




# Ingegneri e approccio alla cybersecurity Indagine campionaria

*Febbraio 2022*



# L'indagine sulla cybersecurity— Sintesi dei risultati

L'indagine è stata promossa dal Comitato C3I e realizzata con il supporto del Centro Studi CNI nel mese di novembre 2021.


Il questionario a risposte chiuse è stato somministrato on line agli iscritti all'Albo degli Ingegneri. I questionari ritenuti validi, perché compilati correttamente, sono stati 4805.

L'obiettivo dell'indagine è stato di analizzare l'approccio degli ingegneri al tema della cybersecurity, le modalità d'uso agli strumenti per la sicurezza informatica, l'approccio ai problemi e alle soluzioni ad essa connessi.

I rispondenti si dividono in due macrogruppi: da un lato chi esercita in via esclusiva la libera professione e dall'altro chi affianca a questa un lavoro dipendente presso una Azienda o un Ente pubblico. Tra i rispondenti, ovviamente, vi è anche chi svolge solo lavoro dipendente. In linea generale, chi svolge un lavoro dipendente ha un atteggiamento leggermente più «evoluto» o un approccio «più dinamico o innovativo» rispetto ai temi complessi della cybersecurity, così come lo stesso può dirsi per gli ingegneri collocati nella fascia di età «intermedia», ovvero tra i 30 ed i 50 anni, mentre sia i più giovani che i più anziani rivelano generalmente un interesse ancora relativamente limitato verso il tema.

L'indagine è divisa sostanzialmente in due parti. In un primo caso sono stati posti dei quesiti legati alla gestione della cybersecurity nell'esercizio della libera professione (le domande sono state somministrate a liberi professionisti full time e a liberi professionisti che hanno anche un lavoro dipendente). Nella seconda parte invece sono state poste domande solo agli ingegneri che hanno un lavoro dipendente, fondamentalmente per capire se essi conoscono come la struttura di appartenenza affronta la questione della cybersecurity.

In linea generale sembra emergere un livello di «alfabetizzazione» - a questo tema di grande attualità - abbastanza elevato, sebbene non manchino alcuni elementi di debolezza. Dai dati emerge, inoltre, che gli ingegneri che operano in ambito informatico hanno un approccio, per così dire, più avanzato al tema, mentre ad esempio il libero professionista che opera in ambito civile-edile o ambientale rivela minore interesse per l'argomento o adotta ancora un numero limitato di strumenti nell'ambito della cybersecurity.



# L'indagine sulla cybersecurity— Sintesi dei risultati

---

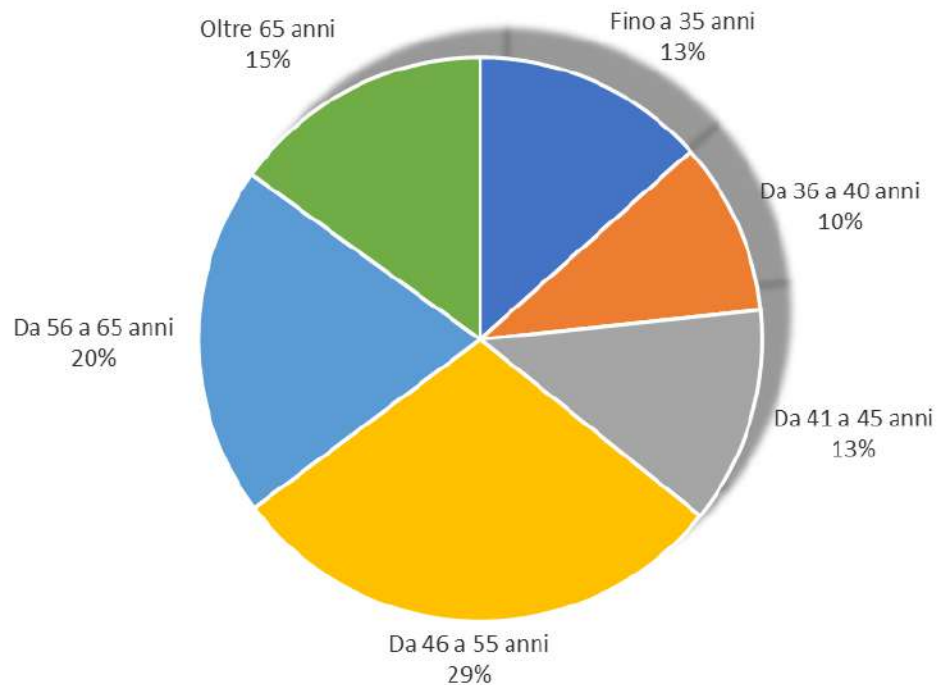
Un aspetto interessante che emerge dall'indagine riguarda la rapida diffusione dell'accesso da remoto tramite VPN ai documenti e file di lavoro. E' probabile che la pandemia iniziata nel 2020 abbia accelerato tale processo anche tra gli studi professionali sebbene sia «dirimente» l'ambito ingegneristico in cui i singoli professionisti operano. E' infatti dotato di collegamento VPN il 66% di chi opera nell'ingegneria dell'informazione a fronte del 30% di chi opera in ambito civile-edile-ambientale. E' chiaro che occorrerebbe comprendere meglio quanto l'accesso a distanza a file di lavoro sia realmente utile e praticabile per chi opera in ambito civile-edile ed ha spesso a che fare con disegni tecnici o con dossier particolarmente voluminosi di difficile consultazione immediata direttamente dal PC. Resta il fatto che molti, soprattutto in alcuni ambiti di specializzazione, non sanno neanche cosa sia una VPN, per cui un'operazione di sensibilizzazione, soprattutto tra gli studi professionali, sulle potenzialità della rete e sui servizi in rete risulterebbe utile.

Vi è un secondo aspetto che emerge sia tra chi opera nella libera professione che tra coloro i quali hanno un lavoro dipendente: gli strumenti di prevenzione e contrasto a possibili minacce informatiche sono, nei casi più diffusi, ad un livello per così dire basic. Anche in questo caso, soprattutto i liberi professionisti (che spesso non fanno ricorso a specialisti del settore) dovrebbero ricevere informazioni adeguate sia sulle principali minacce che sui principali strumenti di tutela da tali minacce.

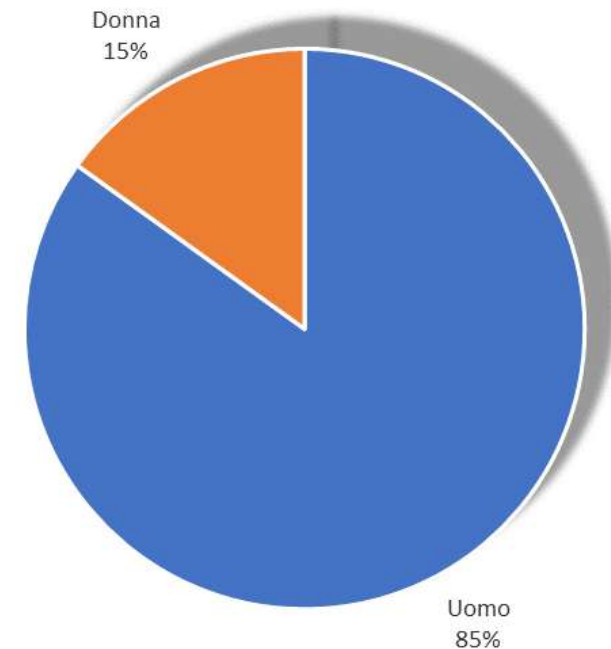
# Caratteristiche del campione di 4.449 rispondenti

