiamento profondo dei comportamenti di acquisto. I progetti di digitalizzazione per l'anno in corso vedono come principale area di investimento le soluzioni per il Digital Customer, in particolare per il ridisegno e l'ottimizzazione dei processi di e-commerce, l'innovazione delle campagne marketing e di loyalty e il ripensamento delle strategie di comunicazione in ottica omnicanale e la digitalizzazione del punto vendita.

Infine, nel settore **Travel & Transportation** la spesa digitale è prevista in crescita del 4,2% nel 2021, a 2.460 milioni di euro, e del 4,3% nel 2022, a 2.567 milioni. Seppure il settore risulti profondamente colpito dalla situazione pandemica, nel periodo di emergenza sanitaria le imprese hanno investito in soluzioni digitali per supportare le proprie attività e garantire la continuità delle relazioni con i principali attori esterni, principalmente con i clienti. Gli investimenti previsti coinvolgono in primo luogo le aree marketing, vendite e operations. I progetti digitali riguardano l'adozione del cloud in particolare in ambito infrastrutturale e di piattaforma, soluzioni di RPA per efficientare ed automatizzare il back office, gli advanced analytics, soluzioni di digital customer per gestire al meglio le relazioni con clienti e prospect lungo l'intero processo commerciale, grazie all'implementazione di soluzioni, come ad esempio CRM/Social CRM, Chatbot, Social engagement, apps, che permettono di digitalizzare il processo di vendita in virtù dello sviluppo del canale e-commerce.

Gli investimenti del PNRR con elevato contenuto ICT

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.

Inoltre, seguendo le linee guida elaborate dalla Commissione Europea, 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 come sovvenzioni e 122,6 miliardi come prestiti.
Occorre inoltre considerare anche le risorse previste dal Fondo Complementare e dal Programma REACT_EU che portano le risorse complessive a disposizione del Paese da 191,5 miliardi di euro a 235,1 miliardi nel periodo 2021-2026 per la realizzazione di 142 progetti e riforme abilitanti, orizzontali e settoriali previste nel Piano.
Già nel corso dell'estate l'Italia ha ricevuto un prefinanziamento pari a 24,9 miliardi di euro (di cui 8,95 miliardi di euro a titolo di sovvenzioni e circa 15,9 miliardi di euro a titolo di prestiti), le future tranche verranno sbloccate in base alla realizzazione del cronoprogramma prestabilito, che per il 2021 prevede la realizzazione di 51 interventi complessivi (27 riforme che sono in linea con il programma e 24 investimenti), alcuni dei quali procedono più a rilento.
Fatta questa premessa, è evidente che il PNRR avrà un impatto significativo sul mercato digitale nei prossimi anni: diverse componenti delle missioni prevedono stimoli ed investimenti indirizzati alle tecnologie e al digitale.
Secondo le stime sono circa 41,1 i miliardi di euro che, all'interno delle varie missioni, componenti e investimenti, sono riconducibili a progetti digitali e ICT e che avranno quindi un diretto impatto sul mercato digitale. Di questi, circa 29 miliardi saranno spesi entro il 2024 secondo le stime di ripartizione tra i vari anni coperti dal Piano.
Per quanto riguarda il 2021, sono circa 3.352 i milioni che l'Italia dovrebbe impiegare su progetti digitali, una buona parte collocata nella missione 1, componente 2, relativa alla digitalizzazione, innovazione e competitività del sistema produttivo (circa 1,9 miliardi di euro) (Tab. 3).
Sempre nel 2021, altri centri di investimenti rilevanti sono rappresentati dalla PA (missione 1, componente 1) e dalla Sanità (missione 6, componente 2 relativa all'aggiornamento tecnologico e digitale).
Nel 2022 le risorse del PNRR impiegate in investimenti digitali e tecnologici dovrebbero passare a 7,8 miliardi, per diventare oltre 9 nell'anno successivo e assestarsi a 8,9 miliardi nel 2024. Digitalizzazione e ammodernamento del sistema produttivo e della Pubblica Amministrazione continueranno a rappresentare i principali centri di spesa nel periodo considerato.

Scenari di previsione del mercato digitale e impatto del PNRR

Le previsioni a tutto il 2024 del mercato digitale in Italia saranno condizionate in misura crescente dagli investimenti in ICT finanziati attraverso il PNRR. Per una prima valutazione dell'impatto di questi investimenti sul mercato digitale si è ritenuto opportuno delineare due scenari di previsione.
Scenario 1: rappresenta lo scenario ottimistico. Se-

	2021	2022	2023	2024
M1C1: PA - DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA PA				
1: Digitalizzazione PA	451	938	1.316	1.516
M1C2: DIGITALIZZAZIONE, INNOVAZIONE E COMPETITIVITÀ NEL SISTEMA PRODUTTIVO				
1: Competitività Sistema Produttivo	1.928	4.909	5.555	4.799
M1C3: TURISMO E CULTURA 4.0				
1: Patrimonio culturale di prossima generazione	11	59	124	147
2: Turismo 4.0	6	24	33	27
3: Industria culturale e ricreativa 4.0	6	6	34	34
M2C4: AMBIENTE - TUTELA DEL TERRITORIO E DELLA RISORSA IDRICA				
1: Rafforzare la capacità previsionale degli effetti del cambiamento climatico	0	150	150	100
3: Salvaguardare la qualità dell'aria e la biodiversità del territorio attraverso la tutela delle aree verdi	9	26	27	19
M3C2: INTERMODALITÀ E LOGISTICA INTEGRATA				
2: Logistica Integrata	38	41	44	76
M4C1: POTENZIAMENTO DELL'OFFERTA DEI SERVIZI DI ISTRUZIONE: DAGLI ASILI NIDO ALLE UNIVERSITÀ				
2: Miglioramento dei processi di reclutamento e di formazione degli insegnanti	150	200	300	100
3: Ampliamento delle competenze e potenziamento delle infrastrutture	0	550	450	550
M6C1: SANITA' - RETI DI PROSSIMITÀ, STRUTTURE E TELEMEDICINA PER L'ASSISTENZA SANITARIA TERRITORIALE				
1: Reti di prossimità, strutture e telemedicina per l'assistenza sanitaria	108	216	293	335
M6C2.1: SANITA' - AGGIORNAMENTO TECNOLOGICO E DIGITALE	419	373	499	695
INVESTIMENTI NEL DIGITALE DAL FONDO COMPLEMENTARE (D.L. 59 2021)				
1) Servizi digitali e cittadinanza digitale - Piattaforma PagoPA e App « IO »	50	100	100	50
2) Servizi digitali e cittadinanza digitale – Piattaforma notifiche digitali	1	47	27	29
3) Strade sicure – Messa in sicurezza e implementazione di un sistema di monitoraggio dinamico per il controllo da remoto di ponti, viadotti e tunnel (A24 – A25)	150	150	90	337
4) Strade sicure – Implementazione di un sistema di monitoraggio dinamico per il controllo da remoto di ponti, viadotti e tunnel della rete viaria principale	25	50	100	100
TOTALE INVESTIMENTI PNRR E FONDO COMPLEMENTARE IN TECNOLOGIE E DIGITALIZZAZIONE	**3.352**	**7.839**	**9.142**	**8.915**

Tabella 3:

I progetti ICT finanziati dal PNRR in base alle missioni e alle componenti, 2021-2024

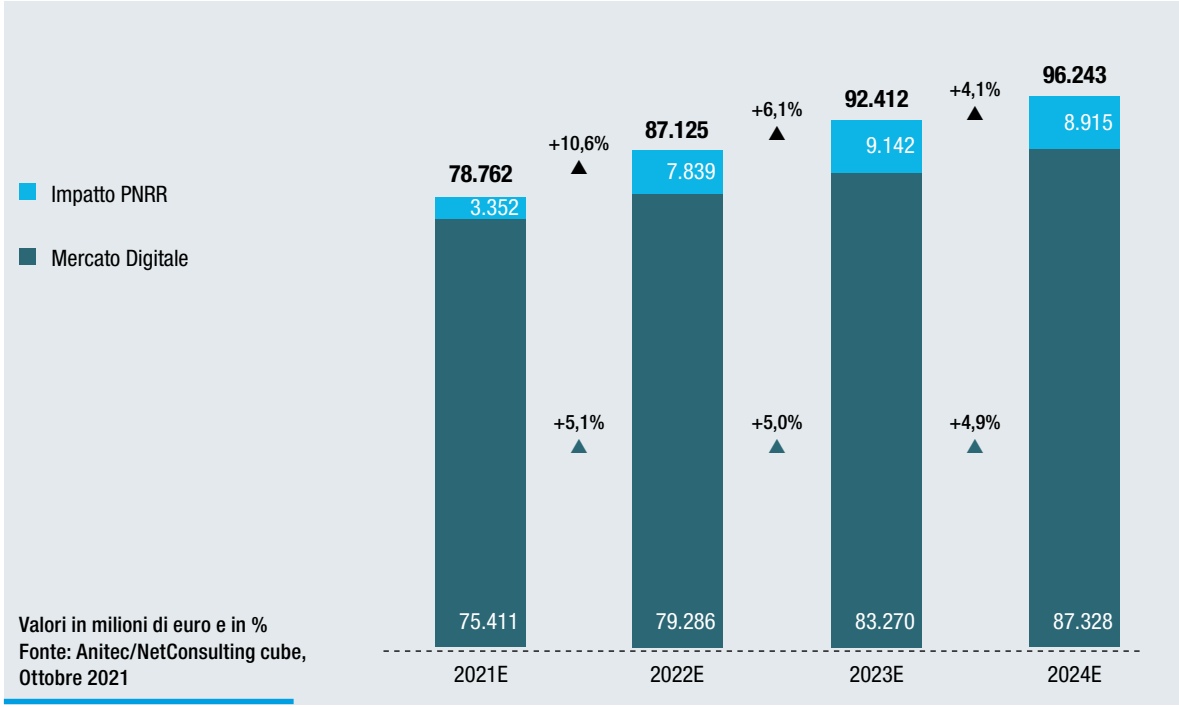
Valori in milioni di euro
Fonte: NetConsulting cube, Ottobre 2021

condo questo scenario alle previsioni descritte nei paragrafi precedenti si aggiungeranno le nuove risorse del PNRR, che incideranno complessivamente nel periodo 2021-2026 per 41,1 miliardi e nel periodo di analisi 2021-2024 per 29,2 miliardi.
Gli assunti macroeconomici validi per tale scenario riguardano:

- la conferma della ripresa economica e le stime sul PIL realizzate dal Governo;
- il completamento della campagna vaccinale arrivando a superare l'80% della popolazione vaccinata, procedendo con la terza dose per determinate categorie di cittadini;
- l'esecuzione delle riforme e la progressione degli investimenti come da cronoprogramma del PNRR e l'effettivo e pieno utilizzo delle risorse previste per il Paese.

Questo scenario si basa sull'assunzione che il 100% delle risorse messe a disposizione per il Paese venga sbloccato (previo il rispetto della realizzazione delle riforme e degli investimenti previsti nelle varie tranche, generalmente corrispondenti ai semestri) ed effettivamente utilizzato. Per raggiungere questo obiettivo, tuttavia, sono necessarie ulteriori condizioni, tra cui la capacità di bandire e assegnare le gare con modalità efficaci e tempestive, e la capacità di esecuzione dei progetti. Un tema particolarmente critico è quello delle competenze necessarie non solo per la governance e il monitoraggio del Piano ma anche per l'indirizzo delle scelte sui progetti da realizzare e sulla capacità di visione che li deve accompagnare.
Lo scenario prevede, a fronte di un mercato digitale pari a 75,4 miliardi di euro nel 2021, un impatto del PNRR di 3,3 miliardi per un totale complessivo di oltre 78,7 miliardi e un incremento del 10,1% rispetto al 5,5% che si registrerebbe al netto del PNRR.
I tassi di crescita previsti per il mercato digitale, inclusivi dell'impatto del PNRR secondo questo scenario, saranno pari al 10,6% nel 2022, al 6,1% nel 2023 e al 4,1% nel 2024 (Fig. 6).
Per quanto riguarda i settori, come già accennato, saranno in particolare Industria, Pubblica Amministrazione, Sanità e Telecomunicazioni che beneficeranno in modo diretto degli investimenti previsti dal Piano. Complessivamente nel periodo 2021-2024 all'Industria dovrebbero essere destinati finanziamenti per oltre 13 miliardi, alla PAC per oltre

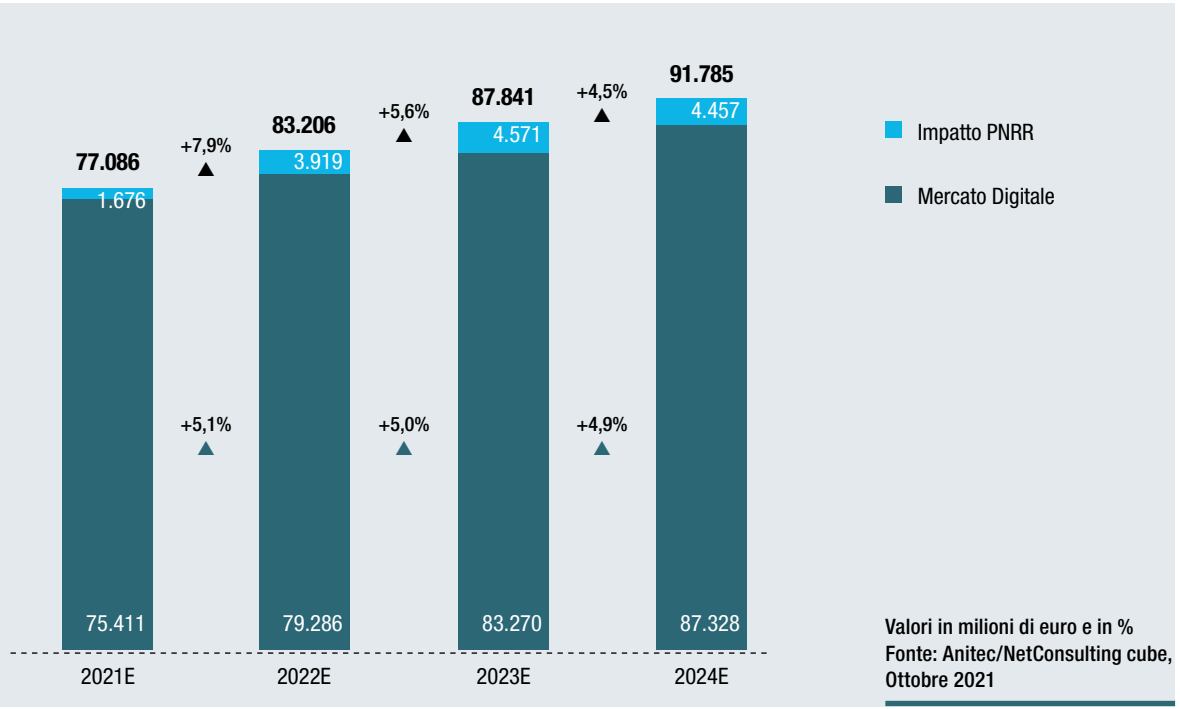
Figura 6:
L'impatto del PNRR sul mercato digitale secondo lo scenario 1 (ottimistico), 2021-2024E



