

L'indispensabile road-book
per rendere sempre più digitale
e competitiva la tua impresa



IN QUESTO NUMERO:

Voucher Cloud & cybersecurity:

150 milioni per innovare e proteggere le imprese

Nuove regole Cloudflare:

verifica se il tuo sito rischia di perdere visibilità

FWA Business fino a 1 Gbps:

più velocità e continuità per le imprese

NIS2:

dal 31 ottobre la sicurezza diventa verificabile





Voucher Cloud e Cybersecurity:

150 milioni per innovare e proteggere le imprese

Non è un semplice incentivo per acquistare tecnologia, ma l'occasione per rinnovare infrastrutture, sicurezza e processi aziendali sostenendo soltanto metà dell'investimento.

È questa la portata del **Voucher Cloud & Cybersecurity** promosso dal Ministero delle Imprese e del Made in Italy.



150 milioni di euro

di dotazione complessiva



PMI e lavoratori autonomi

su tutto il territorio nazionale



fino al 50%

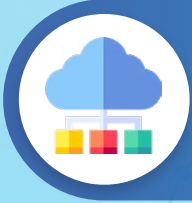
delle spese ammissibili con un massimo di 20.000€ per beneficiario

Dalla protezione dei dati alla digitalizzazione

Il Voucher consente di costruire interventi diversi in base alle effettive priorità dell'impresa.



Sul fronte della cybersecurity possono rientrare **firewall di nuova generazione, sistemi IDS/IPS, antivirus, monitoraggio delle reti**, gestione delle **vulnerabilità, SIEM e crittografia**.



Per aumentare resilienza e continuità operativa sono previsti **virtual machine, storage e backup, VPN, e servizi cloud IaaS e PaaS**.



L'agevolazione comprende anche software **ERP e CRM, soluzioni per contabilità e risorse umane**, strumenti di produttività con **intelligenza artificiale, CMS, e-commerce**, piattaforme di **collaborazione** e **centralini virtuali**.

Servizi inclusi e cosa non è sufficiente

Possono essere inclusi servizi di configurazione, monitoraggio e assistenza continuativa **fino al 30% del piano di spesa.**

Non sono invece sufficienti il semplice rinnovo di una licenza o un aggiornamento privo di un miglioramento sostanziale: l'investimento deve introdurre soluzioni nuove, aggiuntive o più avanzate e sicure



Chi può partecipare

Il piano deve avere un valore minimo di **4.000 euro.**

Il richiedente deve inoltre disporre, al momento della domanda, di una connettività di **almeno 30 Mbps in download** e può presentare **una sola richiesta.**

AllYou S.r.l., società del Gruppo I-TEAM, è iscritta nell'elenco MIMIT dei fornitori abilitati, supporta le imprese nella valutazione dell'infrastruttura, nell'individuazione degli interventi e nella formulazione dell'offerta tecnica. La presentazione della domanda resta a cura dell'impresa o del professionista incaricato.



Calendario



Precompilazione

Il 20 Ottobre 2026 alle ore 12.00



Domande

Dal 10 novembre 2026 fino al 20 gennaio 2027, salvo esaurimento delle risorse.

Poiché saranno valutate in ordine cronologico, attendere l'apertura per iniziare a progettare potrebbe significare arrivare tardi.

Pronti a trasformare l'opportunità in un progetto?

I-TEAM è a disposizione per analizzare le esigenze delle imprese, individuare gli interventi cloud, cybersecurity e digitali più adeguati e predisporre un'offerta tecnica coerente con l'agevolazione. Pianificare l'investimento prima dell'apertura dello sportello significa arrivare preparati e aumentare concretamente le possibilità di accesso al contributo.



Nuove regole CLOUDFLARE:

verifica se il tuo sito rischia di perdere visibilità

Dal 15 settembre 2026 cambierà la gestione dei bot AI e dei crawler utilizzati per l'indicizzazione. Una configurazione non corretta potrebbe influire sulla presenza del sito nei motori di ricerca.



Scadenza chiave
**15 settembre
2026**

Cos'è Cloudflare

Cloudflare è uno dei servizi più utilizzati per proteggere siti e applicazioni web, migliorandone sicurezza, disponibilità e prestazioni. In molti casi viene configurato dal fornitore che gestisce il sito e l'azienda potrebbe quindi utilizzarlo senza esserne pienamente consapevole.

Dal 15 settembre 2026 Cloudflare introdurrà nuove regole per distinguere i crawler impiegati per la ricerca da quelli utilizzati per l'addestramento dei modelli di intelligenza artificiale e per le attività degli agenti AI.

Le tre categorie di traffico automatizzato

SEARCH

Crawler che indicizzano le pagine per renderle disponibili nei risultati di ricerca. Continueranno ad essere autorizzati.

AGENT

Sistemi che accedono a un sito per svolgere attività richieste da un utente. Bloccati per default nei domini con inserzioni pubblicitarie.

TRAINING

Crawler che acquisiscono contenuti per addestrare o perfezionare modelli AI. Bloccati per default nei nuovi domini con inserzioni.