---

Distribuzione del campione per classe d'età dei rispondenti



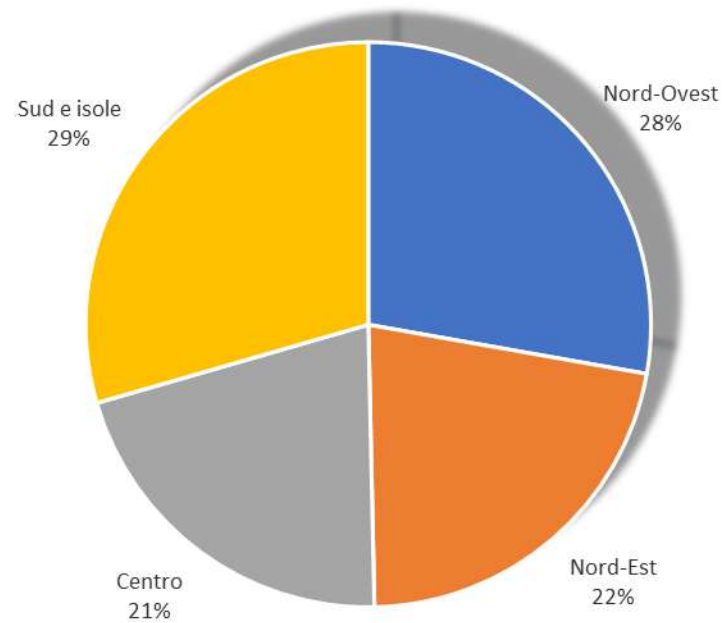
Distribuzione del campione per sesso dei rispondenti



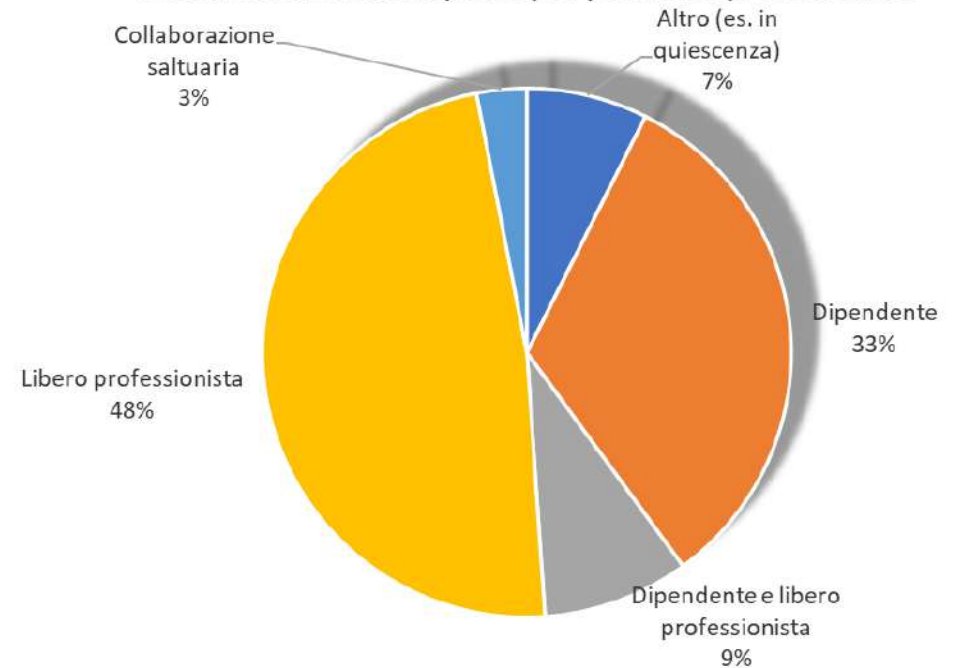
# Caratteristiche del campione

---

Distribuzione del campione area geografica di residenza

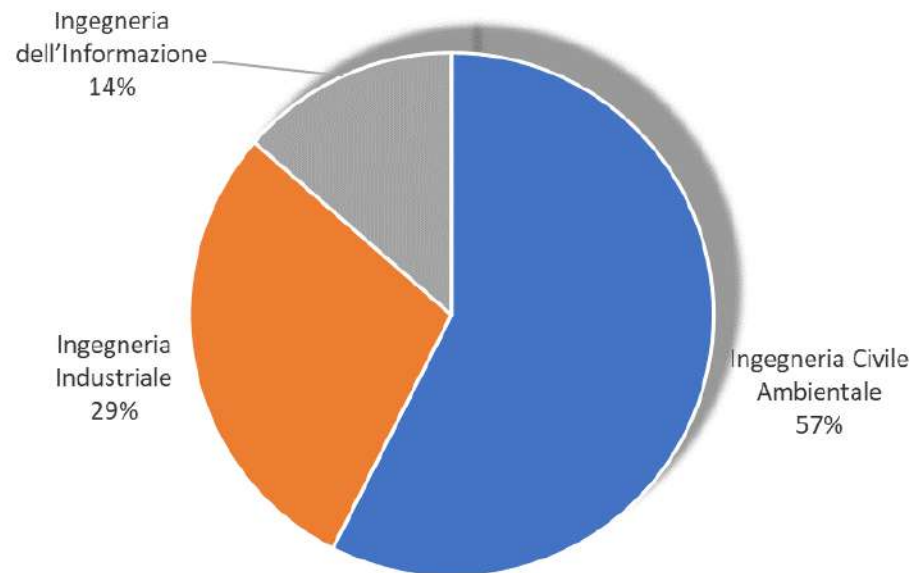


Distribuzione del campione per posizione professionale

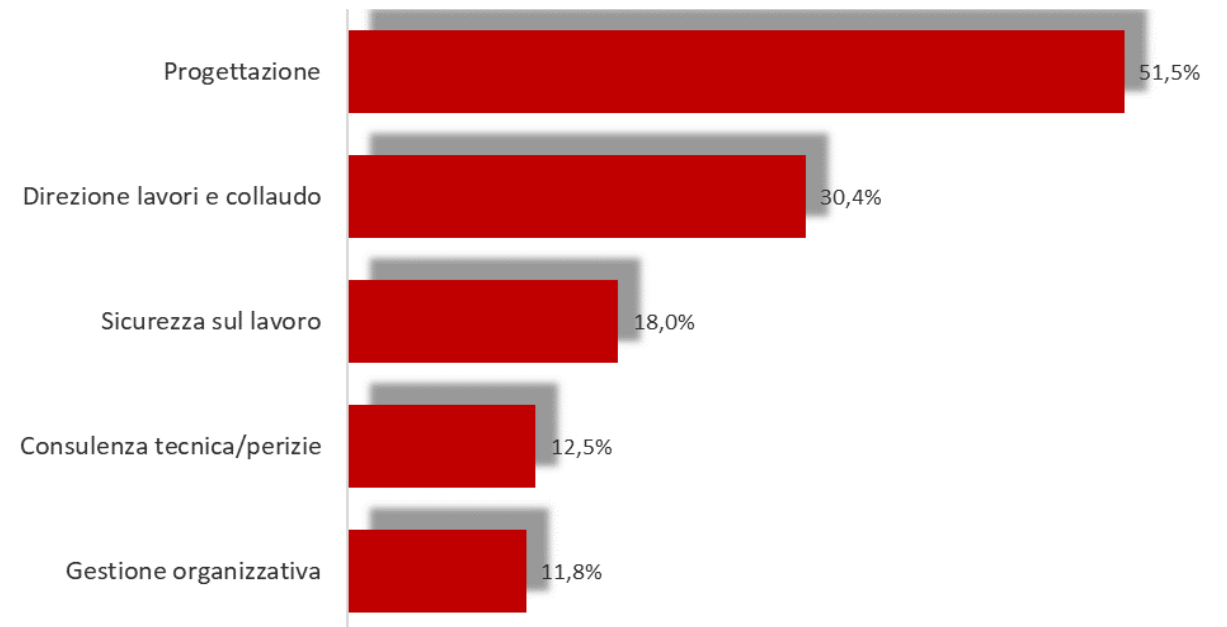


# Caratteristiche del campione

Ambito di attività prevalente degli intervistati



Attività in ambito ingegneristico più diffuse tra gli intervistati



An abstract background on the left side of the slide, featuring a dark tunnel-like perspective with multiple curved light trails in shades of orange, red, and white, creating a sense of motion and depth.