Valori in milioni di euro e in %
Fonte: Anitec/NetConsulting cube, Ottobre 2021

4,7 miliardi, agli enti locali per 3,6 miliardi e alla Sanità per 2,9 miliardi. Le Telecomunicazioni dovrebbero beneficiarne per 3,8 miliardi di euro.
Tra gli ambiti più impattati dal PNRR, oltre ai sistemi abilitanti la Fabbrica 4.0 e la Supply Chain, anche l'ambito infrastrutturale, sia attraverso la sensorizzazione delle infrastrutture e delle reti, sia per la maggiore adozione di sistemi di monitoraggio, anche in logica predittiva, delle stesse. Tra le reti naturalmente si considerano anche quelle di telecomunicazioni di nuova generazione ultraveloci (Banda Larga e 5G).
A livello infrastrutturale, una componente che sicuramente trarrà beneficio dal PNRR è il Cloud Computing, considerato quanto previsto dalla Strategia Nazionale per il cloud.
Scenario 2: rappresenta la visione pessimistica legata a ipotetici ostacoli che potrebbero frenare i progetti previsti nel PNRR. Secondo questo scenario, alle previsioni descritte nei paragrafi precedenti si aggiungeranno le nuove risorse messe in campo dal PNRR, che incideranno per 20,5 miliardi di euro nel periodo 2021-2026 e per 14,6 miliardi nel periodo di analisi 2021-2024.
L'assunto principale alla base di tale scenario è relativo all'utilizzo dei fondi messi a disposizione dal PNRR solo per il 50%, ovvero considerando che non si riesca a rispettare il cronoprogramma delle riforme e degli investimenti e dunque non si possa accedere interamente ai fondi successivi. Inoltre, in questo scenario si ipotizza che vi siano degli ostacoli nell'arruolamento delle competenze e delle risorse per la messa in campo dei progetti previsti, per la loro esecuzione e per il monitoraggio e controllo. Questa serie di difficoltà allungherebbe le tempistiche delle riforme e degli investimenti da effettuare, generando un circolo vizioso rispetto allo sblocco delle successive tranche di finanziamento.
Lo scenario prevede, a fronte di un mercato digitale pari a 75,4 miliardi di euro nel 2021, un impatto del PNRR pari a 1,7 miliardi per un totale complessivo di 77 miliardi e un incremento, rispetto all'anno precedente che non ha visto il contributo del Piano, del 7,8%.
I tassi di crescita previsti per il mercato digitale, inclusivi dell'impatto del PNRR secondo questo scenario, saranno pari al 7,9% nel 2022, al 5,6% nel 2023 e al 4,5% nel 2024 (Fig. 7).

Figura 7:
L'impatto del PNRR sul mercato digitale secondo lo scenario 2 (pessimistico), 2021-2024E



Valori in milioni di euro e in %
Fonte: Anitec/NetConsulting cube, Ottobre 2021

CYBERSECURITY E TRANSIZIONE DIGITALE

Gli attacchi di Cybersecurity sono in continua crescita, sia in termini numerici sia per quanto riguarda i danni economici causati a soggetti pubblici e aziende private. Questa tendenza è influenzata dalla diffusione dello smart working e dall'accelerazione della transizione verso il cloud. Di fronte a questi attacchi informatici, le aziende hanno cominciato ad attrezzarsi per contrastarli, organizzandosi internamente e adottando particolari misure. Alla luce di tale situazione si prevede che la spesa complessiva destinata a prodotti e servizi in ambito Cybersecurity cresca del 12,4% nel 2021.
Si tratta di un aumento più elevato rispetto a quello stimato per il mercato digitale nel suo complesso.
Anche sul piano normativo e istituzionale si registrano innovazioni come la recente nascita dell'Agenzia per la Cybersicurezza Nazionale.

2020

1.871 ATTACCHI INFORMATICI NEL MONDO

+66%

2017

DANNI ECONOMICI NEL MONDO

1% PIL

2020 ▶ 945 mld$

I danni economici causati da Cybercrime nel 2020 sono stati pari a 945 miliardi di dollari: l'1% del PIL mondiale

smart working

Questo scenario è stato influenzato dalla diffusione dello smart working e dalla transizione verso il cloud

La rilevanza del tema

Cybersecurity

si riflette anche nella definizione di team e strutture organizzative dedicate: figura del Chief Information Security Officer

Security Operation Center

Fondamentale l'adozione di misure per l'erogazione di servizi di monitoraggio, gestione e difesa dai Cyber attacchi: ruolo del Security Operation Center

SPESA CYBERSECURITY

1.393 mln€

2021 **+12,4%**

Spesa complessiva destinata a prodotti e servizi in ambito Cybersecurity

Tasso di crescita medio annuo

2022 **13,1%**

2024
SPESA CYBERSECURITY

> 2mld €

ACN

Nascita dell'Agenzia per la Cybersicurezza Nazionale (ACN)

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

Nel corso del 2020 e del 2021 gli attacchi di Cybersecurity hanno continuato a crescere, non solo in termini numerici ma anche dal punto di vista dell'impatto su organizzazioni pubbliche e aziende. Gli attacchi informatici a livello globale hanno raggiunto il picco massimo nel 2020, con 1.871 attacchi gravi di dominio pubblico rilevati e un incremento pari al 12% rispetto all'anno precedente (Rapporto Clusit 2021).

Preoccupante anche il trend in aumento degli attacchi gravi: +66% rispetto al 2017.

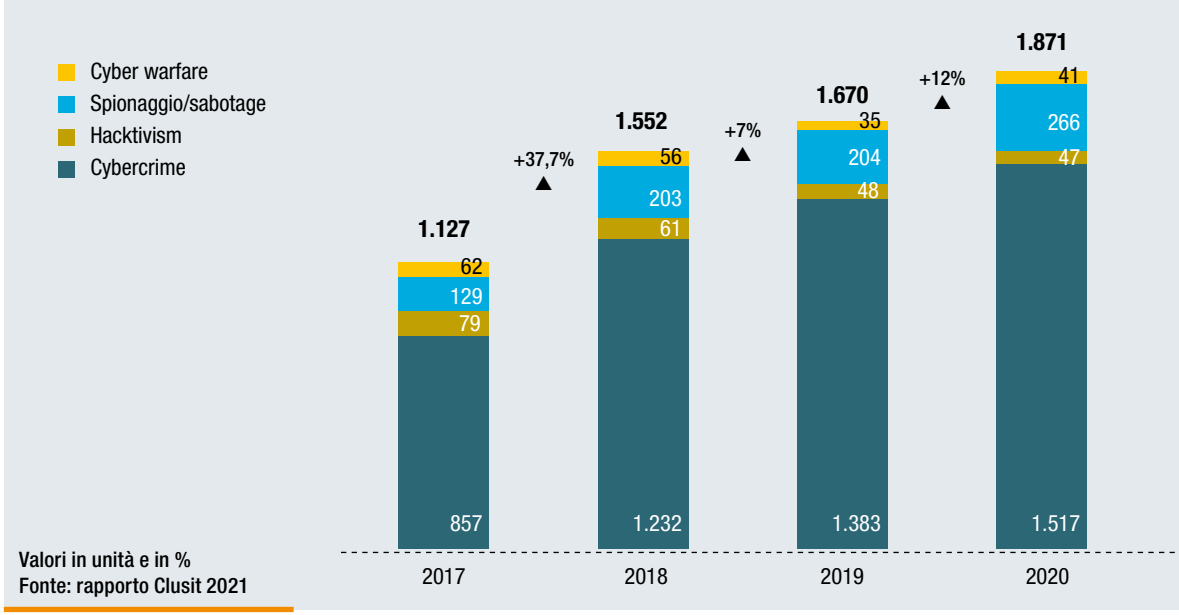
In termini assoluti, nel 2020 la categoria "Cybercrime" ha fatto registrare il numero di attacchi più elevato degli ultimi dieci anni, con una crescita del +77% rispetto al 2017 (1.517 contro 857) e del +9,7% rispetto al 2019. La categoria "Hacktivism" è l'unica a registrare un calo (-2,1%) rispetto al 2019, mentre in aumento sono stati gli attacchi gravi compiuti per finalità di "Cyber Espionage" (+30,4%) e quelli appartenenti alla categoria "Cyber Warfare" (+17,1%) (Fig. 1).

Il dato più rilevante riguarda i danni economici causati da Cybercrime, che nel 2020 sono stati pari a 945 miliardi di dollari: l'1% del PIL mondiale (Report McAfee Hidden Cost of Cybercrime). Questo valore non include il furto di proprietà intellettuale dovuto ad attività di Cyber intelligence economica, né i costi legati alle conseguenze delle operazioni relative a fake news e disinformazione, con finalità politiche interne e geopolitiche.

Secondo il Report del Viminale, il trend per il 2021 risulta in ulteriore peggioramento, con 4.938 attacchi dal 1° agosto 2020 al 31 luglio 2021, oltre dieci volte il numero rilevato per lo stesso periodo dell'anno precedente.

Questo scenario è stato influenzato dalla diffusione dello smart working, che si è affermato come "nuova normalità", e dall'accelerazione della transizione

Figura 1:
Andamento del numero dei Cyber attacchi per tipologia, 2017-2020



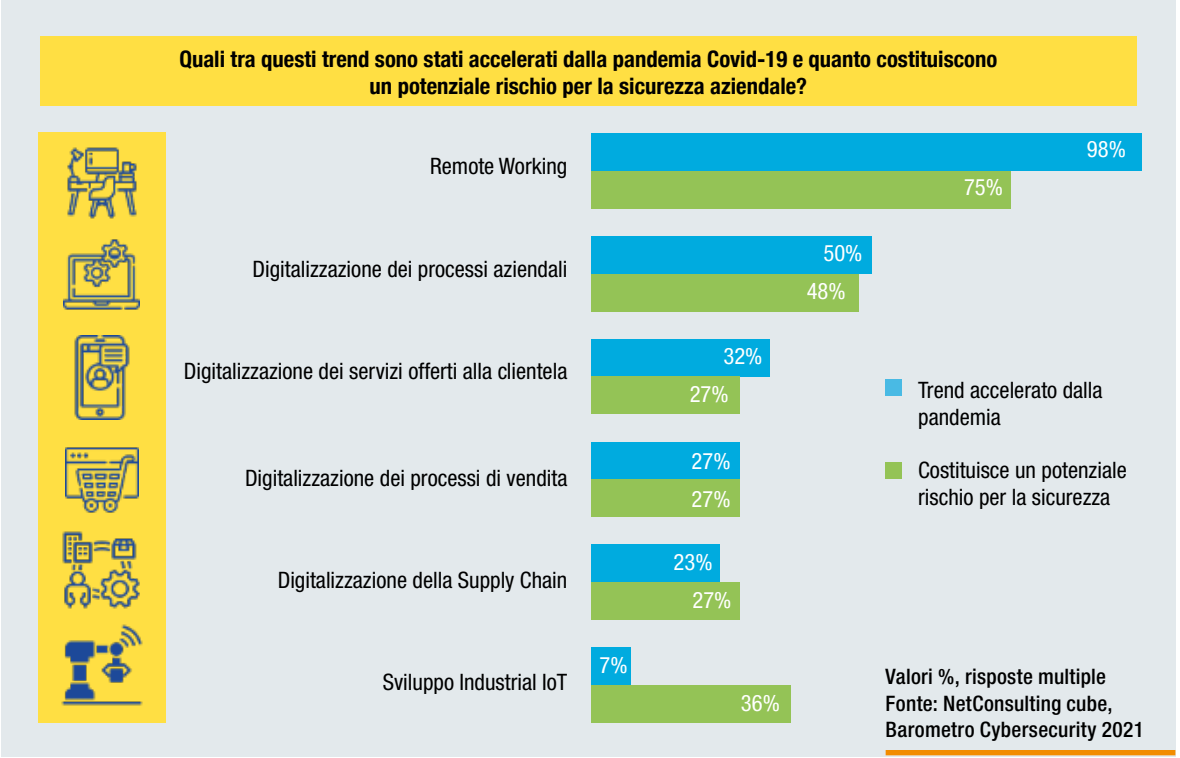
Valori in unità e in %
Fonte: rapporto Clusit 2021

verso il cloud, comportando l'estensione della superficie d'attacco ed esponendo le organizzazioni a minacce crescenti e sempre più sofisticate.
Il Threath Cybersecurity Landscape pubblicato ad ottobre 2021 da ENISA evidenzia 8 macro-categorie di attacchi maggiormente osservati nel corso dell'ultimo anno:

- Ransomware, che nel corso del 2021 hanno rappresentato la minaccia più diffusa e in maggior crescita, tanto che in tutta l'area EMEA (Europa, Medio Oriente e Africa), i Ransomware rappresentano la tipologia di attacco Cyber maggiormente in aumento (+422% tra febbraio 2020 e maggio 2021), e l'Italia risulta essere il quarto Paese europeo colpito da questa tipologia di attacchi, secondo la classifica stilata da Mandian. I Ransomware si indirizzano sia ad organizzazioni pubbliche che private, facendo insorgere anche casi di rilevante risonanza mediatica (tra gli ultimi, il caso della Regione Lazio). I settori maggiormente colpiti sono il manifatturiero, che si conferma al primo posto, seguito da servizi legali e professionali, retail e industria ingegneristica.
- Malware, software o firmware malevoli che penetrano nei sistemi attaccati, con lo scopo di rubare dati o comprometterne l'integrità, o anche la disponibilità di un sistema. Sono stati fino ad oggi gli attacchi più diffusi, ma hanno registrato un calo nel 2021, probabilmente per il crescente successo di nuove tecniche di contrasto.
- Cryptojacking, finalizzato a sfruttare la capacità elaborativa dei sistemi della vittima per cryptomining. Si tratta di una modalità di attacco in crescita nell'ultimo anno per effetto della diffusione delle criptovalute.
- Minacce veicolate tramite e-mail, che includono phishing e altre tipologie che puntano soprattutto a sfruttare le vulnerabilità degli utenti e che, nonostante la crescente diffusione di programmi di awareness, continuano a rappresentare una minaccia.
- Data Breach e Data Leaks, ovvero il furto di dati confidenziali o sensibili, che in genere possono essere non solo oggetto di un attacco da parte di un soggetto esterno ma anche da parte di dipendenti. Anche questa minaccia continua ad essere nelle top 10, con finalità di estorsione, diffamazione o altro tipo di danno indirizzato ad un'organizzazione.
- Minacce contro la disponibilità e l'integrità di sistemi, come ad esempio gli attacchi di Denial of Service (DoS) e a siti web. Questa minaccia rimane ancora molto elevata nello scenario complessivo, sia per essere stata oggetto di attacchi recenti, sia per l'impatto elevato che può avere soprattutto quando indirizzata a sistemi industriali di produzione, compromettendo la continuità dell'attività.
- Disinformazione o diffusione di informazioni false con lo scopo di danneggiare un brand o un'azienda, spesso usate negli attacchi ibridi per indebolire ulteriormente l'organizzazione o i suoi rappresentanti.
- Attacchi non malevoli / non intenzionali, che sono generalmente basati su errori umani o configurazioni errate di software e programmi informatici.