Non basta attivare uno strumento di sicurezza e considerare concluso il lavoro. Le piattaforme **evolvono**, le impostazioni **cambiano**, nascono **nuove categorie di traffico**.

Il rischio dei crawler a uso misto

Googlebot, Applebot e Bingbot possono svolgere attività che non si limitano alla sola indicizzazione. Cloudflare applicherà la regola più restrittiva tra quelle configurate: se nell'account è attivo il blocco dei bot Training, il sistema potrebbe bloccare anche un crawler impiegato per indicizzare le pagine.

Nessuna impostazione vale per tutti

Una configurazione troppo permissiva potrebbe consentire ai sistemi AI di acquisire e riutilizzare i contenuti pubblicati. Una configurazione troppo restrittiva potrebbe invece impedire l'accesso a crawler importanti per la presenza del sito nei motori di ricerca.



Troppo permissivo

I sistemi AI acquisiscono e riutilizzano i contenuti pubblicati.



Troppo restrittivo

I crawler di Google e Bing vengono bloccati, riducendo la visibilità.

La configurazione deve essere valutata considerando insieme sicurezza, indicizzazione e strategia digitale, tenendo conto di:

- ✓ Il valore dei contenuti pubblicati
- ✓ L'importanza del traffico dai motori di ricerca
- ✓ La presenza di informazioni proprietarie
- ✓ Le categorie di bot da autorizzare o bloccare
- ✓ Gli obiettivi commerciali e di visibilità del sito

Un processo continuo, non una tantum

Il cambiamento annunciato da Cloudflare evidenzia un principio fondamentale: non basta attivare uno strumento di sicurezza e considerare concluso il lavoro. Una configurazione corretta al momento dell'attivazione potrebbe non essere più adeguata dopo alcuni mesi.



Verifica gratuita GlobalNet Italia & I-Team

Molte aziende potrebbero non sapere se il proprio sito utilizza Cloudflare o quali impostazioni siano attualmente configurate.

GlobalNet Italia e il gruppo I-Team mettono a disposizione una consulenza gratuita per verificare:

- Se il sito utilizza Cloudflare ←
- Le regole applicate ai crawler e ai bot AI ←
- I possibili effetti delle modifiche previste ←
- dal 15 settembre
- Eventuali rischi per l'indicizzazione e la ←
- visibilità online
- L'adeguatezza della configurazione di ←
- sicurezza attuale

La sicurezza non è una configurazione da effettuare una sola volta, ma un processo da controllare e aggiornare nel tempo.

I-TEAM

FWA Business fino a 1 Gbps:

più velocità e continuità per le imprese

La tecnologia Fixed Wireless Access compie un ulteriore salto di qualità. Ora raggiunge velocità fino a 1 Gbps, aprendo nuovi scenari per le imprese.

Una tecnologia già consolidata

La Fixed Wireless Access permette di collegare una sede aziendale attraverso un'antenna installata presso l'edificio, utilizzando una rete radio in alternativa al collegamento fisico in fibra. È già utilizzata da molte aziende, soprattutto nelle zone non raggiunte dalla FTTH, nei territori periferici e nelle aree produttive dove la realizzazione di un collegamento cablato può richiedere tempi più lunghi.

La novità non è quindi la FWA in sé, già presente tra le soluzioni di GlobalNet Italia, ma la sua evoluzione tecnologica e prestazionale: grazie a tecnologie radio più avanzate, frequenze licenziate e infrastrutture di nuova generazione, il collegamento può ora raggiungere velocità fino a 1 Gbps.

• L'attivazione rimane subordinata
• alla copertura e alla verifica del-
• la fattibilità radio presso la sede
• interessata.
•

Velocità fino a

1 Gbps

Fixed Wireless
Access Business

Applicazioni supportate dalla nuova FWA

Scenari di utilizzo abilitati a 1 Gbps

Applicazioni cloud aziendali ←

Centralini VoIP ←

Videoconferenze ad alta qualità ←

VPN aziendali ←

Sistemi gestionali e ERP ←

Servizi ad alta capacità di
trasmissione ←



Dove la FWA è la soluzione ideale

Zone non raggiunte dalla fibra FTTH

Territori periferici e aree produttive

Nuove sedi da collegare rapidamente

Sedi in attesa di attivazione della
linea cablata

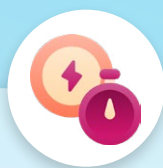


La flessibilità come punto di forza



Accesso principale

Nelle aree in cui la fibra non è disponibile, la FWA fino a 1 Gbps offre prestazioni adeguate anche alle imprese più esigenti.



Soluzione temporanea

Permette di collegare rapidamente nuove sedi o di mantenere l'operatività in attesa dell'attivazione di una linea cablata.



Linea di backup

Affiancata a una linea FTTH o altra tecnologia, riduce il rischio che un singolo guasto interrompa completamente l'operatività.