# Approccio alla cybersecurity

---

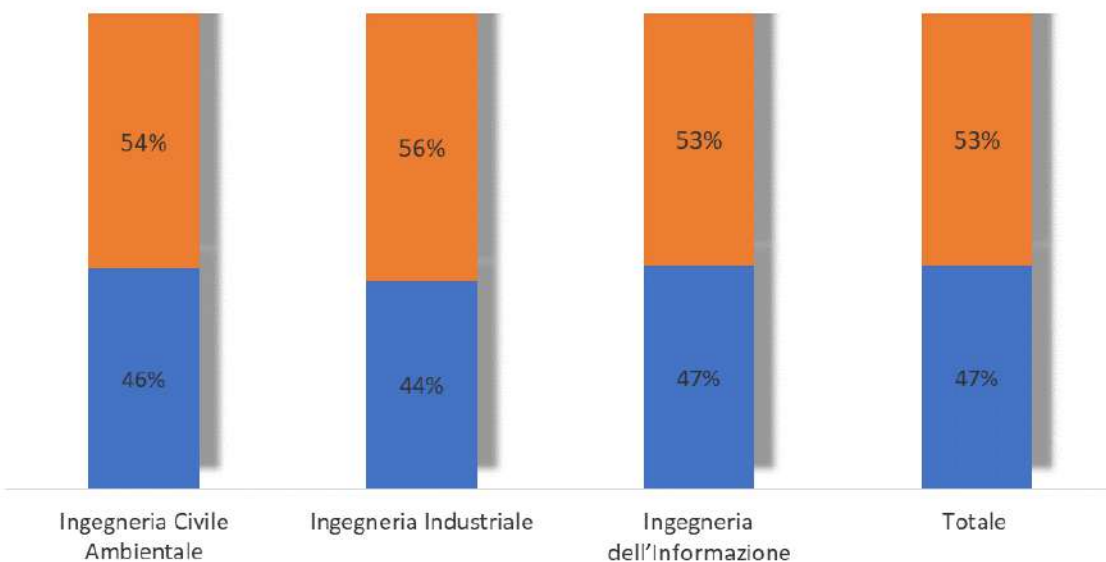
## Parte 1

Risposte degli Ingegneri liberi  
professionisti  
(liberi professionisti in via esclusiva  
e liberi professionisti che hanno  
anche un lavoro dipendente)

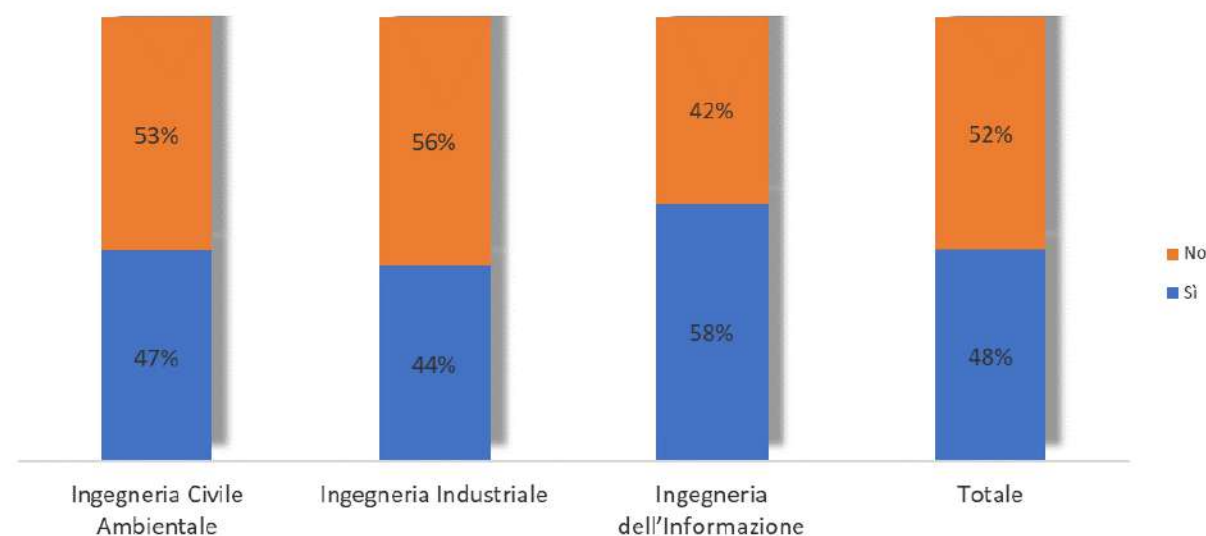
2.573 rispondenti

Meno della metà degli studi professionali ha predisposto l'informativa essenziale per il trattamento dei dati personali del cliente. Tra chi opera nell'ambito dell'ingegneria dell'informazione si riscontra un approccio più avanzato su questo aspetto

Nell'ambito dell'attività di lavoro autonomo ha predisposto i documenti per i clienti sull'informativa per il trattamento dati personali?



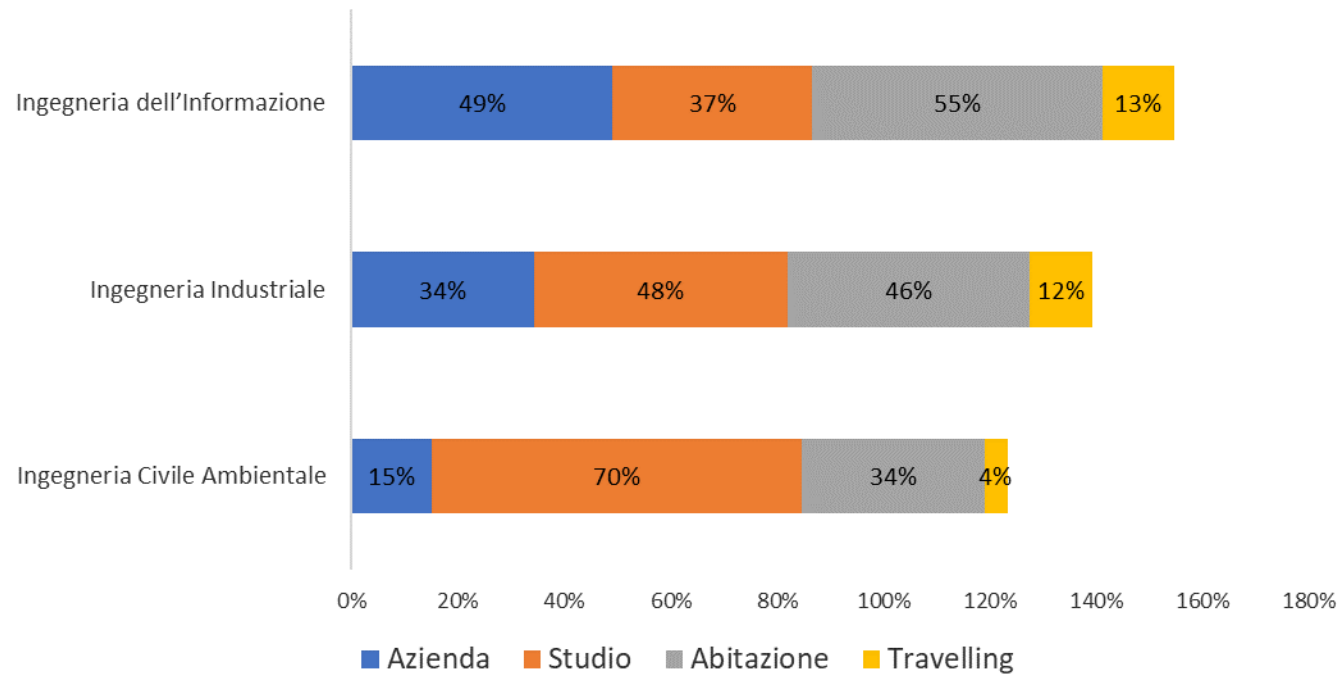
Nell'ambito dell'attività di lavoro autonomo ha predisposto i documenti per il consenso al trattamento dati personali dei clienti?