Figura 2:

Pandemia Covid-19: accelerazione della trasformazione digitale e incremento dei rischi per la sicurezza



Impatto della trasformazione digitale sul fronte Cybersecurity: Smart working, Cloud, IoT

Il processo di trasformazione digitale, in crescita nella maggior parte delle organizzazioni italiane e tra i punti fondanti il PNRR per lo sviluppo del "sistema Paese", è intrinsecamente legato ad un incremento delle vulnerabilità derivanti principalmente dall'estensione del tradizionale "perimetro fisico" di aziende ed enti.

Come evidenziato dal Barometro Cybersecurity, una ricerca condotta annualmente da NetConsulting cube, nell'ultimo biennio la pandemia Covid-19 ha fortemente accelerato alcuni trend relativi alla digitalizzazione, a partire dall'introduzione del Remote Working (in crescita presso il 98% delle organizzazioni intervistate), alla digitalizzazione dei processi aziendali e dei servizi offerti a clienti e utenti (50%), dei processi di vendita e delle supply chain di riferimento (23%).

Particolarmente alta, anche se nel corso del 2020 questo ambito non ha avuto un'accelerazione, l'attenzione verso le criticità relative ai sistemi di Industrial IoT per le aziende che ne fanno utilizzo (36%), dato che tradizionalmente sono ambienti caratterizzati da una minore diffusione della cultura della sicurezza e in cui spesso sono adottati sistemi obsoleti, maggiormente esposti alle vulnerabilità (Fig 2).

In tutti i casi si registra anche un potenziale incremento dei rischi per la sicurezza informatica a causa del fenomeno di dissoluzione dei tradizionali confini organizzativi.

Politiche di Remote e Smart Working sono state accelerate dal processo di digitalizzazione legato alle contingenze pandemiche, dove in ottica di continuità operativa una larga porzione della forza lavoro ha potuto svolgere la propria attività lavorativa tramite l'utilizzo di dispositivi informatici, fissi e mobili, e software erogati in modalità as a service. I rischi per la sicurezza informatica e la protezione dei dati, relativi a modalità di lavoro agile, ormai parte integrante di nuovi modelli lavorativi post pandemia,

sono molteplici e includono:

- l'utilizzo di reti non sicure;
- l'impiego di dispositivi aziendali e di soluzioni informatiche non approvati dalla propria organizzazione (Shadow IT) e quindi non in linea con le disposizioni aziendali in materia di sicurezza;
- la condivisione di dati e documenti con soggetti non autorizzati.

In questo scenario, criticità elevate sono infatti connesse allo sfruttamento delle vulnerabilità da parte dei Cyber attaccanti nei confronti del comportamento umano, tramite phishing e social engineering sempre più sofisticati, non sempre supportati da un'adeguata protezione in termini di procedure e tecnologie di sicurezza al di fuori del perimetro della propria organizzazione.

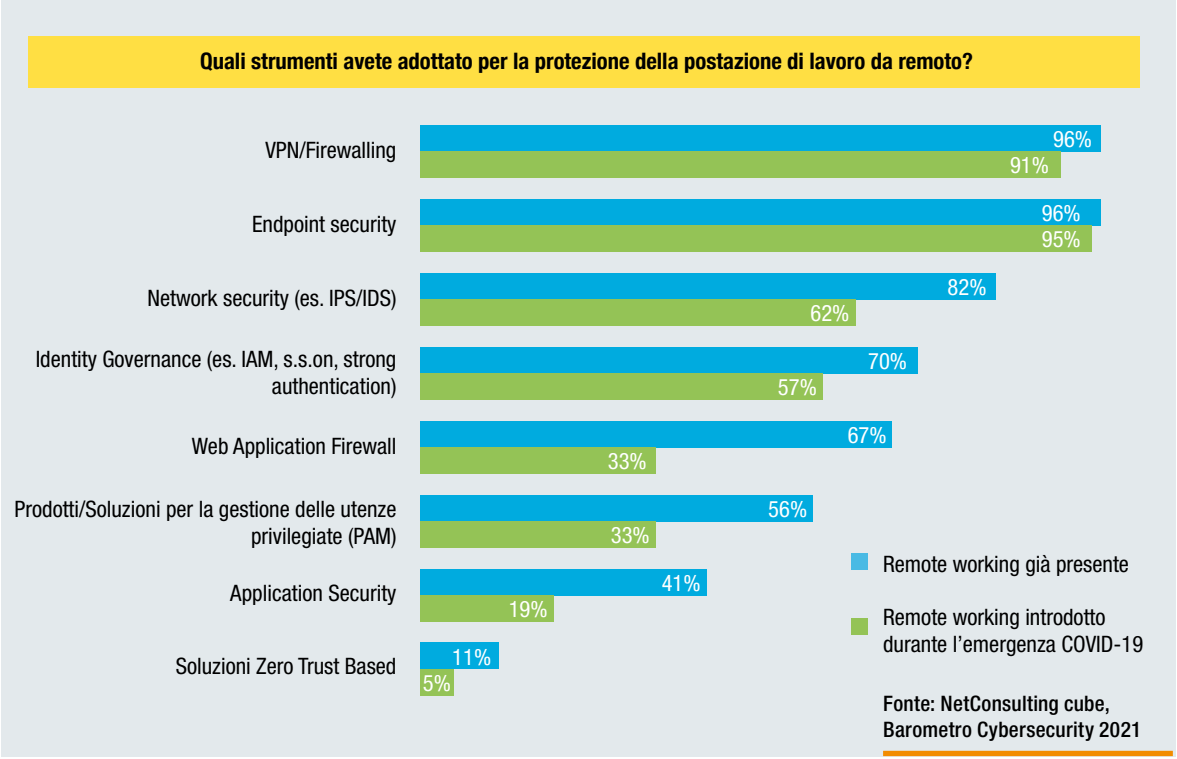
Tra i principali strumenti adottati dalle aziende italiane per la messa in protezione del lavoro da remoto, in primo luogo l'utilizzo di VPN (con frequenze di citazione oscillanti tra il 96% e il 91% a seconda che il Remote Working fosse o meno già in uso prima dell'emergenza sanitaria), l'impiego di soluzioni di Endpoint Security (diffusi presso circa il 95% del panel) e di Network Security (IPS/IDS) (Fig. 3).

Meno diffusa è l'adozione di soluzioni di Identity Governance, pari al 70% per le organizzazioni che avevano già in essere politiche di lavoro agile, mentre tra quelle che sono migrate alla nuova modalità di lavoro per effetto dell'emergenza Covid-19 solo il 57% ha introdotto strumenti di gestione di identità e accesso. Per queste ultime, inoltre, risultano carenti l'Application Security e la gestione delle utenze privilegiate ai sistemi e ai dati critici aziendali, adottate solo da un terzo del campione.

Decisamente ancora agli inizi è l'introduzione di soluzioni/piattaforme basate su framework Zero Trust ("sicurezza senza perimetro") e fondate su di un rigido processo di verifica delle identità. Oltre all'introduzione di soluzioni tecnologiche specifiche, l'erogazione di corsi di formazione specifici per la sicurezza informatica si rivela fondamentale per la riduzione delle vulnerabilità legate a comportamenti umani errati.

Le criticità per la sicurezza sono numerose anche in merito al diffondersi dell'utilizzo del Cloud Computing (SaaS, IaaS, PaaS), sempre più attrattivo per

Figura 3:
Principali strumenti per la sicurezza del lavoro da remoto

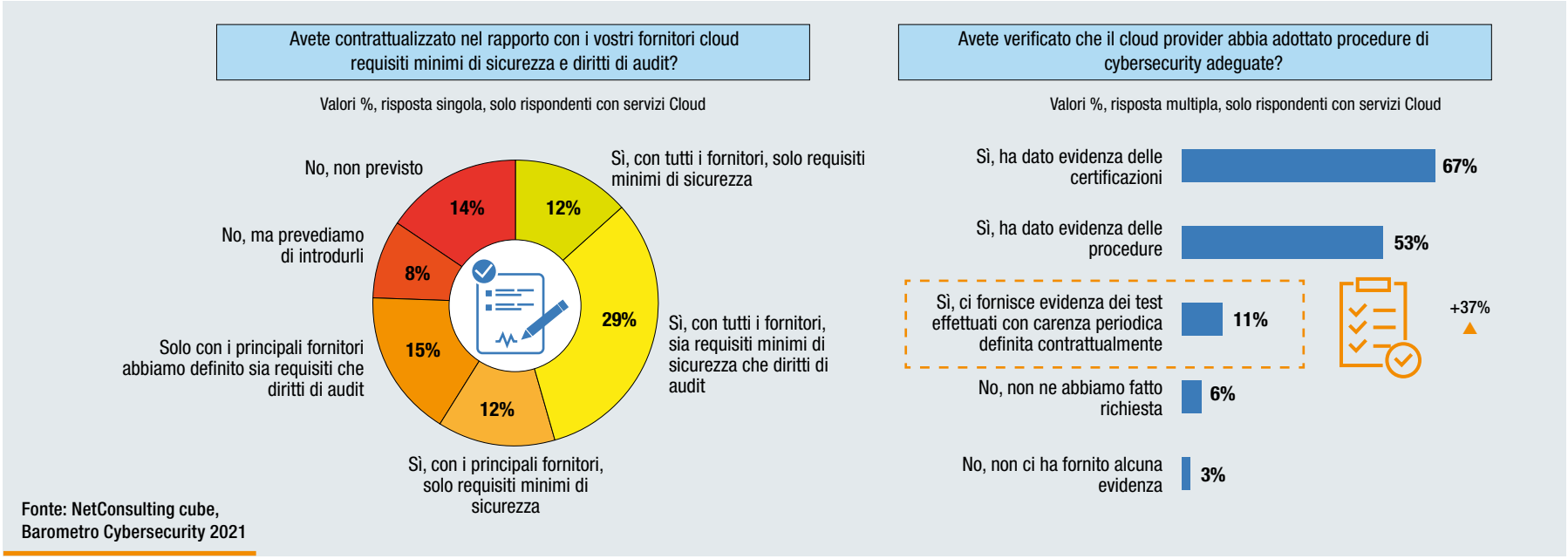


gli attaccanti Cyber, sia per attività di spionaggio industriale e crimini finanziari, sia per attacchi sponsorizzati da Stati nazionali per eventuali applicazioni mission-critical erogate in cloud.
Se da un lato i fornitori di servizi cloud sono tenuti a garantire la sicurezza della propria infrastruttura e i controlli di sicurezza, al cliente che ne usufruisce rimane la responsabilità della loro applicazione a protezione dei propri dati, definendo modelli a responsabilità condivisa in cui i possibili punti di debolezza possono essere sfruttati per portare a termine attacchi informatici con successo.
Tra le principali categorie di rischi collegati all'utilizzo di soluzioni as a service, si possono includere:

- Rischi organizzativi: in particolare legati alla governance con il Cloud Service Provider e nell'attribuzione delle responsabilità tra cliente e fornitore, a un possibile lock-in (su dati, a livello contrattuale, o di informazione), oppure a dinamiche di concentrazione del mercato, in caso di sub-esternalizzazione dei servizi, per la sicurezza della supply chain.
- Rischi tecnologici: compromissione di dati e informazioni presso il Cloud Service Provider (data breach), che possono derivare da un attacco informatico rivolto al fornitore stesso o dalla compromissione nell'operatività del fornitore di servizi cloud, con ricadute sulle attività del cliente.
- Rischi legali: vincoli normativi diversi relativi alla

Figura 4:

Cloud Security: contrattualizzazione dei requisiti minimi e verifica delle procedure di Cybersecurity



Fonte: NetConsulting cube, Barometro Cybersecurity 2021

localizzazione geografica del Cloud Service Provider (ad esempio, cambio di giurisdizione, protezione dei dati e gestione delle licenze).

Le misure adottate dalle organizzazioni per una maggiore protezione da queste categorie di rischio sono a loro volta numerose, e vanno dall'utilizzo di modelli multi-cloud per ridurre la dipendenza da un singolo fornitore, alla definizione di Exit Strategy, alla verifica del possesso e mantenimento di adeguate misure e certificazioni di sicurezza da parte del fornitore.

Le organizzazioni che hanno partecipato alla rilevazione del Barometro Cybersecurity mostrano ad esempio una buona attenzione nella contrattualizzazione di almeno uno tra i requisiti minimi di sicurezza e diritti di audit nel 78% dei casi, di entrambi i requisiti per quasi un terzo dei rispondenti, mentre un ulteriore complessivo 27% ha previsto la contrattualizzazione di uno dei due requisiti con riferimento ad almeno i principali Cloud Provider di riferimento. Inoltre, gli stessi fornitori si sono strutturati per garantire i propri clienti fornendo loro evidenza delle proprie certificazioni di sicurezza (67% dei casi), delle procedure (nel 53%) e, con una frequenza minore ma in crescita rispetto alle precedenti rilevazioni (11%), anche dei test di sicurezza effettuati, definiti contrattualmente (Fig. 4).

Le organizzazioni clienti possono inoltre dotarsi di soluzioni tecnologiche per la protezione degli ambienti cloud, come l'impiego di Cloud Security Access Broker (CASB), per monitorare le attività degli utenti in ambienti multi-cloud, di soluzioni di Data Loss Prevention, per la classificazione e protezione dei dati, anche con l'ausilio di tecniche di cifratura con chiavi a disposizione del cliente, di soluzioni per la migrazione sicura tra ambienti differenti.