ATTENZIONE: Il backup non è automatico



Disporre di due collegamenti non garantisce da solo la continuità operativa. Per un failover efficace sono necessari:

- ✔ Appareti configurati per il failover automatico
- ✔ Monitoraggio costante di entrambe le linee
- ✔ Verifiche periodiche del funzionamento della linea secondaria

GlobalNet Italia & Gruppo I-Team

La FWA Business fino a 1 Gbps rappresenta un'importante evoluzione di un servizio già disponibile, offrendo maggiori prestazioni, rapidità di attivazione e nuove opportunità per garantire la continuità operativa delle imprese.

L'approccio del Gruppo I-Team

Una connettività integrata e su misura

All'interno del Gruppo I-Team, GlobalNet Italia integra più tecnologie di connettività per progettare collegamenti principali e soluzioni di backup adeguati alle esigenze specifiche di ogni impresa.

Le tecnologie disponibili

Aggiornamento

FWA

Fixed Wireless Access fino a 1 Gbps. Radio, senza posa in opera.

Disponibile

FTTH

Fibra fino all'edificio. Massime prestazioni dove disponibile.

Disponibile

FTTC

Fibra fino all'armadio. Soluzione consolidata nelle aree miste.

Disponibile

Mobile

Connettività 4G/5G per backup o sedi in mobilità.

La **continuità operativa** non dipende da una sola tecnologia, ma da come le diverse soluzioni vengono **integrate e monitorate nel tempo**.



NIS2:

dal 31 ottobre la sicurezza diventa verificabile

Non è l'ultimo giorno per adeguarsi: è il momento da cui le organizzazioni devono essere pronte a dimostrare che le misure di sicurezza adottate sono operative e documentate.



Scadenza chiave
**31 ottobre
2026**

La vera scadenza viene prima

Per i soggetti del primo elenco NIS, il termine per l'adozione delle misure è collegato ai 18 mesi successivi alla comunicazione ricevuta dall'Agenzia per la Cybersicurezza Nazionale.

Arrivare a ottobre con policy appena approvate o strumenti da configurare potrebbe non essere sufficiente. ACN potrà verificare non soltanto l'esistenza delle misure, ma anche la loro applicazione.

• **Il 1° novembre non sarà il momento di iniziare: sarà il momento di poter dimostrare quanto è già stato fatto.**

La conformità non è solo sulla carta

-  Un backup mai ripristinato non dimostra la capacità di recuperare i dati
-  Un piano di continuità mai testato non garantisce la prosecuzione delle attività
-  Una procedura di gestione degli incidenti senza registrazioni non è verificabile

Misura > Evidenza richiesta

- 1 Analisi dei rischi**
Registri delle valutazioni e aggiornamenti periodici documentati
- 2 Gestione accessi**
Log, responsabilità assegnate, revisioni periodiche dei permessi
- 3 Backup**
Test di ripristino effettuati e registrati con esito verificabile
- 4 Continuità operativa**
Piano testato, verbali delle simulazioni, azioni correttive intraprese
- 5 Risposta incidenti**
Procedure documentate, registrazioni degli eventi gestiti
- 6 Protezione reti/dati**
Controlli periodici, report, azioni correttive documentate



La conformità si misura attraverso verbali, registri, controlli periodici, test effettuati, responsabilità assegnate e azioni correttive. Sono queste evidenze a dimostrare che la sicurezza non è rimasta sulla carta.



Non solo i soggetti NIS

Effetti a cascata sulla filiera

La NIS2 produce conseguenze anche per imprese non direttamente inserite nell'elenco ACN. I soggetti NIS devono valutare la sicurezza della propria catena di approvvigionamento e l'affidabilità dei fornitori che possono incidere sulla continuità dei processi.



I-TEAM

Dal 1° novembre: vigilanza e sanzioni

Decorso il termine applicabile, ACN potrà esercitare le attività di vigilanza previste dal Decreto NIS.

Eventuali carenze potranno determinare richieste di adeguamento, provvedimenti correttivi e, in presenza di violazioni, l'applicazione delle relative sanzioni.

Il supporto I-Team per la conformità NIS2

Il supporto comprende un percorso strutturato che accompagna l'impresa dall'analisi iniziale fino all'adeguamento operativo:

- | | |
|----------------------------------|-----------------------------|
| → Analisi di applicabilità | → Pianificazione interventi |
| → Valutazione delle carenze | → Protezione reti e dati |
| → Definizione adempimenti | → Backup e continuità |
| → Predisposizione documentazione | → Monitoraggio e accessi |



La conformità NIS2 non si dimostra con le intenzioni, ma con le evidenze: documenti, test, registri e controlli che attestano una sicurezza reale e operativa.



I·TEAM

Cinque società che si sono unite per dare forma ad un grande progetto: aiutare le imprese a crescere nella digitalizzazione e nella rivoluzione digitale, per avere performance sempre più efficaci ed efficienti, all'altezza dei grandi cambiamenti dell'economia e della società contemporanea.

 Allyou.srl

 ego
communication

 GLOBALNET
ITALIA

 OMEGASISTEMI
Soluzioni Informatiche Professionali

 PANTAREI INFORMATICA
La tecnologia resa semplice

www.i-team.tech

project by Allyou.srl

Via Benedetto Dei 64 • 50127 FIRENZE • Numero Verde 800-199760 • info@i-team.tech