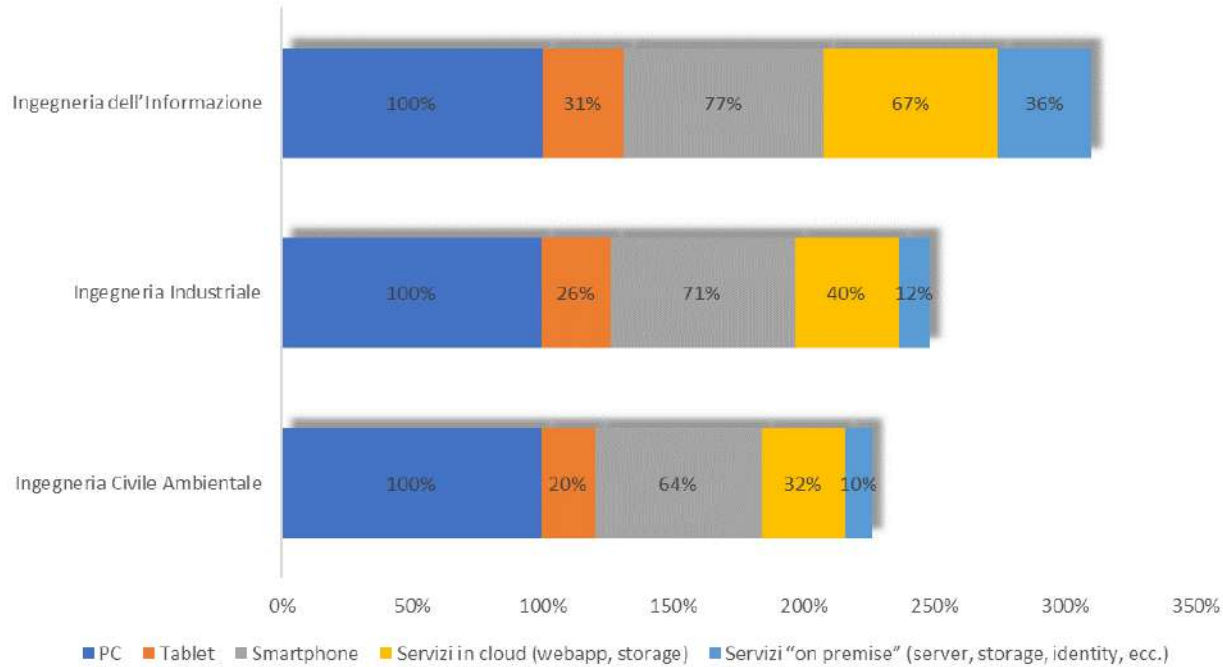
Gli spazi di lavoro cambiano a seconda dell'ambito di lavoro. Lo studio è prevalente tra gli ingegneri civili-ambientali, mentre per chi opera in ambito industriale e dell'informazione il mix è più vario

Spazi in cui gli ingegneri svolgono in prevalenza l'attività lavorativa, risposte in %

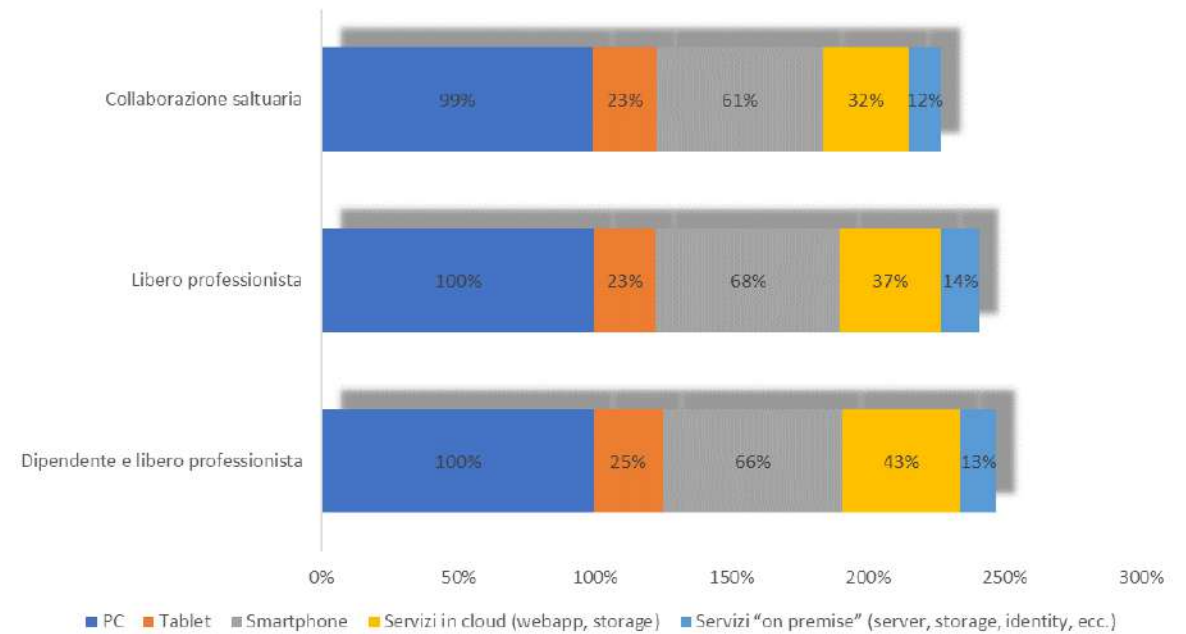


I servizi in cloud e quelli «on premise» sembrano essere quasi prerogativa dei soli ingegneri che operano nel settore dell'informazione, negli altri settori il fabbisogno di questi strumenti è ancora piuttosto latente