Lo stato dell'arte nelle aziende e le principali misure adottate

Lo scenario descritto nel precedente paragrafo evidenzia la presenza di un processo di digitalizzazione diffuso presso aziende ed enti italiani. L'espansione del perimetro aziendale, in congiunzione con l'incremento degli attacchi informatici perpetrati da Cyber criminali, evidenziano sempre più come la Cybersecurity rappresenti una priorità strategica, frequentemente inserita come punto chiave all'interno di piani di sviluppo pluriennali, non solo per chi detiene infrastrutture critiche.

PRESENZA DI TEAM DEDICATI/DIREZIONE CON FOCUS SU CYBERSECURITY

La rilevanza del tema Cybersecurity si riflette anche nella definizione di team e strutture organizzative dedicate, pur con notevoli differenze legate alla dimensione e al settore di appartenenza di aziende ed enti, come rilevato dalle analisi di NetConsulting cube.

Il modello organizzativo prevede la presenza di una figura responsabile per la sicurezza informatica (Chief Information Security Officer, o ruoli assimilabili, nel 48% dei casi), all'interno del dipartimento IT, trasversalmente a tutti i comparti settoriali. Per quelle organizzazioni che costituiscono infrastrutture criti-

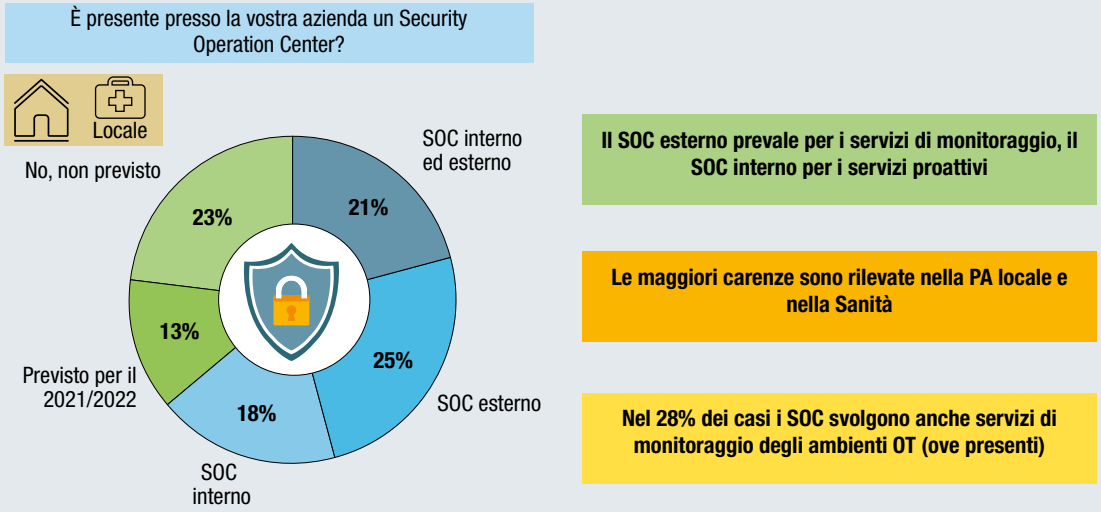
Figura 5:

Organizzazione adottata per la governance e la gestione della Cybersecurity

che, in particolare Energy-Utility, Telecomunicazioni, Banche e servizi finanziari, la sicurezza informatica è di competenza di un responsabile di sicurezza di gruppo, generalmente fisica e logica (Chief Security Officer, CSO, 30%) (Fig. 5). Solo nel 7% dei casi, per strutture organizzative di grandi dimensioni, si rileva la presenza contemporanea in azienda di CISO e CSO per la governance della Cybersecurity.
Tuttavia, in molte organizzazioni la gestione delle attività di Cybersicurezza è demandata a risorse all'interno del dipartimento IT, senza una figura responsabile dedicata. In questi casi, profili tecnici come CTO, Responsabile Infrastrutture o Networking sono anche deputati alla governance della Cybersecurity, in particolare nei settori GDO-Retail, media Industria, Pubblica Amministrazione locale e Sanità pubblica. I recenti attacchi informatici, che hanno coinvolto nello specifico il settore pubblico e sanitario, sottolineano la necessità di un maggiore livello di maturità organizzativa, con figure dirigenziali dedicate per coordinare e gestire le attività Cyber.
Trattandosi inoltre di competenze verticali specialistiche, una percentuale minoritaria di organizzazioni, tra cui un'ulteriore porzione di aziende della media Industria, e del macro comparto Servizi-Trasporti, ha scelto di esternalizzare la maggior parte delle attività di Cybersecurity.

Figura 6:

Presenza di un Security Operation Center (SOC) e sue principali funzioni



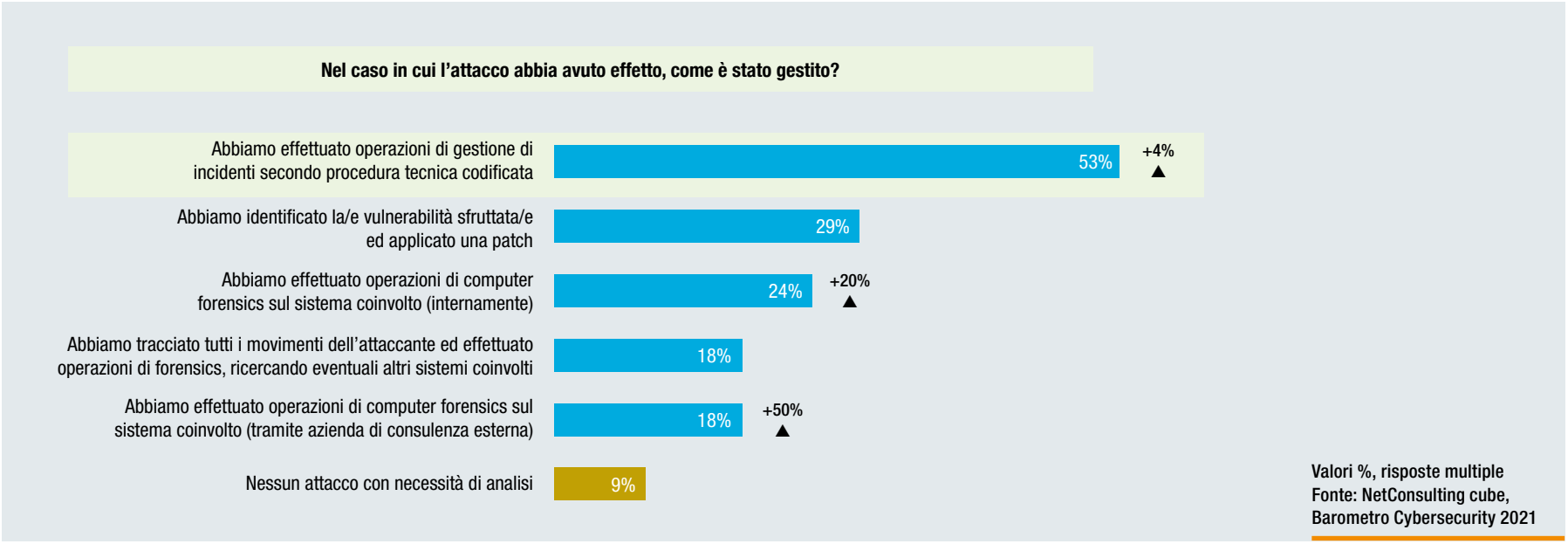
Valori %
Fonte: NetConsulting cube, Barometro Cybersecurity 2021

ADOZIONE DI MISURE DI DETECTION AND RESPONSE

Oltre ad un'organizzazione dedicata per la gestione della Cybersecurity, fondamentale per la protezione aziendale è l'adozione di misure, in termini di governance e tecnologie, per un'individuazione e una risposta efficace agli attacchi informatici. Tra queste, la presenza di un Security Operation Center (SOC) garantisce l'erogazione di servizi di monitoraggio, gestione e difesa dai Cyber attacchi.
Il ricorso ai servizi di un SOC è presente nel 64% del panel, con un ulteriore 13% che ne prevede l'introduzione entro il 2022. I SOC esterni all'organizzazione (25%), gestiti da fornitori terzi, erogano principalmente servizi di monitoraggio (Log Management, Security Monitoring & Alerting, Security Incident Management), mentre i SOC interni, diffusi in particolare presso chi gestisce infrastrutture critiche, svolgono con maggiore frequenza servizi di tipo proattivo, maggiormente vicini alla sfera operativa di CERT e CSIRT, con l'inclusione di attività di Threat Intelligen-

ce per la prevenzione degli attacchi, così come di assistenza nelle procedure di Response e Recovery. Il restante 23%, che non si doterà di un Security Operation Center neanche nel breve termine, include organizzazioni ed enti della Pubblica Amministrazione e della Sanità, evidenziando nuovamente un gap da colmare nella protezione di dati critici (Fig. 6).
Dal momento che nessuna organizzazione può dirsi realmente al sicuro, anche la pianificazione della risposta agli attacchi informatici deve rappresentare una pratica consolidata e matura per una corretta remediation. In caso d'incidente, il 53% del panel utilizza una procedura tecnica codificata di gestione, che quindi deriva da framework e standard internazionali (NIS e ISO27001 in primis). In altri casi l'attività si limita all'identificazione della vulnerabilità e all'applicazione di una patch, come fase di riconoscimento dell'attacco.
Crescono però anche le attività di forensics sui sistemi coinvolti, svolte internamente (24%) o tramite il ricorso a fornitori esterni (18%), mentre meno diffusa è l'estensione di queste attività anche per l'individuazione dell'eventuale coinvolgimento di altri sistemi (Fig. 7).
L'abilità di aziende ed enti di rilevare possibili attacchi alla sicurezza può essere ulteriormente rafforzata attraverso l'adozione di soluzioni di Cybersecurity basate su algoritmi di Machine Learning e di tool di Endpoint Detection & Response.
Se le piattaforme di endpoint protection e firewall consentono di bloccare gli attacchi già noti, nel

Figura 7:
Procedure adottate nella gestione degli attacchi informatici

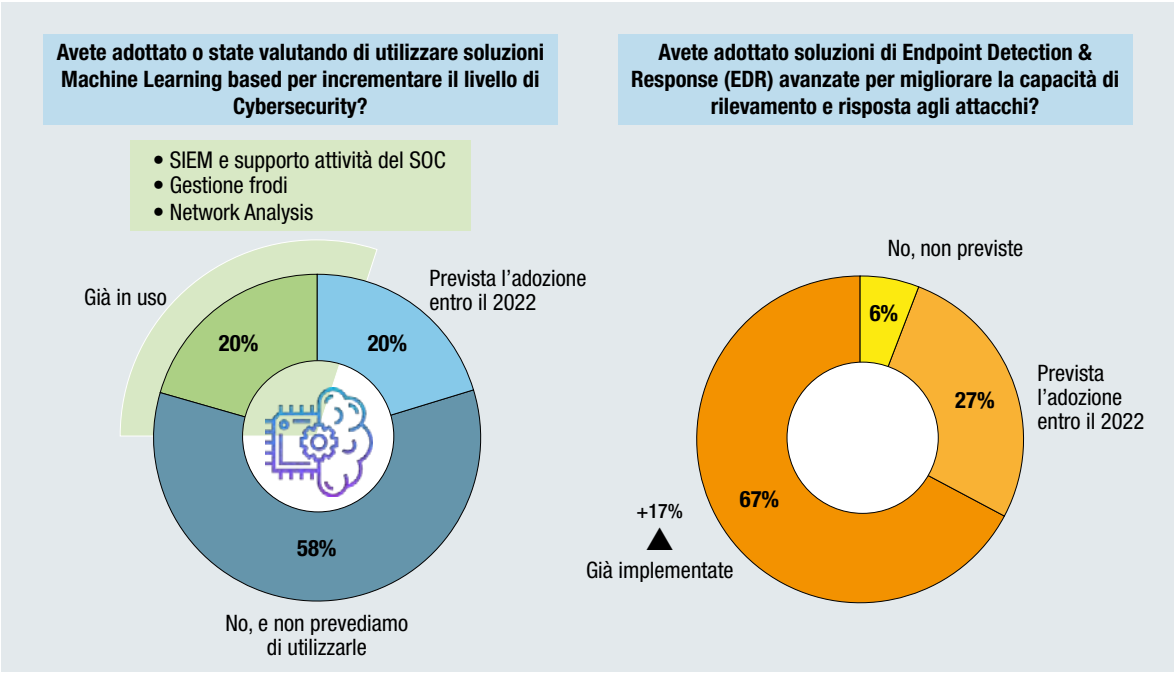


Valori %, risposte multiple
Fonte: NetConsulting cube, Barometro Cybersecurity 2021

caso invece di attacchi avanzati le soluzioni di IA possono contribuire all'individuazione di anomalie che fanno sospettare un attacco e consentono di essere tempestivi in fase di rilevamento, così come nella minimizzazione dei falsi positivi.
La diffusione di soluzioni di Cybersecurity basate su Machine Learning è ancora ridotta al 20% del panel di rilevazione, con algoritmi integrati in soluzioni di SIEM avanzati e nel supporto alle attività del SOC, nella gestione delle frodi informatiche e nell'analisi per il monitoraggio del network, mentre un ulteriore 20% ne prevede l'adozione entro il 2022 (Fig. 8).
L'Endpoint Detection and Response raggruppa gli strumenti avanzati che hanno il compito di rilevare minacce su dispositivi ed eseguire attività di indagine e risposta, con la possibilità di estensione anche ai sistemi critici.
Gli strumenti di EDR avanzati, anche a causa della remotizzazione del lavoro, risultano implementati dal 67% delle organizzazioni e saranno utilizzati nel prossimo futuro dal 27% del panel.
L'utilizzo di strumenti avanzati di sicurezza è comunque subordinato alla necessità di disporre di adeguate competenze e risorse, interne o esterne, in grado di gestire adeguatamente gli strumenti implementati.

