

Clicca qui sotto per andare all'articolo originale

<https://www.ilsole24ore.com/art/cybersicurezza-incentivi-meta-burocrazia-e-spesa-escluse-AH7AOOuD>

[Vai alla navigazione principale](#)
[Vai al contenuto](#)
[Vai al footer](#)

Italia Attualità

24+

Abbonati

Accedi

In Evidenza

Criptovalute

Spread BTP-Bund

FTSE-MIB

Petrolio

Pubblicità

24

I NOSTRI VIDEO

24

Rafforzare l'UE attraverso lo sviluppo delle infrastrutture del...

24

Sicurezza psicologica in azienda

24

Fratoianni (Avs): Destra vuole cambiare brutta legge elettorale so...

Servizio | Il quadro

Cybersicurezza: incentivi a metà fra burocrazia e spese escluse

Dal maxi ammortamento con detrazione dei costi al voucher del Mimit con plafond da 150 milioni: tutte le misure a sostegno delle imprese per il 2025-2026. Fuori gli oneri per servizi It. Procedure complesse e tempi di accesso frenano l'utilizzo

di Ivan Cimmarusti

26 novembre 2025



▲ Michael Traitov - stock.adobe.com

I punti chiave

- Le misure in campo
- I nodi da sciogliere

Ascolta la versione audio dell'articolo

4' di lettura

English Version

Loading...

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - 6489



Non è solo una questione di quanti soldi ci sono in campo. Il punto vero, quando si parla di **cybersicurezza** delle Pmi italiane, è come quelle risorse sono progettate, rese accessibili, strutturate nel tempo.

Le misure pubbliche oggi in vigore sono davvero adeguate a proteggere le imprese, mentre **gli attacchi informatici** si moltiplicano e diventano sempre più sofisticati? Quanto lo Stato accompagna concretamente queste realtà produttive nell'investimento – spesso oneroso – in infrastrutture di sicurezza? E soprattutto: gli strumenti messi sul tavolo sono davvero all'altezza della minaccia o stiamo combattendo **ransomware** e **phishing** con armi spuntate?

Publicità
Loading...

24

Per capire quanto e come il sistema pubblico stia aiutando le imprese in questa transizione, **Tinexta** – gruppo specializzato in trasformazione digitale e crescita delle Pmi – tramite le aziende del Gruppo **Tinexta Cyber** e **Tinexta Innovation Hub** ha elaborato per il Sole 24 Ore una mappa dettagliata di **agevolazioni**, contributi, finanziamenti e programmi Ue disponibili tra il 2025 e il 2026 per potenziare la **cybersicurezza** aziendale (si veda la tabella sotto). Perché se è vero che una parte della partita si gioca sulla consapevolezza – riconoscere ed evitare una mail anomala resta essenziale – è altrettanto vero che non basta: senza investimenti in **sicurezza informatica** (sistemi aggiornati, infrastrutture, gestione professionale) il confine tra tentato attacco e disastro resta sottilissimo. La “geografia degli incentivi”, pur rappresentando un punto di svolta, dimostra però un quadro incompleto.

LA MAPPA DEGLI AIUTI

Loading...

Le misure in campo

Il perno è il nuovo **maxi ammortamento 2026** – previsto allo stato dal Ddl di Bilancio –, che aumenta le quote deducibili per beni strumentali nuovi, inclusi software, sistemi e piattaforme per proteggere reti, dati e impianti, secondo gli allegati A e B della legge 232/2016 (legge di Bilancio 2017) in tema cyber. In base al testo attuale del Ddl, vale per investimenti effettuati nel 2026 (con possibile coda al 30 giugno 2027) e prevede **maggiorazioni decrescenti**, ma con intensità massima su investimenti **fino a 2,5 milioni di euro**. È la misura chiamata a rimpiazzare progressivamente **Transizione 4.0 e 5.0**, restando cumulabile con altri incentivi entro il costo del bene.

Novità 24GPT, il tuo assistente di

STRUMENTI
Comparatore di

educazione e
informazione
finanziaria
Scopri di più →

24

tariffe internet casa,
telefonia mobile,
energia, gas e pay
TV
Scopri di più →

24

Sul fronte dei contributi diretti spicca il voucher «Cloud & Cybersecurity» del Mimit (2025), che rimborsa **fino al 50% delle spese** per servizi cloud e soluzioni di sicurezza (Mfa, firewall, cifratura, Siem, backup), con importi tra 4mila e 40mila euro per impresa e una dotazione di circa 150 milioni, rivolto a Pmi e microimprese.