Strumenti di lavoro utilizzati abitualmente, risposte in %

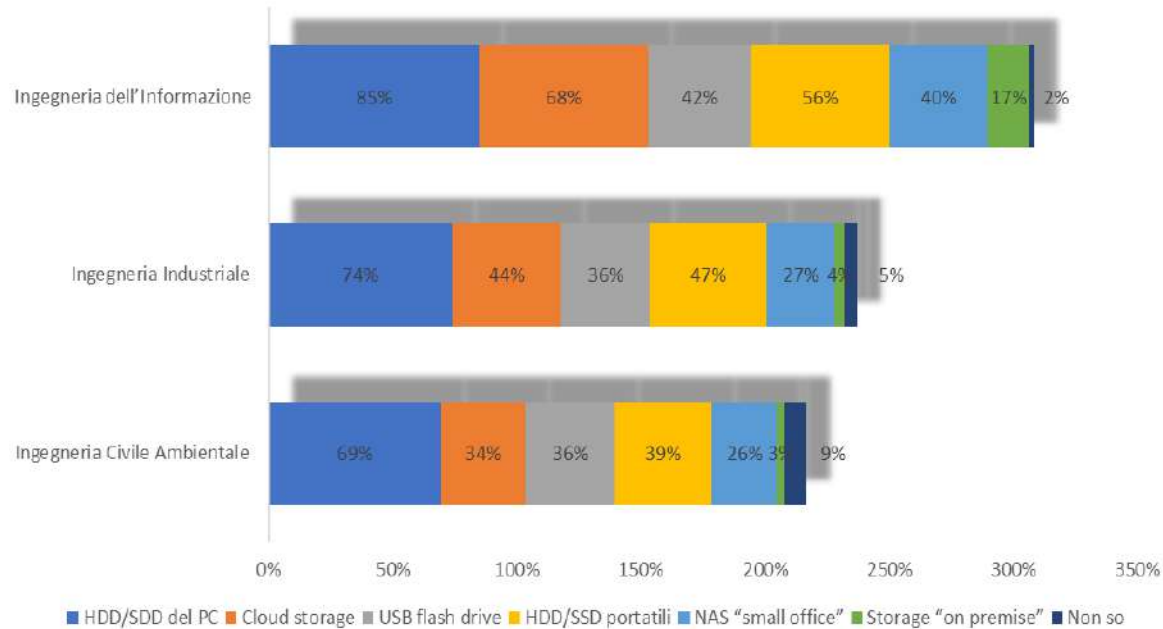


Strumenti di lavoro utilizzati abitualmente, risposte in %

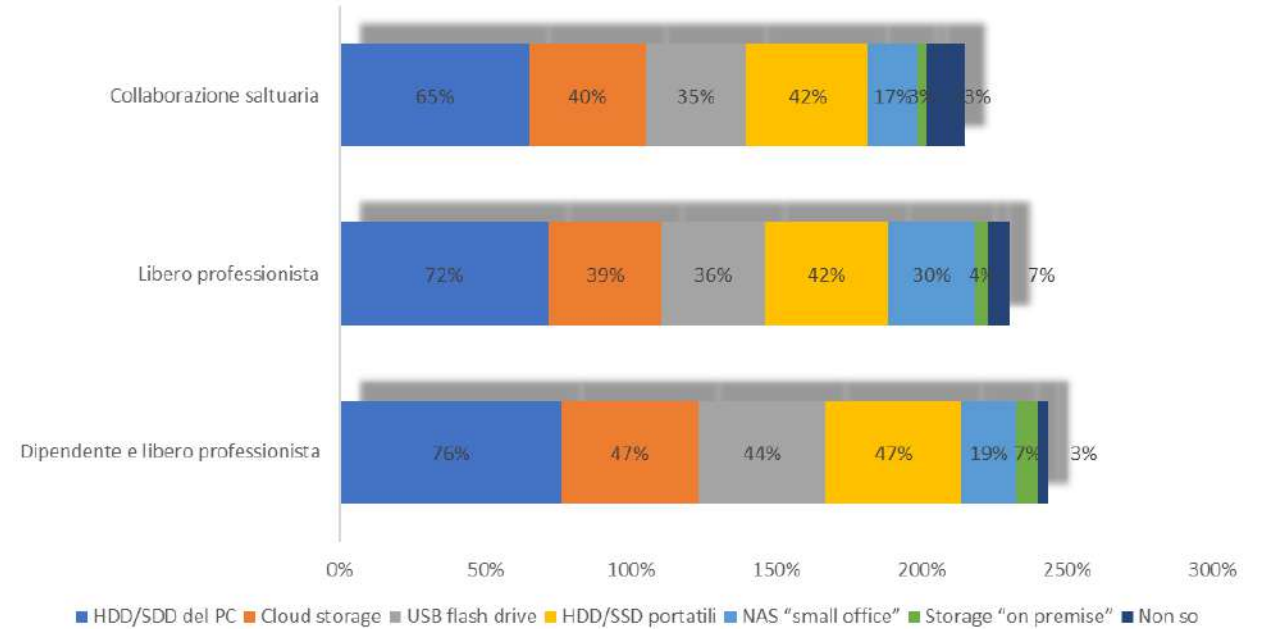


Tra i sistemi di archiviazione dati quelli su cloud iniziano a diffondersi, mentre forme più evolute come lo storage on premise sono più rari. Sono relativamente pochi gli ingegneri che non conoscono nessuno degli strumenti presi in considerazione

Sistemi di storage dei dati utilizzati dagli ingegneri che svolgono la libera professione, risposte in %

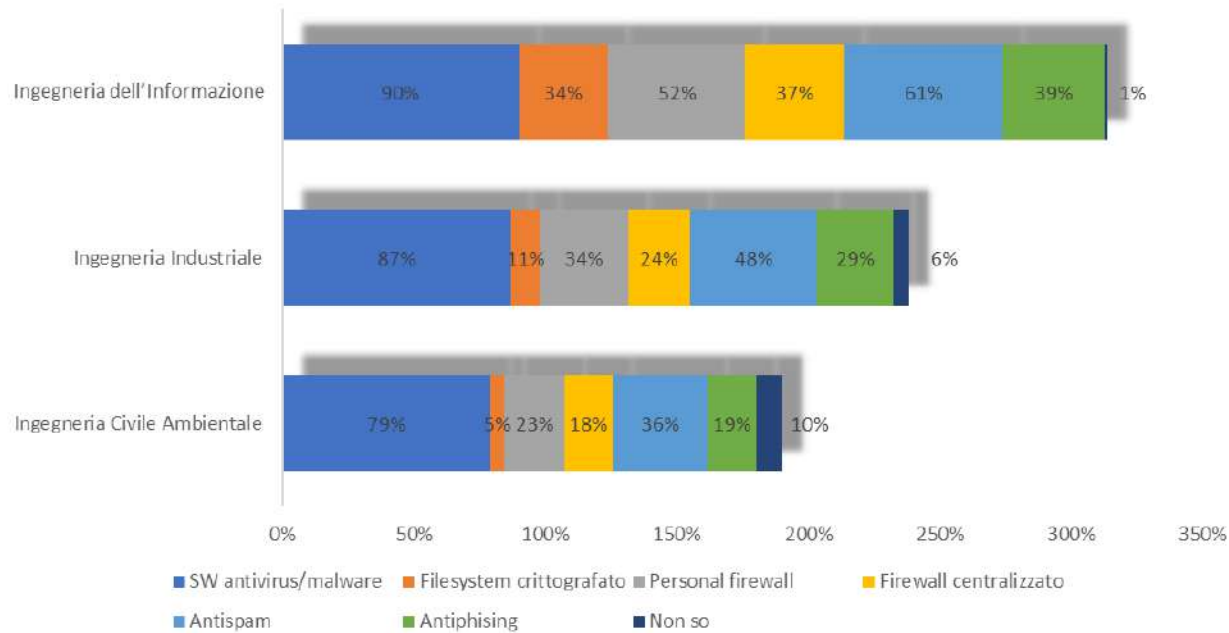


Sistemi di storage dei dati utilizzati dagli ingegneri che svolgono la libera professione, risposte in %

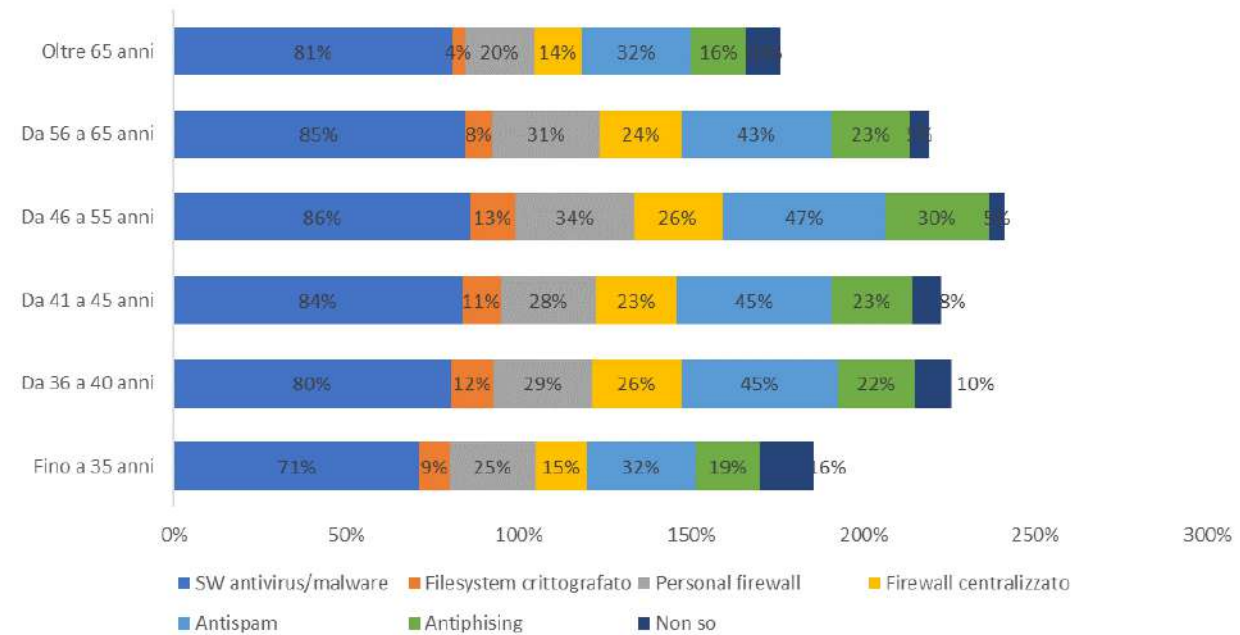


# Se si escludono i software antivirus e l'antispam, gli altri strumenti per la sicurezza sono relativamente poco diffusi

Strumenti per la cybersecurity utilizzati dagli ingegneri che svolgono la libera professione, risposte in %