Figura 8:

Adozione di strumenti avanzati di analisi: Machine Learning ed Endpoint Detection and Response



Valori %
Fonte: NetConsulting cube, Barometro Cybersecurity 2021

Il trend del mercato Cybersecurity 2020-2024

Il mercato Cybersecurity è previsto in continua crescita nei prossimi anni, per effetto della diffusione della digitalizzazione che richiederà una maggiore adozione da parte delle aziende di strumenti e servizi per prevenire le minacce Cyber e individuare possibili vulnerabilità.
La spesa complessiva destinata a prodotti e servizi in ambito Cybersecurity si prevede che giunga a 1.393 milioni di euro a fine 2021, con una crescita del 12,4%, più elevata rispetto a quella stimata per il mercato digitale nel suo complesso.
Anche nel prossimo triennio si attende una dinamica in aumento, con un tasso di crescita medio annuo del 13,1% e una spesa che supererà i 2 miliardi di euro nel 2024 (Fig. 9).
Le dinamiche previste sono positive per tutti i segmenti:

- Managed Security Services, in cui rientrano anche i servizi di Cloud Security, che rappresenta il segmento più consistente e con la crescita maggiore (TCMA del 15,4%). Il trend previsto è sostenuto dalla crescita della Cloud Security e dall'esigenza delle aziende di ricorrere a servizi di

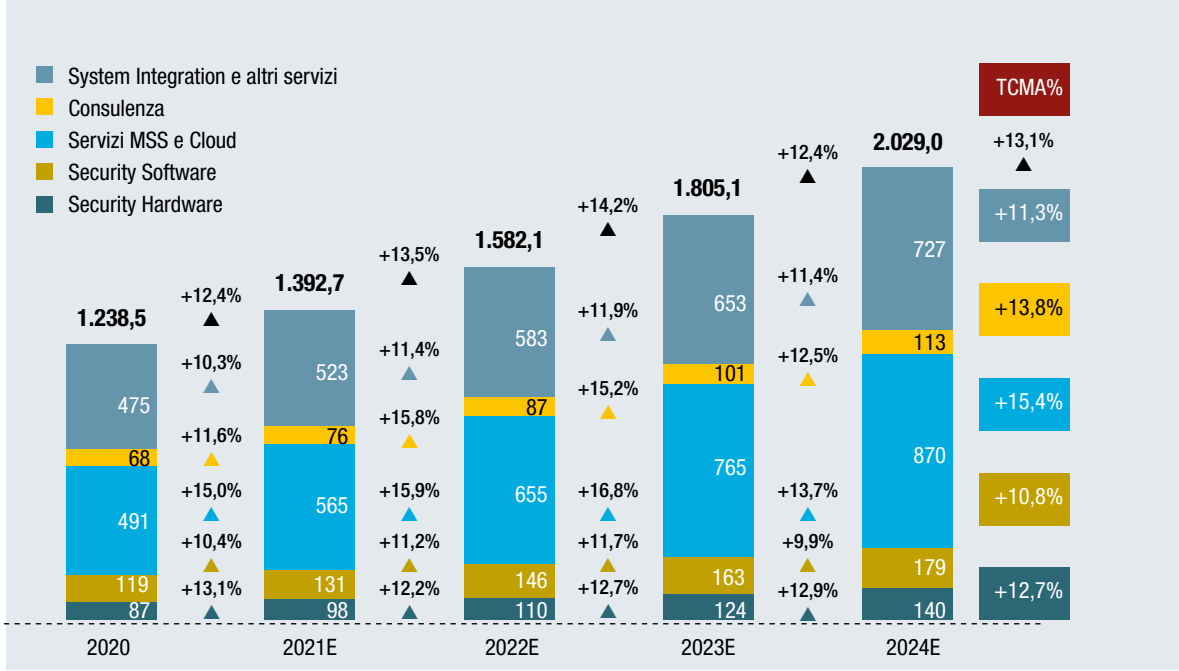


Figura 9:
Il mercato della Cybersecurity in Italia, 2020-2024E

Valori in milioni di euro e in %
Fonte: Anitec/NetConsulting cube, Ottobre 2021

SOC esterno 24X7, diffusa in tutti i settori, e dalla crescita del perimetro aziendale da monitorare.
In particolare, si prevede una crescente estensione dei servizi di SOC anche agli ambienti industriali (OT e Industrial IoT) in cui proseguirà la crescita degli apparati connessi, che vanno adeguatamente protetti e monitorati.

- System Integration e altri servizi, che rappresenta il segmento più importante dopo i Managed e Security Services, con una dimensione prevista a fine 2024 di 727 milioni di euro e un tasso di crescita medio annuo pari all'11,3%. Tra le componenti su cui si prevede una forte crescita vanno evidenziati lo sviluppo sicuro del software, in ottica security by design, e la formazione, su cui le aziende si stanno focalizzando per colmare il gap di conoscenza sul fronte dei rischi attinenti la sicurezza informatica, considerata l'elevata vulnerabilità rappresentata dal fattore umano.
- Consulenza, in cui si rileva il crescente ricorso a servizi di Risk e Vulnerability Assessment, Penetration Test, finalizzati ad avere un quadro aggiornato delle vulnerabilità e del livello di esposizione alle minacce. Cresce anche la consulenza strategica e organizzativa e quella mirata a risolvere situazioni di criticità conseguenti ad attacchi in continua crescita.
- Hardware, per cui la domanda è trainata principalmente dalla crescente diffusione del remote working e dal conseguente rafforzamento della sicurezza di rete, a partire dalle VPN che sono state oggetto di investimenti nel biennio 2020 e 2021, e dalla crescente adozione di appliance dedicate all'implementazione di software.
- Soluzioni software, con un trend positivo determinato sia dal rafforzamento delle soluzioni di endpoint security che dalla gestione delle Identità e accessi, che sempre più saranno orientate all'adozione del modello ZeroTrust per gestire la maggiore mobilità e ubiquità dei membri dell'organizzazione.

La crescita del mercato riceverà inoltre una forte spinta dal PNRR e dall'esigenza di colmare il gap in questo ambito accumulato dalla Pubblica Amministrazione e dalla Sanità, due dei settori maggiormente esposti alle minacce per effetto della digitalizzazione.
Dall'analisi della missione 1 destinata alla PA, emerge infatti una focalizzazione di investimenti sulla Cybersecurity. L'investimento è volto alla creazione ed al rafforzamento delle infrastrutture relative alla protezione cibernetica del Paese a partire dall'attuazione della disciplina prevista dal Perimetro di sicurezza nazionale cibernetica (PSNC).
L'intervento si articola in 4 aree principali, per un valore complessivo di 623 milioni di euro in sovvenzione:

- rafforzamento dei presidi di front-line per la gestione degli alert e degli eventi a rischio verso la PA e le imprese di interesse nazionale (rientranti nel PSNC);
- consolidamento delle capacità tecniche di valutazione e audit della sicurezza dell'hardware e del software;
- potenziamento del personale delle forze di polizia dedicate alla prevenzione e investigazione del crimine informatico;
- implementazione degli asset e delle unità incaricate della protezione della sicurezza nazionale.

È in questo scenario che rientrano le recenti gare indette da Consip tra luglio e settembre 2021 per un valore di 585 milioni di euro, che metteranno a disposizione delle PA servizi per la gestione della sicurezza informatica e la protezione dei dati:

- la prima gara bandita lo scorso luglio riguardava i "Servizi di sicurezza on premises: strumenti di gestione, protezione email, web e dati";
- la seconda i "Servizi di sicurezza da remoto, di compliance e controllo", pubblicata nel mese di ottobre, ha per oggetto la fornitura di servizi di protezione della sicurezza dei perimetri tecnologici nonché di servizi volti alla misura dello stato di salute della sicurezza dei sistemi informativi e di supporto nell'identificazione dei "fabbisogni" in ambito servizi e forniture di sicurezza ovvero servizi di compliance e controllo (Security Strategy, Vulnerability Assessment, Testing del codice, Supporto all'analisi e gestione degli incidenti, Penetration Testing, Compliance normativa).

La Cybersecurity nell'Industria 4.0

IOT E INDUSTRIAL IOT

La protezione di dispositivi e ambienti IoT, IIoT (Industrial IoT) e OT (Operational Technology) è un tema che ad oggi presenta particolari criticità in settori che spaziano dall'Industria all'Energy-Utility, dai Trasporti alla Logistica. In questi ambiti, infatti, prosegue la crescita di impianti di produzione e sistemi connessi, sensoristica e dispositivi, ma nello stesso tempo si rileva l'obsolescenza di tecnologie

di controllo e monitoraggio dei sistemi produttivi, come ICS, SCADA e PLC. La sicurezza relativa a questi dispositivi e apparati è di tipo cyber-fisico, dal momento che una possibile loro compromissione legata ad un attacco informatico può comportare rischi rilevanti anche per la sicurezza di lavoratori e utenti finali, qualora l'attacco sia indirizzato a uno stabilimento industriale, così come per la salute dei pazienti in ambito sanitario, in caso di attacchi mirati ad apparecchi elettromedicali o a sistemi di telemedicina.
Con riferimento al settore industriale e all'affermarsi del modello Industria 4.0, che prevede l'adozione di sistemi di produzione connessi, le nuove sfide che le organizzazioni si trovano a dover affrontare relativamente alla sicurezza di ambienti OT e IoT sono sia tecnologiche che organizzative, come evidenziato anche dalle rilevazioni del Barometro Cybersecurity. Nel novero delle criticità tecnologiche, l'aggiornamento delle componenti di sicurezza dei dispositivi connessi (82%) rappresenta una delle principali criticità per l'IoT e l'OT Security, legate nel primo caso alla memoria limitata di dispostivi e sensori, e nel secondo all'utilizzo di sistemi spesso obsoleti. Un'ulteriore difficoltà, data anche la proliferazione dei dispositivi connessi, è dettata dalla possibilità di avere piena visibilità e mappatura di tutti gli asset connessi a livello di rete (79%), rendendo difficile proteggere "ciò che non si vede" (Fig. 10).
A questi elementi si associano anche le criticità negli aggiornamenti dei controlli di sicurezza e nell'identificazione del traffico sospetto (50%), che può essere supportata dal tracciamento dell'accesso ai dati di sicurezza (18%), così come la mancanza di sistemi centralizzati per il monitoraggio e il controllo di dispositivi e apparati connessi (29%). Critica è anche la ricerca di attacchi zero-day (25%), vulnerabilità nascoste nei sistemi IoT di cui nemmeno i produttori possono essere a conoscenza.

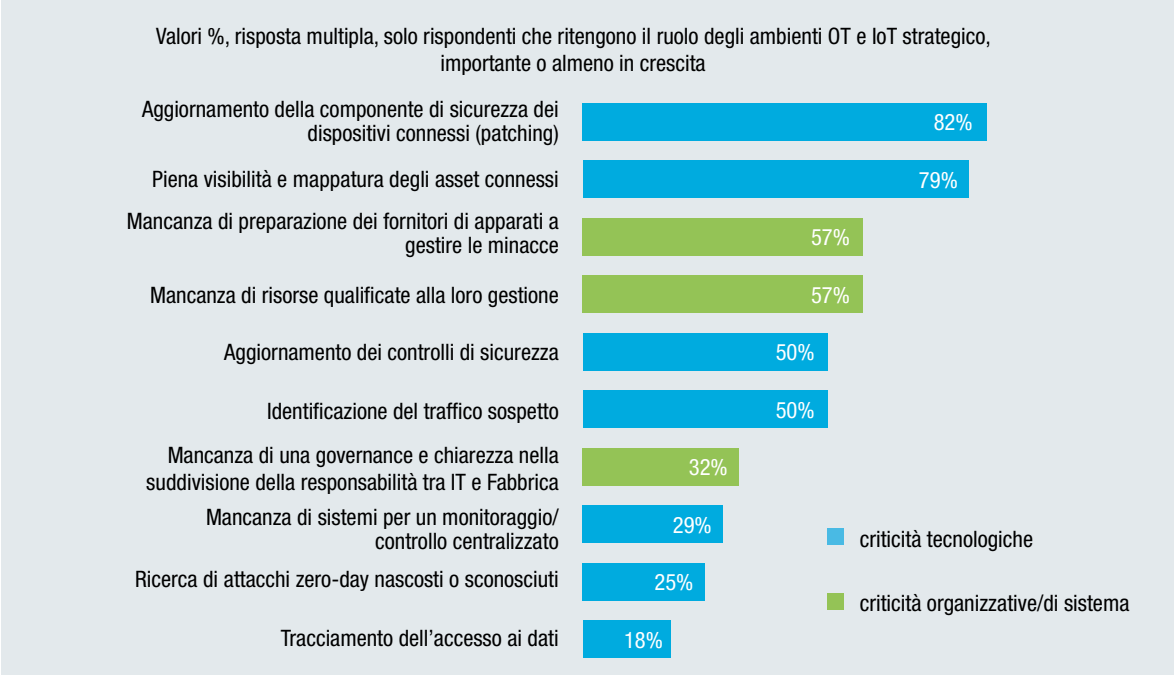


Figura 10:
Sfide tecnologiche e organizzative nell'ambito dell'IoT/OT Security

Fonte: NetConsulting cube, Barometro Cybersecurity 2021

Dal punto di vista organizzativo, la mancanza di preparazione a gestire l'evoluzione delle minacce di sicurezza da parte degli stessi fornitori di apparati, così come la mancanza di risorse qualificate alla gestione della sicurezza OT e IoT, possono costituire ulteriori elementi di vulnerabilità, evidenziando anche la necessità di upskilling/reskilling delle figure competenti in quest'ambito. Sempre più rilevante è anche la governance nella gestione di impianti e apparati connessi tra le funzioni IT e Produzione od Operations (33%), pur rimanendo il principio della segregazione delle reti: eventuali lacune possono essere sfruttate per attacchi informatici con ricadute sull'operatività.