Accanto a queste leve agiscono strumenti finanziari già noti ma orientabili al cyber: **Nuova Sabatini** (contributo in conto interessi su finanziamenti per tecnologie digitali); **finanziamenti Simest** per progetti di digitalizzazione per la competitività internazionale con quota a fondo perduto; **Fondo di garanzia Pmi**, che copre fino all'80% dei prestiti per progetti It, riducendo costi e assorbimento di capitale.

A livello locale, bandi regionali e camerali (ad esempio i Voucher digitali L4.o) coprono audit, consulenze e soluzioni di sicurezza con incentivi **tra il 40% e il 60 per cento**. Nei grandi contratti di sviluppo e nelle Zes/Zls, infine, la componente cyber è finanziabile se integrata nei progetti industriali sopra i 20 milioni di euro.

I nodi da sciogliere

Secondo **Tinexta** Innovation Hub, c'è grande attesa per i nuovi maxi ammortamenti 2026, che possono realmente alleggerire il peso degli investimenti tecnologici sui bilanci aziendali. E si iniziano finalmente a vedere misure specifiche, pensate proprio per la **cybersicurezza** delle Pmi.

Tuttavia, molte agevolazioni – pur citando la **cybersicurezza** tra gli obiettivi – non coprono in modo pieno tutte le spese effettivamente necessarie per garantire livelli adeguati di protezione. Restano spesso ai margini i costi ricorrenti per servizi It, **attività di governance**, **gestione del rischio** e servizi gestiti: elementi ormai indispensabili per un approccio maturo e continuativo alla sicurezza informatica.

Come ricordano gli esperti, la **cybersecurity** non è un intervento “una tantum”, né un progetto che si conclude con la consegna di un software. È un processo continuo, che richiede **prevenzione**, monitoraggio costante e adattamento alle nuove minacce. Se gli incentivi non seguono questa logica, rischiano di mitigare solo parzialmente il problema.

A tutto questo si aggiunge un altro ostacolo ben noto agli imprenditori: la complessità delle procedure e **i tempi di accesso** alle misure. Bandi complicati, documentazione stratificata, finestre temporali ristrette e iter lunghi scoraggiano molte imprese, che spesso non hanno un ufficio interno dedicato solamente a intercettare e gestire incentivi pubblici.

Un quadro, insomma, che dovrà essere modellato. Anche perché c'è un livello più alto che inquieta: le intelligence europee registrano il proliferare di attacchi di natura “statuale”. Sono offensive condotte da Paesi come **Russia, Cina, Corea del Nord, Iran** con l'obiettivo esplicito di

indebolire le economie del continente europeo (secondo la società CrowdStrike l'Italia è tra i primi cinque Paesi europei per numero di attacchi).

Una forma di **guerra ibrida** che colpisce al cuore i sistemi produttivi, con attacchi alle imprese, e mina la fiducia dei cittadini verso le istituzioni, anche attraverso campagne di **disinformazione** che tendono a mitizzare altre economie rivali, come nel caso della Russia. Temi oggetto del Consiglio supremo della difesa della scorsa settimana, presieduto dal presidente della Repubblica, Sergio Mattarella. Si pensi che secondo l'Agenzia per la **cybersicurezza** nazionale, nei primi sei mesi del 2025 gli eventi sono aumentati del 53% rispetto allo stesso periodo dello scorso anno.

Riproduzione riservata ©

ARGOMENTI [incentivo](#) [Il Sole 24 Ore](#) [Russia](#) [Unione Europea](#) [Iran](#)

Per approfondire

Cybersicurezza, la Pubblica amministrazione è il settore più colpito in Italia

24

Cybersecurity, solo sei aziende su cento sono in grado di difendersi

24

Ivan Cimmarusti
redattore

<https://twitter.com/ivancimma?lang=it> [in](#) LinkedIn [Email](#)

Espandi ▾

Loading...

Brand connect

Loading...

I prossimi eventi

24 ORE
EVENTI

Tutti gli eventi →

Newsletter

Notizie e approfondimenti sugli avvenimenti politici, economici e finanziari.

Iscriviti

I video più visti