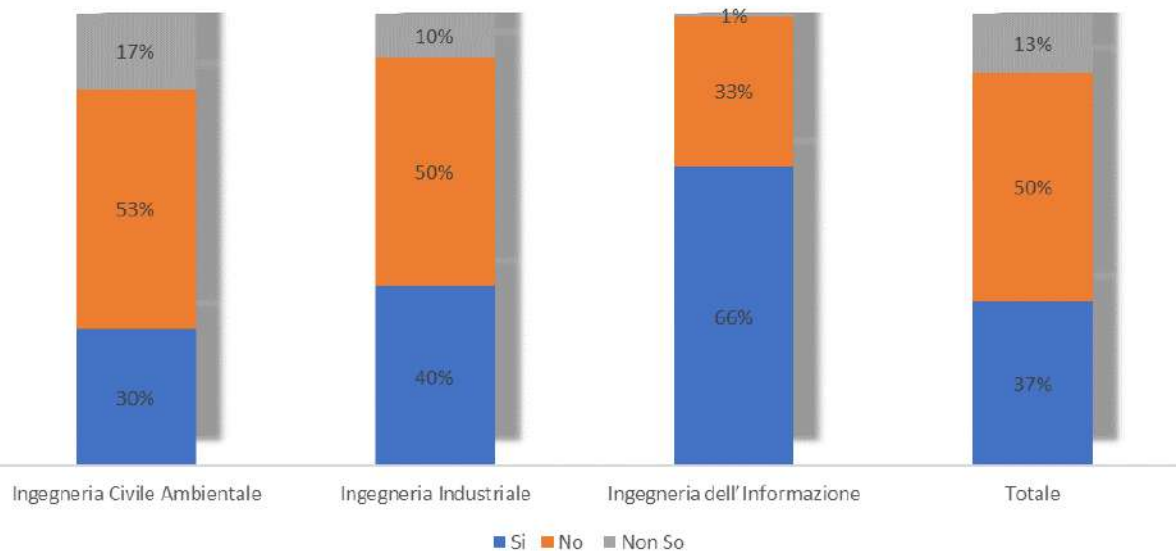


Strumenti per la cybersecurity utilizzati dagli ingegneri che svolgono la libera professione, risposte in %

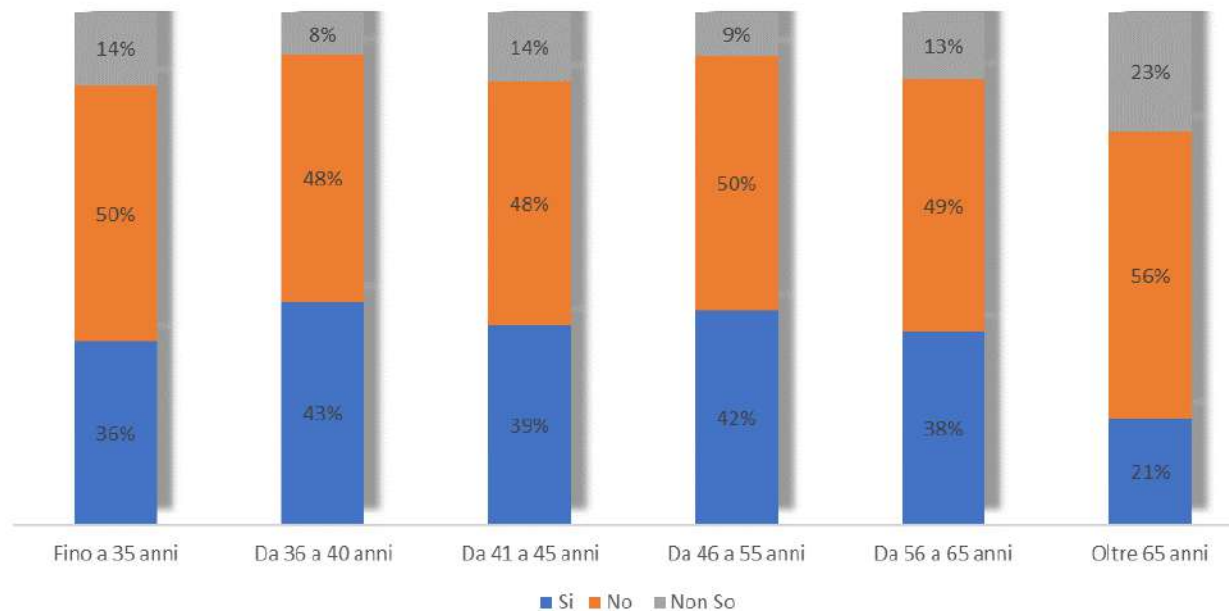


Sul collegamento da remoto con VPN emerge una certa confusione. Il 13% non sa se ne dispone o meno. L'accesso ai file di lavoro con VPN è più diffuso tra gli ingegneri dell'informazione mentre scende drasticamente tra gli ingegneri industriali e civili-ambientali. Occorrerebbe verificare però quanto effettivamente per un professionista sia praticabile lavorare da remoto per valutare veramente le regioni di alcune risposte ottenute nell'indagine