IL TREND DEGLI ATTACCHI IN AMBITO IOT

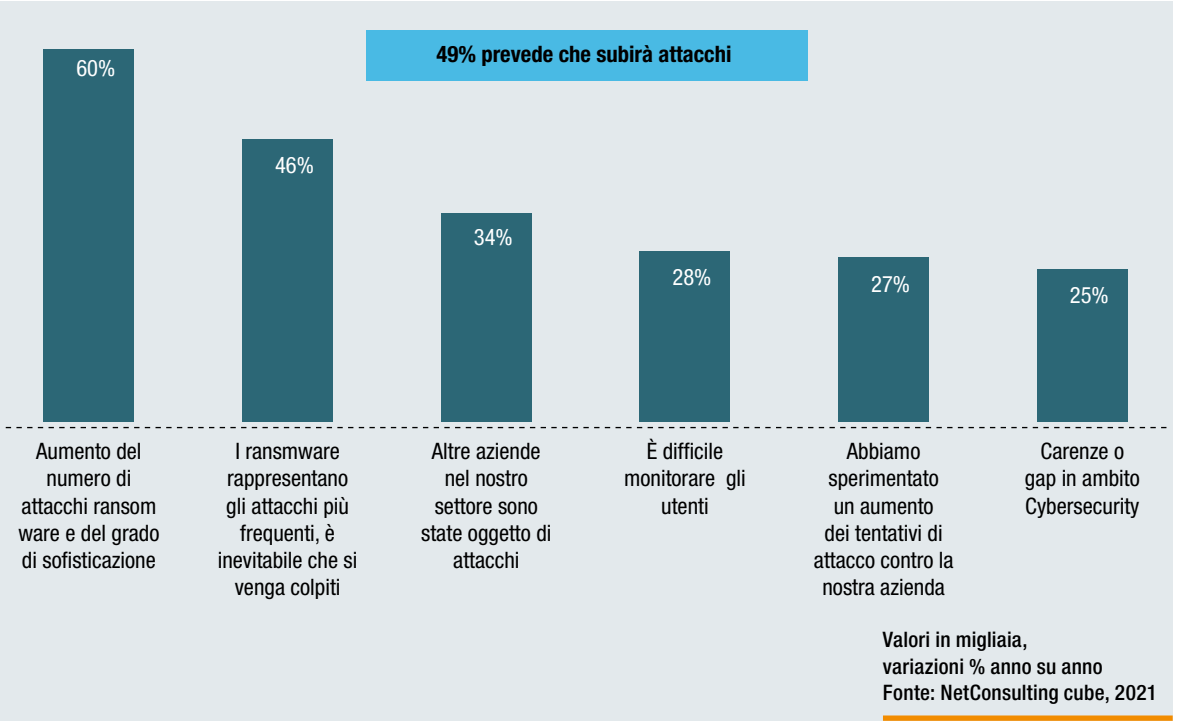
La crescente convergenza tra sistemi IT e Operations, conseguente all'affermarsi del modello Industria 4.0, comporta l'aggravarsi delle minacce e della vulnerabilità, dal momento che non sempre ad una maggiore digitalizzazione degli ambienti industriali corrisponde una piena consapevolezza dei rischi sul fronte Cyber e l'adozione di adeguate misure di prevenzione e di protezione.

Nel 2020 il 61% delle aziende manifatturiere è stato vittima di un attacco informatico; di queste il 75% ha dovuto fronteggiare un blocco della produzione, secondo il rapporto TrendMicro "The State of Industrial Cybersecurity: Converging IT and OT with People, Process, and Technology". Per il 43% di queste aziende vittime di attacchi informatici, l'interruzione produttiva è durata oltre quattro giorni, con conseguenti danni economici.

Secondo una survey condotta da Sophos nel 2020, i ransomware hanno rappresentato una delle principali modalità di attacco, avendo colpito il 36% delle organizzazioni manifatturiere. Di queste il 49% ha subito una data encryption, ma solo il 19% ha effettivamente pagato un riscatto, sebbene questo non sempre abbia garantito il recupero dei dati criptati (in media la metà dei dati resta inaccessibile). Il pagamento del riscatto infatti non sempre è legato alla possibilità di recuperare i dati, ma spesso viene richiesto per evitare che dati critici o di elevata strategicità possano essere venduti sul web (ad esempio dati protetti da Intellectual Property). Il costo medio stimato per un attacco ransomware è di 1,52

Figura 11:

Principali motivazioni che inducono le aziende a prevedere di essere bersaglio di attacchi ransomware



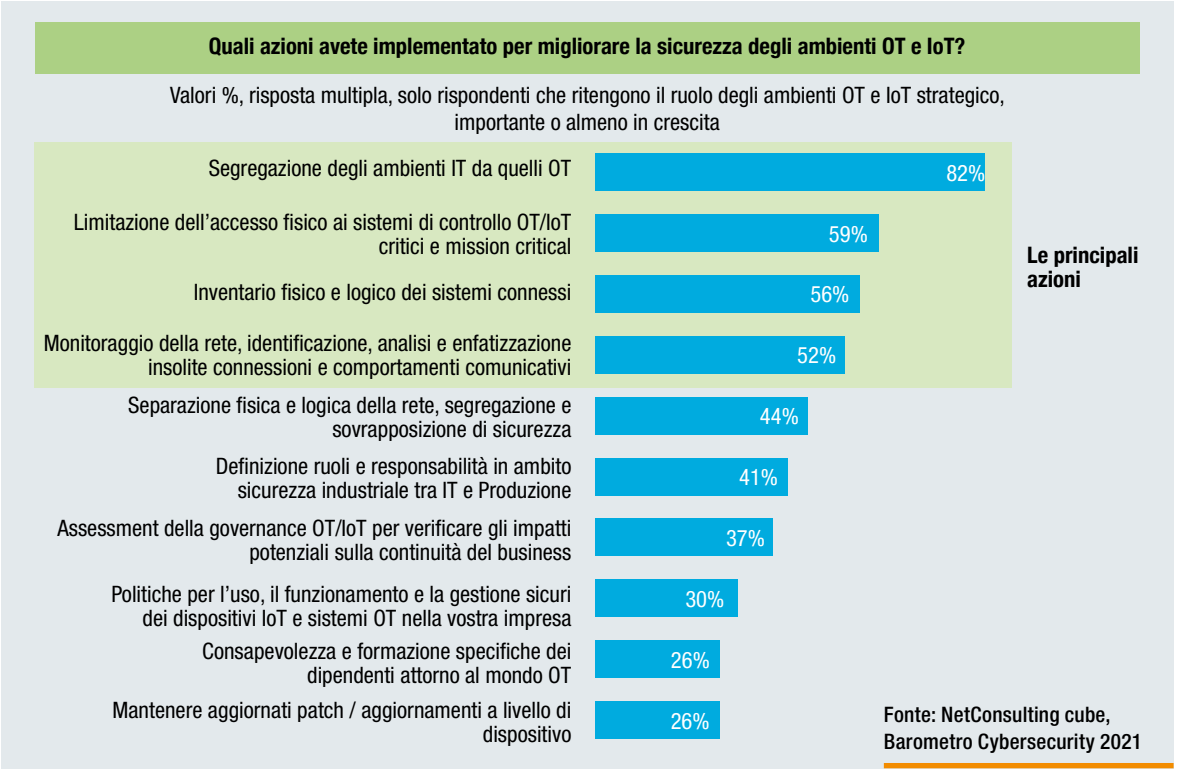
Valori in migliaia,
variazioni % anno su anno
Fonte: NetConsulting cube, 2021

milioni di dollari, considerati il tempo perso per la gestione dell'incidente, i costi per eventuali servizi o tecnologie di remediation e l'interruzione dell'attività produttiva.
La preoccupazione riguardo a questa tipologia di attacchi si mantiene elevata anche per il prossimo anno, con il 49% delle organizzazioni che prevede di essere colpito da un attacco, per effetto della loro crescente sofisticazione (Fig. 11).
La stessa survey evidenzia che tra le aziende che ritengono improbabile di subire attacchi ransomware, il 56% dichiara di avere un team di Cybersecuirty in grado di contrastare e prevenire questa tipologia di attacchi e il 42% ha adottato tecnologie anti-ransomware.

PRIORITÀ DI INVESTIMENTO

La filiera dell'IoT e degli ambienti di produzione connessi può rappresentare uno degli anelli deboli della Cybersecurity, come dimostra il fatto che questa costituisce una delle tecnologie abilitanti del Piano Transizione 4.0, con la possibilità di beneficiare del credito d'imposta per gli investimenti correlati.
In questo contesto, sono numerose le aree di miglioramento su cui operare per la messa in sicurezza dei nuovi ambienti di produzione 4.0.
L'82% del panel intervistato da NetConsulting cube per il Barometro Cybersecurity, dove il ruolo degli ambienti di Industrial IoT e Operational Technology è indicato come importante, strategico o in crescita, prevede la segregazione/segmentazione della rete in ambienti differenti, IT e OT, come principale azione volta a migliorare il livello di sicurezza. Per ottenere maggiore visibilità, il 56% degli intervistati dispone di un inventario fisico e logico dei sistemi connessi, così come di attività di monitoraggio di rete, per l'identificazione di connessioni e comportamenti comunicativi insoliti (52%) (Fig. 12).
Meno diffusa è la separazione fisica e logica (44%) dei sistemi connessi, pur rappresentando una delle principali misure da adottare.
Importante è inoltre, a livello di struttura organizzativa, la definizione di una chiara distinzione di ruoli e responsabilità tra IT e Direzione Produzione/Operations (41%). Si tratta di un tema chiave, se consideriamo che solo il 15% delle aziende intervistate

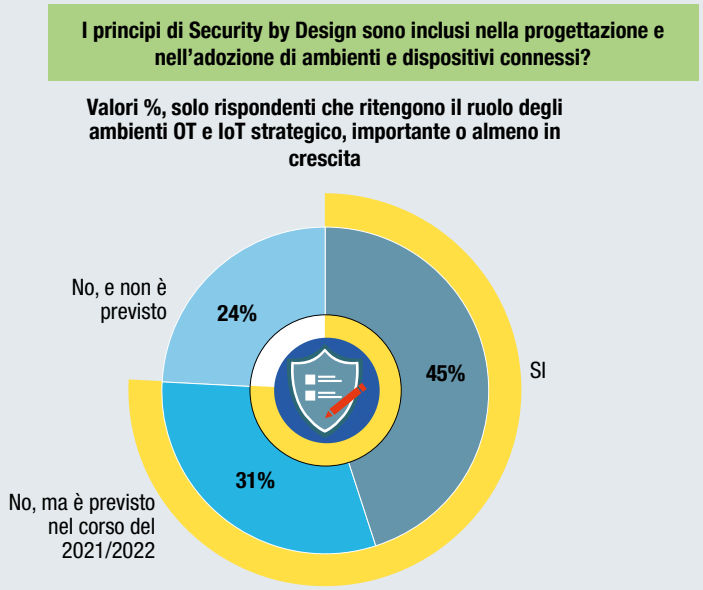
Figura 12:
Le azioni implementate per migliorare la sicurezza degli ambienti OT/IoT



ha individuato un Responsabile Industrial Security, ruolo che risponde nella maggioranza dei casi al CISO o, in termini più generali, alla funzione IT o talvolta alla funzione Security (CSO).
Altre azioni implementate comprendono, a livello di governance e organizzazione, attività di assessment sulla governance stessa OT/IoT per verificare i potenziali impatti sulla Business Continuity (37%), la definizione di policy per il funzionamento e la gestione di apparati e dispositivi connessi (30%), la realizzazione di programmi di awareness e formazione specifica dei dipendenti in tema di sicurezza (26%).

Inoltre, si sta diffondendo l'utilizzo di principi di Security by Design anche nell'adozione e nella progettazione di ambienti e dispositivi connessi, già indicato come best practice dall'ENISA nel rapporto "Guidelines for securing the IoT – Securing Supply Chain for IoT": tali principi sono previsti nel 45% dei casi ed entro il 2022 saranno introdotti nei processi di gestione da un ulteriore 31% (Fig. 13).
Tuttavia, il restante 24% degli intervistati, afferente in particolare al settore della media Industria, non ne prevede l'introduzione nemmeno nel medio termine, evidenziando un gap a livello di governance con aziende di maggiori dimensioni che, se da un lato sconta allo stato attuale il minore livello di digitalizzazione dei processi produttivi, dall'altro evidenzia la necessità di porre maggiore attenzione nei confronti di vulnerabilità che non possono essere considerate marginali.
Ulteriori misure che assumono un ruolo fondamentale nella messa in protezione del perimetro industriale riguardano l'aggiornamento dei firmware, da effettuare periodicamente per colmare i bug a livello firmware, e la sostituzione di sistemi operativi obsoleti.
Le aziende industriali devono inoltre prestare attenzione al livello di protezione della propria catena di fornitura, non solo per le soluzioni tecnologiche o di macchinari di produzione, ma anche, ad esempio, per la logistica. Attaccare l'anello più debole all'interno di una determinata Supply Chain può fornire l'accesso a dati e informazioni critiche di un'azienda con un buon livello di protezione di sicurezza informatica. Per incrementare il livello di sicurezza nella Supply Chain, il panel di aziende appartenenti al settore Industria, intervistate da NetConsulting cube, adotta nell'80% dei casi protocolli standard di Security Management, così come misure di sicurezza standardizzate e attività di formazione specifica sul personale (40%) (Fig. 14).
Ulteriori attività svolte afferiscono ad analisi periodiche del rischio organizzativo, come il Vulnerability Management, e ad analisi del rischio tecnologico, come il Vulnerability Assessment e il Penetration Test.

Figura 13:
Adozione di principi di Security by Design per apparati e dispositivi IoT/OT



Fonte: NetConsulting cube, Barometro Cybersecurity 2021

Il quadro normativo e il ruolo della Cybersecurity nell'evoluzione digitale del Paese

PERIMETRO CIBERNETICO

La definizione del Perimetro di Sicurezza Nazionale Cibernetica, istituito con Decreto Legge 21 settembre 2019, n. 105 getta le basi per garantire un livello di sicurezza adeguato e di resilienza di sistemi e servizi informatici e delle reti di enti e organizzazioni pubbliche e private con presenza nel territorio nazionale, da cui dipende l'esercizio di funzioni essenziali da parte dello Stato.
Con il successivo DPCM 30 luglio 2020, n. 131 sono state definite le modalità e i criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati, inclusi nel Perimetro.
Il quadro normativo è completato da:

- il Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 che individua le procedure, le modalità ed i termini da seguire per l'acquisizione, da parte dei soggetti inclusi nel Perimetro, di oggetti di fornitura.
- Il DPCM 14 aprile 2021, n. 81 che determina le procedure per la notifica degli incidenti di sicurezza informatica.
- Il DPCM 15 giugno 2021 che individua le categorie di beni, sistemi e servizi ICT destinati a essere impiegati nel Perimetro di Sicurezza Nazionale Cibernetica. L'allegato al DPCM determina gli asset ICT ricompresi nel perimetro Cyber e le macrocategorie di riferimento. In particolare:
  - componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione);
  - componenti hardware e software che svolgono

Figura 14:
Attività previste da contratto per la sicurezza della Supply Chain

funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati;
- componenti hardware e software per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali;
- applicativi software per l'implementazione di meccanismi di sicurezza.

Inoltre si prevede che «le categorie individuate dal presente decreto siano aggiornate, con decreto del Presidente del Consiglio dei Ministri, con cadenza almeno annuale, avuto riguardo all'innovazione tecnologica, nonché alla modifica dei criteri tecnici».
L'ultimo tassello a completamento del quadro normativo sarà il DPCM riguardante le regole di accreditamento per i laboratori che potranno effettuare screening tecnologici.
La normativa si applica ad un elenco di società e organizzazioni che sono state individuate in modo puntuale in quanto rappresentano infrastrutture critiche, sebbene sia a livello nazionale che a livello europeo si preveda l'estensione progressiva ad un gruppo di società più ampio.

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

La nascita dell'Agenzia per la Cybersicurezza Nazionale (ACN) viene sancita con la conversione del Decreto Legge 14 giugno 2021, n. 82 nella Legge 4 agosto 2021, n. 109. La conversione segna il completamento della strategia di cyber-resilienza nazionale, avviata con il Perimetro Cibernetico di Sicurezza.
L'Agenzia, con sede a Roma, dispone di personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria.
In accordo con l'articolo 7 del Decreto Legge n. 82 l'Agenzia:

- svolge il ruolo di Autorità nazionale in materia di Cybersecurity, a tutela degli interessi nazionali e della resilienza dei servizi e delle funzioni essenziali dello Stato da minacce cibernetiche;
- ha il compito di sviluppare le capacità nazionali di prevenzione, monitoraggio, rilevamento e mitigazione, per far fronte agli incidenti di sicurezza informatica e agli attacchi informatici, anche attraverso il Computer Security Incident Response Team (CSIRT) italiano e l'avvio operativo del Centro di valutazione e certificazione nazionale;
- ha l'obiettivo di contribuire all'innalzamento della sicurezza dei sistemi ICT dei soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica, delle Pubbliche Amministrazioni, degli Operatori di Servizi Essenziali (OSE) e dei Fornitori di Servizi Digitali (FSD);
- supporta lo sviluppo di competenze industriali, tecnologiche e scientifiche, promuovendo progetti per l'innovazione e lo sviluppo, con l'obiettivo di stimolare nel contempo la crescita di una solida forza lavoro nazionale nel campo della Cybersecurity e conseguire autonomia strategica nazionale nel settore;
- assume le funzioni di interlocutore unico nazionale per i soggetti pubblici e privati in materia di misure di sicurezza e attività ispettive negli ambiti del Perimetro di Sicurezza Nazionale Cibernetica, della sicurezza delle reti e dei sistemi informativi (direttiva NIS), e della sicurezza delle reti di comunicazione elettronica. L'Agenzia, inoltre, nel ruolo di Centro nazionale di coordinamento italiano, è anche interlocutore con il "Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca", istituito al fine di concentrare gli investimenti nello sviluppo industriale, nella tecnologia e nella ricerca sulla Cybersecurity.

Tra gli obiettivi sottostanti la nascita dell'ACN, vi è quindi anche l'esigenza di una maggiore razionalizzazione della governance della Cybersecurity nazionale. Al di fuori dell'Agenzia, la Polizia Postale rimane responsabile delle attività di Cyber Investigation, mentre la Cyber Intelligence resta sotto l'autorità del Dipartimento delle Informazioni per la Sicurezza (DIS).
In aggiunta, sempre il Decreto n. 82 istituisce il Comitato Interministeriale per la Cybersicurezza (CIC), con funzioni di consulenza, proposta e vigilanza in materia di politiche di Cybersecurity, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, a supporto del Presidente del Consiglio nell'adozione della strategia nazionale di sicurezza.
L'Agenzia opera sotto la responsabilità del Consiglio dei Ministri e dell'Autorità delegata per la Sicurezza, in stretto raccordo con il Sistema di informazione per la sicurezza della Repubblica (art. 2).
Il Presidente del Consiglio ha così facoltà di:

- adottare la strategia nazionale di Cybersicurezza (art.2), sentito il Comitato interministeriale per la Cybersicurezza (CIC);
- nominare e revocare il direttore generale e il vicedirettore generale dell'Agenzia per la Cybersicurezza;
- impartire le direttive per la Cybersicurezza ed emanare ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia.

Il 5 agosto 2021, Roberto Baldoni, dopo aver ricoperto il ruolo di vicedirettore del Dipartimento delle Informazioni per la Sicurezza (DIS), è stato nominato Direttore Generale dell'ACN. Il Direttore Generale dell'Agenzia svolge inoltre le funzioni di segretario del neocostituito Comitato Interministeriale per la Cybersicurezza.

Presso l'Agenzia è stato inoltre creato, in via permanente, il Nucleo per la Cybersicurezza, a supporto del Presidente del Consiglio dei Ministri per gli aspetti relativi alla prevenzione e preparazione di eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento (art. 8). Il Nucleo è presieduto dal Direttore Generale dell'Agenzia o, per sua delega, dal Vice Direttore Generale ed è composto dal Consigliere militare del Presidente del Consiglio dei Ministri, da un rappresentante, rispettivamente, del DIS, dell'Agenzia Informazioni e Sicurezza Esterna (AISE), dell'Agenzia Informazioni e Sicurezza Interna (AISI), di ciascuno dei Ministeri rappresentati nel CIC e del Dipartimento della protezione civile della Presidenza del Consiglio dei Ministri. Per gli aspetti relativi alla trattazione di informazioni classificate, il Nucleo è integrato da un rappresentante dell'Ufficio Centrale per la Segretezza. Il Nucleo può inoltre:

- formulare proposte per iniziative in materia di Cybersecurity attinenti l'Italia;
- promuovere la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati;
- curare lo svolgimento di esercitazioni interministeriali, o la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;
- essere coinvolto nelle crisi relative alla Cybersicurezza.

Tra le sfide che l'Agenzia deve affrontare, oltre al ritardo nella sua nascita rispetto ad istituzioni equivalenti in altri Paesi europei come Francia e Germania, che possono contare su organici rispettivamente di 1.000 e 1.200 unità, vi è la necessità di reperire risorse con competenze specifiche, già ridotte sul mercato, con stipendi concorrenziali. A novembre 2021 sono stati trasferiti all'Agenzia i primi 60 esperti dal DIS con l'obiettivo di arrivare a 90 unità entro la fine dell'anno, a 300 entro la fine del 2023 e a 800 entro il 2027.

TRANSIZIONE AL CLOUD DELLA PUBBLICA AMMINISTRAZIONE E RUOLO DELLA CYBERSECURITY

La transizione al cloud assume un ruolo centrale nella digitalizzazione della Pubblica Amministrazione, in virtù della scalabilità e della flessibilità che caratterizza il cloud rispetto all'IT tradizionale abilitando i nuovi servizi digitali.

La Strategia Cloud Italia fornisce l'indirizzo strategico per l'implementazione e il controllo di soluzioni cloud nella Pubblica Amministrazione stabilendo le seguenti linee di azione:

- la creazione del Polo Strategico Nazionale (PSN), che diventerà un'infrastruttura nazionale per l'erogazione di servizi cloud, la cui gestione e controllo di indirizzo saranno autonomi rispetto a fornitori extra UE. Il PSN sarà articolato in 4 Datacenter in almeno 2 regioni;
- un percorso di qualificazione dei fornitori di cloud pubblico e dei loro servizi per garantire che le caratteristiche e i livelli di servizio dichiarati siano in linea con i requisiti necessari di sicurezza, affidabilità e rispetto delle normative rilevanti;
- lo sviluppo di una metodologia di classificazione dei dati e dei servizi gestiti dalle Pubbliche Amministrazioni, per permettere una migrazione di questi verso la soluzione cloud più opportuna (PSN o cloud pubblico qualificato).

L'evoluzione verso il cloud della PA e di operatori nazionali che gestiscono infrastrutture critiche espone tuttavia il Paese ad alcuni rischi di rilevanza sistemica, primo tra tutti quello di eventuali ingerenze di Paesi extra europei verso quei cloud provider che devono sottostare a legislazioni extra UE, che attualmente detengono una quota rilevante del mercato di questi servizi. In virtù delle normative vigenti in alcuni Paesi, vi sarebbe la possibilità, per uno Stato estero (o Paese Terzo), di accedere a dati (o flussi di dati) particolarmente sensibili e strategici per i cittadini e le istituzioni italiane.

In tale scenario risulta assolutamente fondamentale avere un'autonomia tecnologica nel controllo delle infrastrutture digitali del cloud e conseguentemente nello stoccaggio e nell'elaborazione dei dati, oltre che incentivare lo sviluppo di un comparto tecnologico nazionale in tutti gli ambiti innovativi: Cloud Computing, Artificial Intelligence, IoT, Quantum Computing e Cybersecurity.

Inoltre, al fine di consentire un controllo sui dati presenti sul cloud, la Strategia Nazionale si pone nell'ottica di determinare in modo chiaro, attraverso una procedura di classificazione, quali tipologie di dati potranno essere gestiti da un fornitore extra UE attraverso un cloud pubblico e quali invece avranno

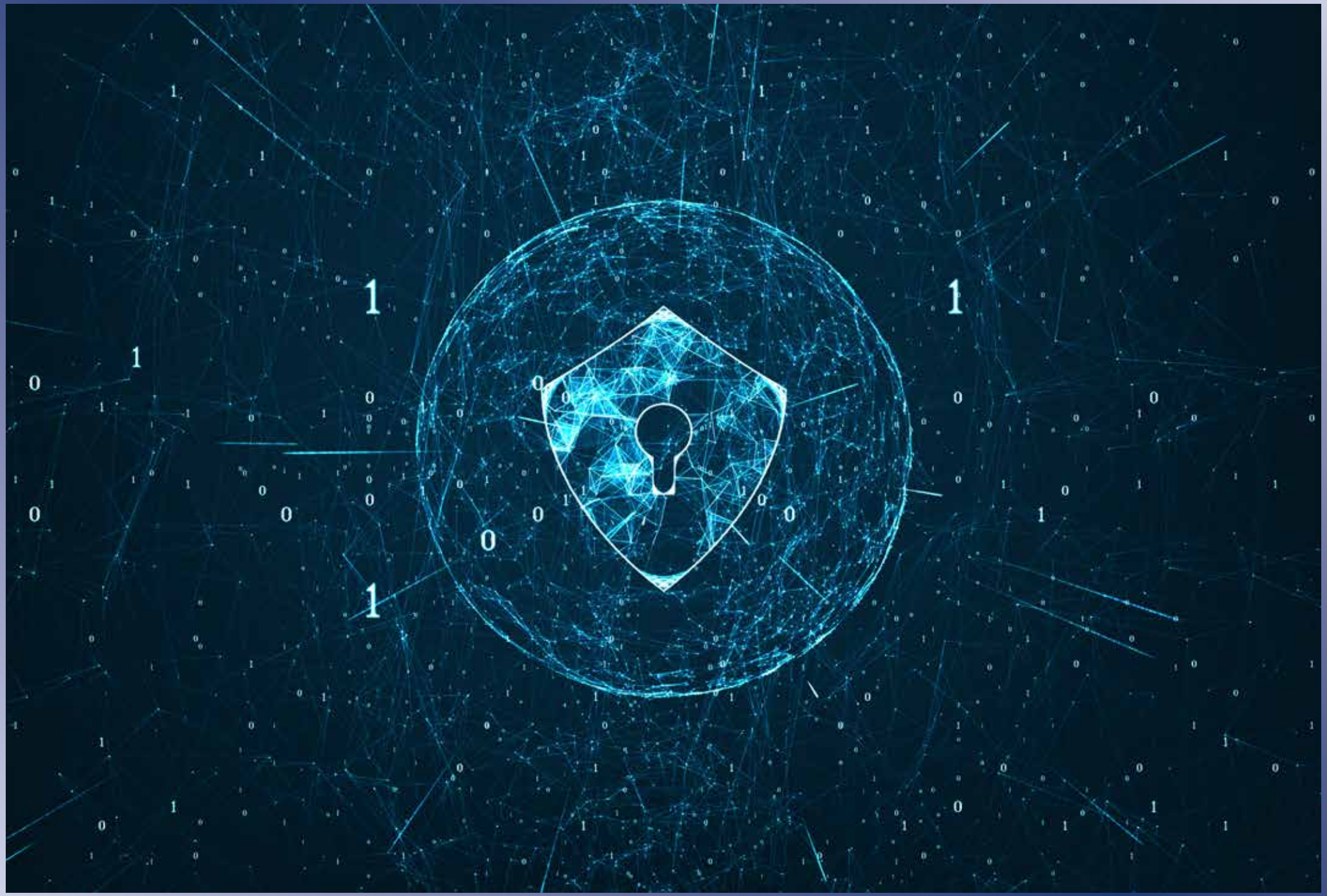
bisogno di essere gestiti da un fornitore cloud che soddisfi specifici requisiti di sicurezza.
Secondo quanto viene illustrato nella Strategia Nazionale, «le classi dei dati e servizi sono identificate sulla base del danno che una loro compromissione, in termini di confidenzialità, integrità e disponibilità, provocherebbe al sistema Paese». Il danno viene pertanto così classificato:

- Strategico: dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale;
- Critico: dati e servizi la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese;
- Ordinario: dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese.

Un ulteriore fattore che andrà considerato è il livello di resilienza dei sistemi e un'adeguata protezione da eventuali incidenti, sia che si tratti di attacchi Cyber, che di guasti tecnici. Questo si traduce, da un lato, nell'applicazione di controlli di sicurezza stratificati conformi ai requisiti specifici dei dati trattati e, dall'altro, nell'introduzione di funzionalità di continuità di servizio e disaster recovery in siti geograficamente distribuiti sul territorio nazionale.
Inoltre, sarà previsto un processo di qualificazione dei fornitori di cloud pubblico e dei loro servizi che siano tali da garantire un livello di sicurezza adeguato e di limitare il rischio di vendor lock-in.
A completamento della Strategia e al fine di costituire un ecosistema integrato e basato su standard comuni, è stato avviato il progetto GAIA-X con l'obiettivo di sviluppare requisiti comuni per un'infrastruttura dati europea e collegare infrastrutture centralizzate e decentralizzate trasformandole in un sistema omogeneo.
Infine, un aspetto centrale dell'Agenzia di Cybersicurezza sarà quello di supportare le Amministrazioni nella classificazione dei dati e dei servizi per attuare la migrazione verso i diversi servizi cloud qualificati. La classificazione e la redazione del piano di migrazione saranno definiti e supportati, per i rispettivi profili di competenza, dall'Agenzia per la Cybersicurezza Nazionale e dal Dipartimento per la Trasformazione Digitale.

CONSIDERAZIONI FINALI

La trasformazione digitale dell'Italia sta proseguendo la sua marcia con innegabili miglioramenti per la vita delle persone e vantaggi per il sistema economico nel suo complesso. In questo quadro, la Cybersecurity rappresenta un ambito che avrà negli anni un'importanza crescente. L'impegno nella prevenzione dei danni e nella gestione dei rischi necessita pertanto di plurimi interventi: la dotazione di regole adeguate e di una governance pubblica integrata a livello europeo ed internazionale; la conoscenza e la consapevolezza, da parte delle imprese, che la sicurezza cibernetica rappresenta una priorità d'azione e d'investimento; la formazione di personale specializzato e qualificato.