Professionisti con accesso da remoto tramite VPN

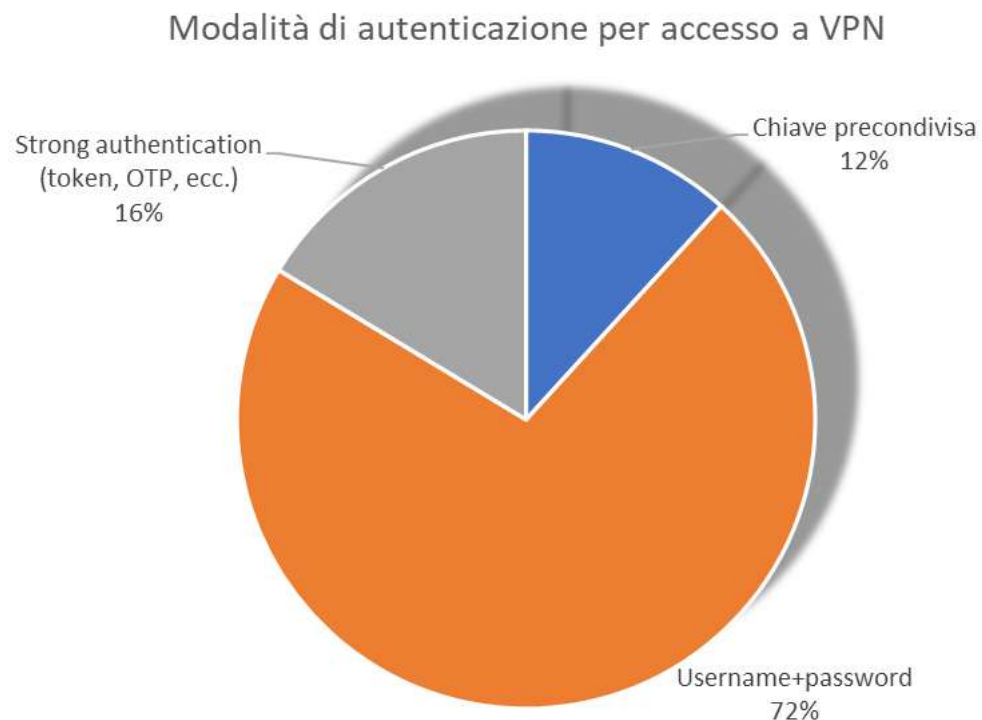


Professionisti con accesso da remoto tramite VPN



# Modalità di autenticazione alla VPN. Le chiavi di accesso più sicure sono prerogativa di una minoranza di ingegneri

---

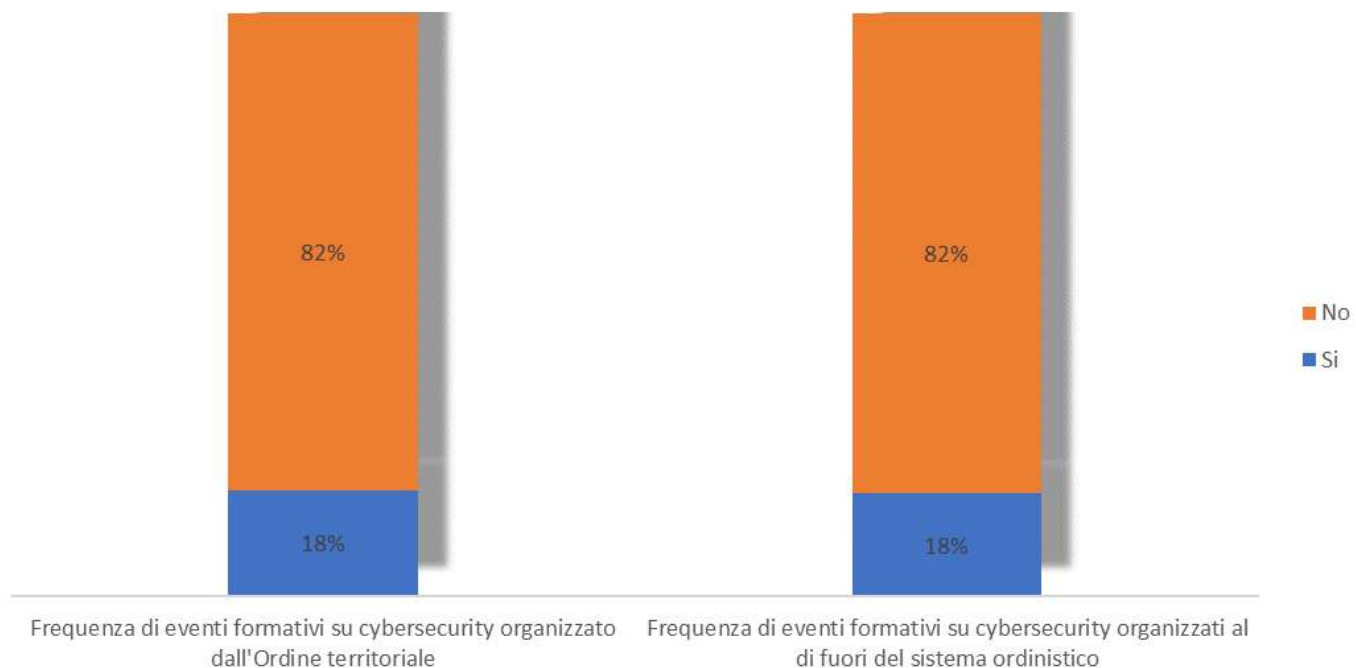


Se da un lato sono pochi gli ingegneri che hanno un accesso da remoto ai file di lavoro (37%), il livello di sicurezza legato a tale accesso appare piuttosto basso tenendo conto che in molti casi la VPN consente l'accesso a documentazione di lavoro o riguardante i clienti.

# Solo il 18% degli intervistati si è aggiornato sui temi della sicurezza informatica

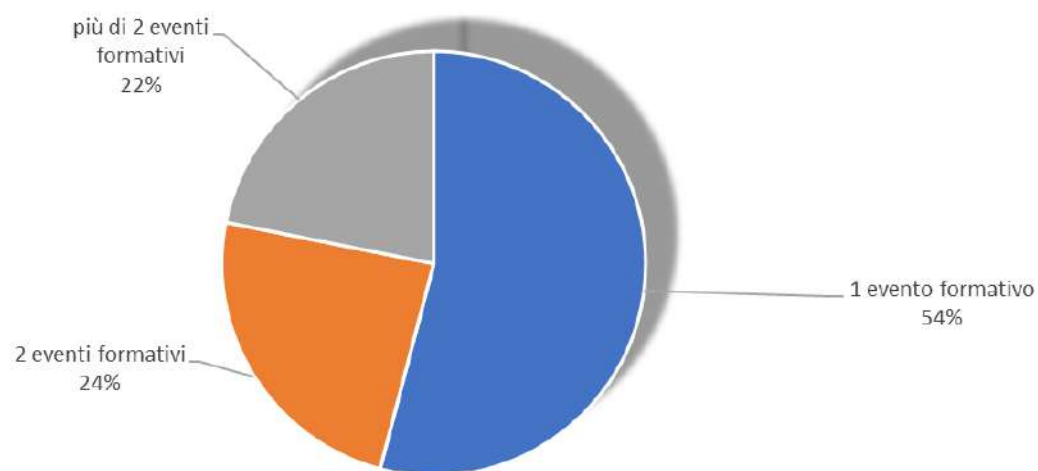
---

% di ingegneri che ha frequentato eventi in materia di sicurezza informatica nell'ultimo anno

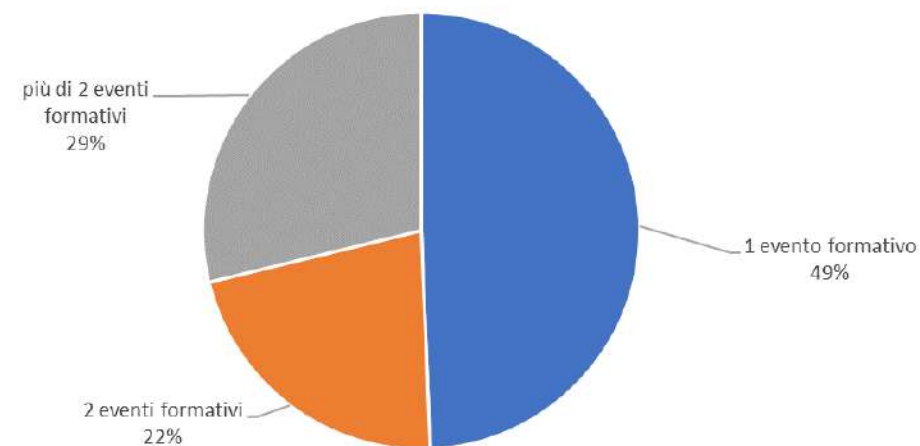


# Numero di eventi formativi frequentati in materia di cybersecurity nell'ultimo anno

Eventi formativi in materia di cybersecurity organizzati dall'Ordine territoriale frequentati nell'ultimo anno



Eventi formativi in materia di cybersecurity fuori dal canale ordinistico frequentati nell'ultimo anno





An abstract background on the left side of the slide, featuring a series of curved, glowing light trails in shades of orange, red, and white, creating a sense of motion and depth.

# Approccio alla cybersecurity

---

## Parte 2

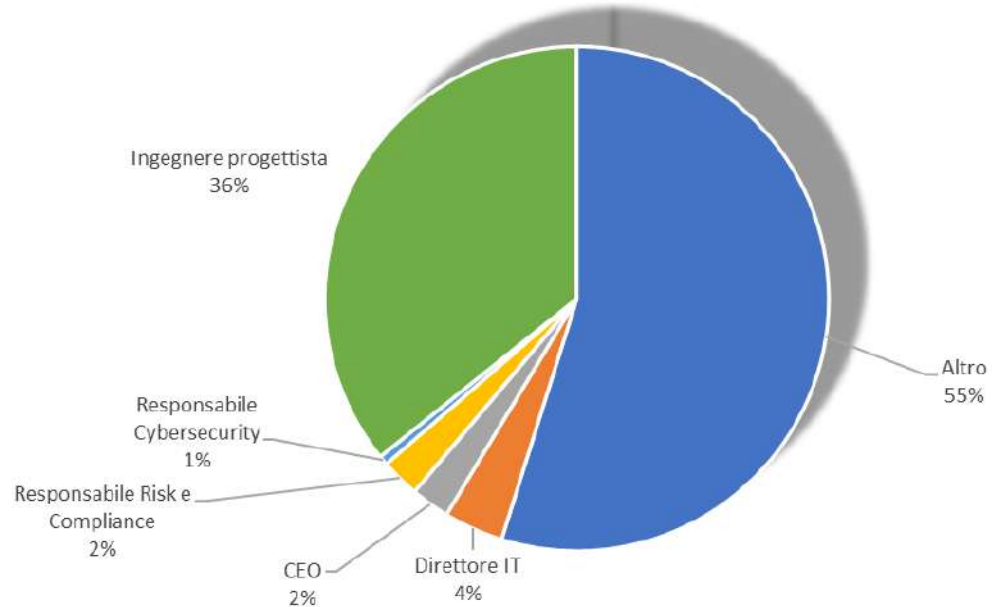
Risposte degli ingegneri che svolgono un lavoro dipendente (lavoro dipendente in via esclusiva o lavoro dipendente associato alla libera professione)

1647 rispondenti

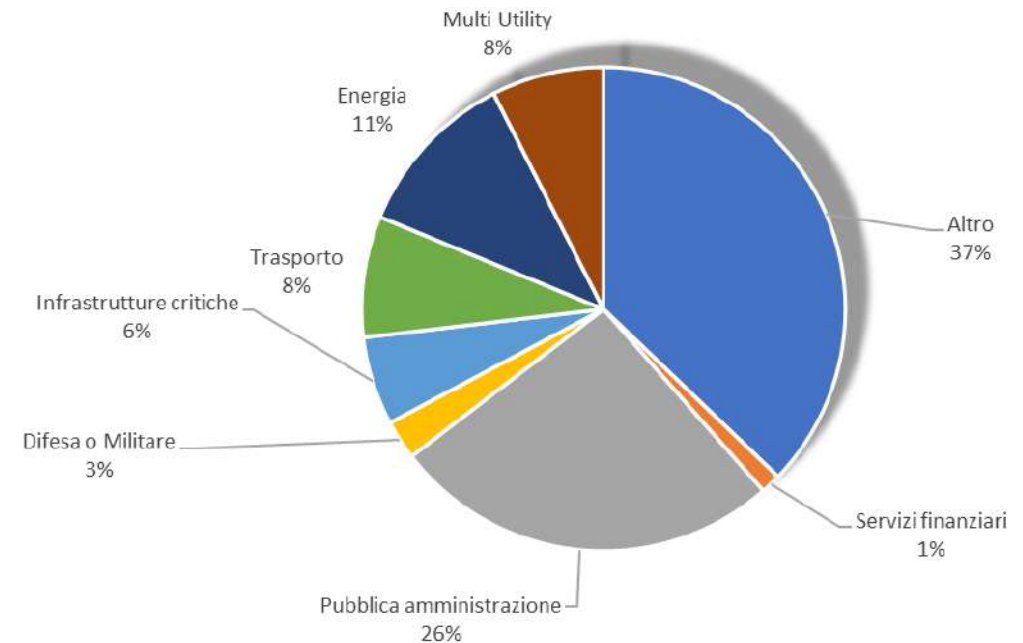
(non tutti i liberi professionisti con lavoro dipendente hanno completato la seconda parte del questionario)