CONSIDERAZIONI FINALI

Il rapporto evidenzia la crescita degli attacchi cyber, a livello nazionale e mondiale, che hanno come obiettivo aziende ed enti pubblici/privati. La transizione digitale, con l'adozione e la diffusione di nuove tecnologie come il cloud, presenta da un lato vantaggi innegabili per la competitività del "sistema paese", a partire dalla produttività e dallo stimolo all'innovazione tecnologica, dall'altro estende le superfici di attacco cyber, aumentando i rischi ed evidenziando le vulnerabilità del comparto economico e amministrativo del Paese.

Eppure, la transizione digitale è un nastro che non si potrà riavvolgere: nel futuro non esisteranno meno servizi digitali, ma accadrà il contrario, e ciò riguarderà ogni campo del vivere. In questo quadro, la Cybersecurity sarà un pezzo indispensabile della **trasformazione digitale**.

Per questo l'impegno deve essere rivolto a gestire i rischi, prevenire i danni e sapere rispondere con celerità e flessibilità ai bisogni emergenti di sicurezza. Per farlo, sono necessari interventi su diversi piani: regole, consapevolezza e competenze.

1. **Dotarsi di regole adeguate e di una governance pubblica integrata a livello europeo e cooperante a livello internazionale.** In questo senso, la proposta di direttiva NIS2, la nuova strategia europea per la Cybersecurity, insieme al pacchetto di misure adottate a livello nazionale (incluso il decreto sul perimetro di sicurezza cibernetica) concorrono a definire procedure, obblighi, tipologia di rischi nonché soggetti coinvolti con l'obiettivo di innalzare il livello di protezione e di prevenire/gestire eventuali criticità. La recente costituzione dell'Agenzia per la sicurezza cibernetica rappresenta un ulteriore e fondamentale passo in avanti non solo per adeguare il nostro Paese a quanto già fatto a livello europeo, ma anche per dotare di poteri di intervento immediati e **promuove una cooperazione tra pubblico e privato basata sulla condivisione delle informazioni,** nonché un coordinamento più efficace tra i diversi soggetti istituzionali coinvolti nelle azioni di prevenzione e repressione dei reati cibernetici. Tutti elementi più che mai necessari a salvaguardare il nostro sistema.

   Sarà necessario, da oggi in poi, sia garantire un costante monitoraggio e aggiornamento delle normative specifiche, in funzione delle evoluzioni dei fenomeni di Cybercrime, quanto presidiare i profili di Cybersecurity relativi ai diversi dossier di policy (dal codice delle comunicazioni, alla digitalizzazione della sanità e dei trasporti etc.) che dovranno dedicare ampia attenzione ai profili di sicurezza.

2. **Consapevolezza e conoscenza.** La digitalizzazione del Paese è uno dei due assi strategici del PNRR. Già la pandemia ha dato una spinta alla digitalizzazione dei processi grazie al ricorso allo smart working, all'e-commerce, alla DAD e in generale alle piattaforme di condivisione in cloud. Ma fino a oggi, nessun programma e nessuna azione per la digitalizzazione erano stati così ampi e pervasivi da impattare pressoché contempo-

raneamente ogni settore: PA, imprese e cittadini sono investiti da un'innovazione tecnologica volta a recuperare il ritardo accumulato negli anni, migliorando la qualità della vita delle persone, innalzando la produttività delle imprese, efficientando e modernizzando processi e servizi che la PA eroga a cittadini e imprese; non da ultimo, sostenendo l'offerta di innovazione del mercato.
In questo senso, tanto la strategia del Piano Strategico Nazionale per il Cloud previsto dalla Missione 1 del PNRR, quanto le azioni di progressivo adeguamento tecnologico degli enti locali si collocano nel quadro di dotare la PA di necessarie soluzioni tecnologiche per sviluppare servizi e applicazioni e definire un perimetro di sicurezza chiaro ove collocare i dati sensibili dei cittadini.
Dal lato delle imprese, la proroga negli anni di Industria 4.0, nelle sue diverse declinazioni, ha sostenuto la digitalizzazione nel privato attivando un circuito virtuoso di investimenti digitali da parte delle industrie manifatturiere tradizionali e sostenendo l'offerta di soluzioni digitali tra le più innovative.
In questo quadro, è tuttavia evidente che le superfici di attacco potenziale da parte di Cybercriminali si stanno estendendo in maniera significativa e la crescita dei dati evidenziati nel rapporto ne testimonia tutta la rilevanza e la gravità. Per questo, più di tutto, è necessaria un'adeguata assunzione di consapevolezza della vulnerabilità delle proprie attività da parte degli imprenditori e, conseguentemente, l'adozione di politiche di investimento e formazione dei lavoratori.
Le PMI in particolare – che stanno affrontando la transizione digitale con più fatica e con limitato accesso a conoscenze qualificate – necessitano di un'iniezione in più di awareness, per far sì che la sicurezza cibernetica diventi una priorità di investimento per i prossimi anni e che si inseriscano figure professionali adeguate a mappare il rischio e intervenire in caso di attacchi. La sicurezza informatica non è un tema che attiene solo alle grandi imprese. Il costo di non presidiare la Cybersecurity è sia economico (il **costo** medio di un data breach si aggira intorno ai 3,8 milioni di dollari, composto da: costi di **indagine**, di **remediation**, di **notifica**, **perdita di business** (40%); il **tempo** medio per contenere un data breach è pari a 280 giorni di cui 200 solo per individuarlo), che di competitività. Tra i rischi, il furto di brevetti o la violazione di diritti di proprietà intellettuale ovvero il fermo di impianti industriali "Industria 4.0" rappresentano quelli più evidenti. Ma non va tralasciato anche il rischio di minare la fiducia dei consumatori o dei clienti laddove le violazioni dovessero colpire anche dati di terzi.
Ancora, le imprese di qualsiasi dimensione non devono e non possono pensare di vivere in oasi protette: sono inserite all'interno di filiere e di catene di fornitura, e molte delle interazioni con partner e clienti viaggiano ormai on line e sul cloud. Questa "operatività" virtuale può essere la porta d'accesso per eventuali Cybercriminali e, pertanto, bisogna adottare comportamenti e soluzioni coerenti che mettano in sicurezza l'intero processo produttivo, sia dentro casa che fuori.
Per tutte queste ragioni, la Cybersecurity non può che essere al centro dell'attenzione dei vertici delle aziende (e parallelamente delle istituzioni): occorre un mandato top down per individuare figure e/o consulenti specializzati cui affidare la sicurezza delle imprese; compiere adeguate valutazioni dei rischi; assicurare ogni forma di cooperazione utile lungo la filiera e con le autorità.

3. **Competenze.** Se già la transizione digitale sta ponendo più di una sfida al mercato del lavoro e alla formazione di giovani e lavoratori attivi, ciò vale ancora di più se si considerano le competenze necessarie per operare in ambito Cybersecurity. Tanto negli apparati pubblici quanto nelle imprese, occorrono specialisti con competenze settoriali per affrontare le sfide che i crimini informatici pongono e che sono, purtroppo, in costante evoluzione. La formazione di personale specializzato richiede risorse finanziarie sia da parte del pubblico che del privato, insieme a una stretta collaborazione tra università e imprese nella progettazione dei corsi di studio.
   In Italia sono attivi ancora pochi **corsi**. Su oltre 100 università nazionali sono presenti corsi specifici in Cybersecurity così distribuiti: una laurea triennale, diciotto lauree magistrali, nove master di I livello, tre master di II livello, tre dottorati di ricerca (dati CINI).
   Numeri decisamente poco confortanti, visto il fabbisogno da colmare e l'urgenza di garantire una competenza diffusa e specializzata costante per accompagnare la transizione digitale.
   In primo luogo, la Cybersecurity deve diventare una professione per i giovani. Coinvolgere le nuove generazioni di studenti nelle attività di prevenzione e gestione dei rischi informatici e prepararli a occupazioni in questo settore implica, per esempio: 1. Far comprendere la gravità e i rischi

che si corrono anche con comportamenti digitali "usuali" (condivisione di materiale, download da siti non autorizzati, phishing) in modo da creare interesse e attenzione; 2. Ideare percorsi didattici, dalle scuole alle università, dedicati alla sicurezza informatica, coinvolgendo specialisti e imprese nelle attività di education: dalla formazione in aula, alla predisposizione di materiali ad hoc, fino a tirocini e stage professionalizzanti; 3. Condividere con il Ministero dell'Università e della Ricerca la destinazione di risorse ad hoc per dottorati industriali in ambito Cybersecurity.

L'obiettivo è creare competenze specialistiche, superando l'abitudine a cooptare in posizioni lavorative in ambito Cybersecurity figure professionali che pur operando in ambito IT non hanno le adeguate conoscenze informatiche per prevenire e gestire gli attacchi.

Secondariamente, la Cybersecurity richiede formazione e aggiornamenti costanti anche per chi opera in azienda: c'è bisogno di fare education dei lavoratori, per evitare comportamenti – soprattutto in caso di lavoro agile – che possano compromettere la sicurezza aziendale o delle amministrazioni (utilizzo promiscuo dei device, accesso a reti non protette etc.); ancora, vanno previsti percorsi di aggiornamento utilizzando anche risorse dei fondi professionali, gli incentivi per la formazione 4.0, le reti di competenze diffuse sul territorio – a partire dai Digital Innovation Hub – capaci di mettere a sistema specialisti in Cybersecurity con cui costruire percorsi di formazione ad hoc per le imprese.

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 – rappresenta un settore vitale e strategico per il nostro Paese. È il riferimento per le aziende italiane dell'high-tech digitale, di ogni dimensione e specializzazione.
Anitec-Assinform aderisce a Confindustria ed è socio fondatore di Confindustria Digitale, la Federazione di categoria che promuove lo sviluppo dell'economia e della società digitale in Italia. È il socio italiano di Digitaleurope, l'Associazione Europea dell'Industria ICT con sede a Bruxelles, ed è membro dell'Executive Board.
La missione di Anitec-Assinform si esplicita lungo tre filoni principali: rappresentanza del settore, servizio operativo, confronto e dialogo fra gli operatori.
Sul fronte della rappresentanza, è il ponte fra le principali forze economiche, politiche e istituzionali e il mondo del digitale. Non solo tutelando i diritti e divulgando le istanze delle imprese del settore, ma anche contribuendo ad alimentare le conoscenze sulle sfide della società digitale e il loro impatto sulla qualità della vita, il sistema della ricerca, la formazione, i servizi al cittadino, le opportunità di impresa, l'occupazione, la collocazione del nostro Paese nel contesto economico europeo e mondiale.
Sul fronte dei servizi, Anitec-Assinform dà risposte puntuali alle aziende del settore che chiedono un supporto di immediato interesse pratico nei più diversi ambiti. Lo spettro è amplissimo: va dalla conoscenza dei mercati all'accesso ai fondi pubblici, dal supporto legale al confronto con le rappresentanze dei principali settori d'utenza e con i soggetti che definiscono norme tecniche. L'autorevolezza delle analisi, delle informazioni e delle posizioni espresse dall'Associazione trova riscontro anche sul Web.
Il sito di Anitec-Assinform è un riferimento per il settore, noto non solo agli Associati, ma anche agli Amministratori e agli opinion leader che si rivolgono all'Associazione per informazioni aggiornate e risposte concrete.
Tutto questo è possibile perché in Anitec-Assinform tutto ruota attorno alle Aziende Associate, che contribuiscono a una missione che va a vantaggio di tutti.

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

18 Months Srl
3M Italia - Sistemi Informativi per la Salute
Accenture Spa
ADS Automated Data Systems Spa
Adamantic Srl
Aitek Spa
Algowatt Spa
AlmavivA Spa
Amazon Italia Service Srl
Apparound Italia Srl
Apple Italia Srl
Array System Srl
Atik Srl
Atos Italia Spa
Auriga Srl
Autec Srl
Avaya Italia Spa
Axle Ict Solutions Srl
Axway Srl
Banksealer
BlueIt Spa
Blulink Srl
BMC Software Srl
BT Italia
BTO Research
C.A.T.A. Informatica
Cadan Srl
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
Cykel Software
Dassault Systemes Italia Srl
Data 4 Services Italy Spa
Datacore Software
Db Elettronica Telecomunicazioni Spa
Dell Spa
Develhope
Digiquest Solutions
Digital Magics Spa
Dilium Srl
DVR Italia Srl
DXC Technology Italia
Easygov Solutions Srl
Ecoh Media Srl
Edicom Srl
El.Ca Elettronic System Srl
Elettromedia Srl
Emme Esse Spa
Epson Italia Spa
Eris Srl
Esri Italia Spa
Euronet Srl
Eustema Spa
Exprivia Spa
Facebook Italy Srl
FacilityLive OpCo Srl
Fasternet Srl
Fibernet Srl
Finix Technology Solutions
Fitre Spa
Flow Factory Srl
FN & Partners Srl

Focus Group Srl
Fondazione Asphi
Formatech Srl
Fracarro Radioindustrie Srl
FreeNow
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
IBM Italia Spa
ICT Consulting Spa
ICT Logistica Spa
ID Technology
Ids Georadar Srl
Ids Spa
IFM Srl
iGenius Srl
INAZ Srl
InfoCamere SCpA
Informatica
Inmatica Spa
Insiel 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
Keysight Technologies Italy Srl
Kibernetes 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
Maggioli Spa
Mare Engineering Spa
Maticmind Spa
Maxfone Srl
Mediafarm Srl
Mega Italia Media Spa
Meliconi 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
Nokia Solutions and Networks Spa
Nolan Norton Italia Srl
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
Present Spa

Proclesis Srl
Proxel Srl
QiBit - Divisione Ict di Gigroup Spa
Qualcomm Inc.
Qualta Spa
Quid Informatica Spa
Red Hat Srl
Reply 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
Skyrobotic Spa
Sogei — Società Generale d'Informatica Spa
Sony Europe BV
Sorint.Lab
Strong Italia Srl
Synergie Italia Spa
Tecnira Srl
Tecnologica Srl
TELE System Digital Srl
Tema Sistemi Informatici
The Next Srl
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
Versya Srl
VMware Italy Srl
Westpole Spa
Zerouno Informatica Spa
Zucchetti
Zucchetti Centro Sistemi

REALIZZATO E PUBBLICATO DA ANITEC-ASSINFORM.

CONTENUTI A CURA DI NETCONSULTING CUBE:

- Le previsioni 2021-2022 per il mercato digitale italiano
- Cybersecurity e transizione digitale

CONTENUTI A CURA DI ANITEC-ASSINFORM:

- Considerazioni finali

Revisione editoriale: Filippo Cavazzoni
Coordinamento: Luisa Bordoni
Grafica e impaginazione: Studio Zanoni sas - Milano
Pubblicato in versione elettronica – Novembre 2021
Chiusura testi - Novembre 2021

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