# Posizione ricoperta e ambito di attività degli ingegneri intervistati

Ruolo ricoperto in azienda dagli ingegneri che svolgono lavoro dipendente in via esclusiva o lavoro dipendente e libera professione

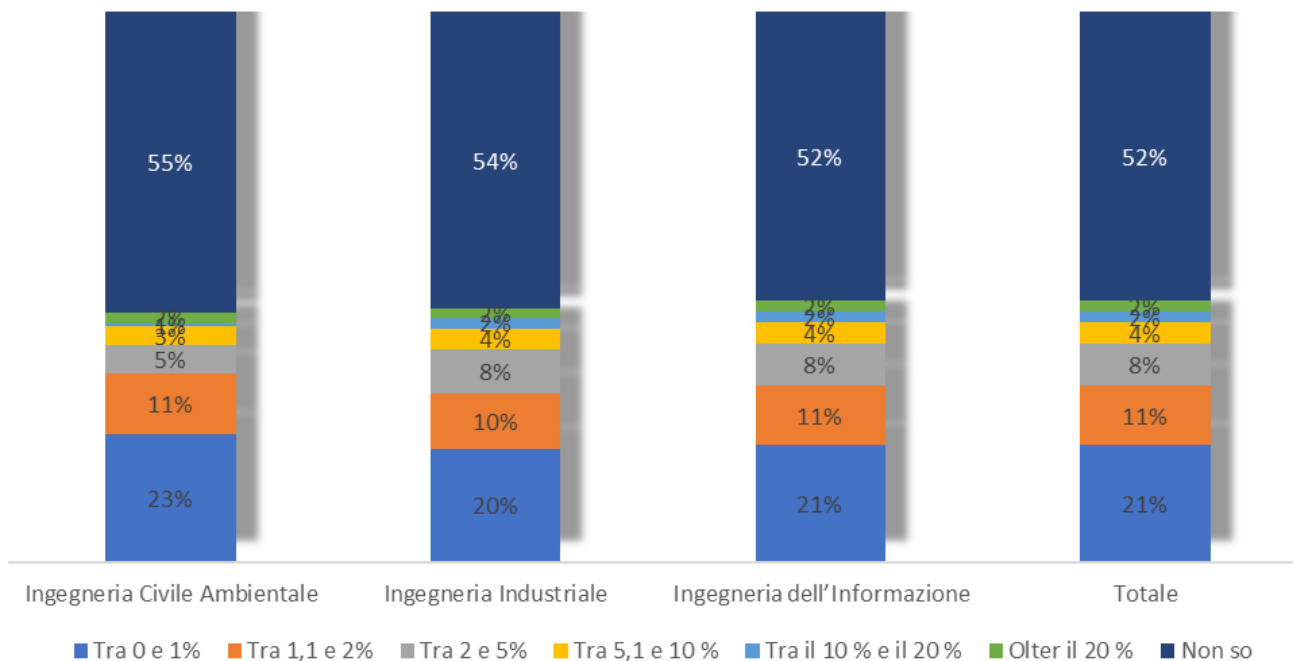


Settore in cui operano gli ingegneri che svolgono lavoro dipendente in via esclusiva o lavoro dipendente e libera professione



# Più della metà degli intervistati non sa se nella propria organizzazione vi è un budget dedicato ad interventi per la sicurezza informatica

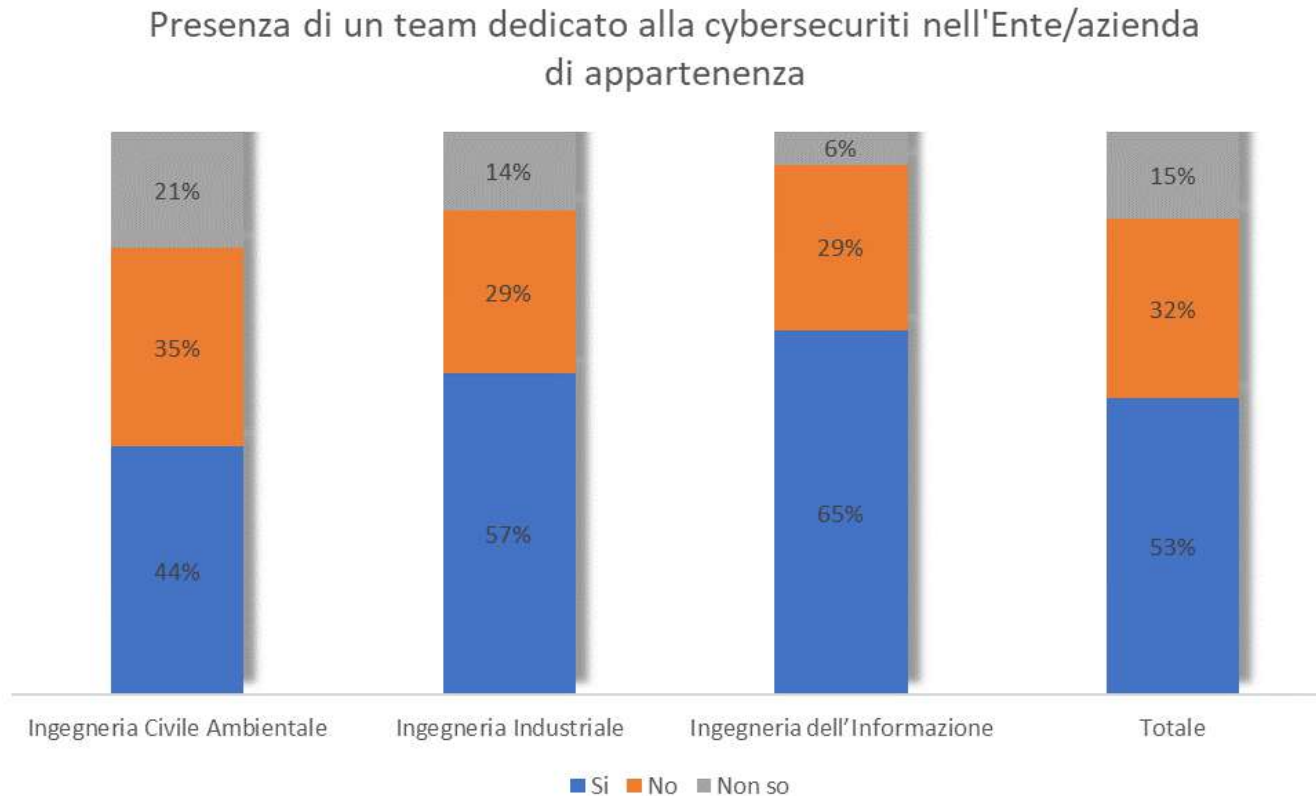
% del budget dell'organizzazione di appartenenza spesa per cybersecurity



Il fatto che una parte cospicua degli intervistati abbia dichiarato di non conoscere se nella propria organizzazione vi sia un budget per la cybersecurity dovrebbe essere soppesato con cura: potrebbe essere fisiologico, essendo la gestione della sicurezza informatica demandata ad altri gruppi di lavoro in cui gli intervistati non operano.

Dall'indagine risulta che la quota media di spesa per la cybersecurity è piuttosto contenuta: per il 21% non va oltre l'1% del budget di spesa generale.

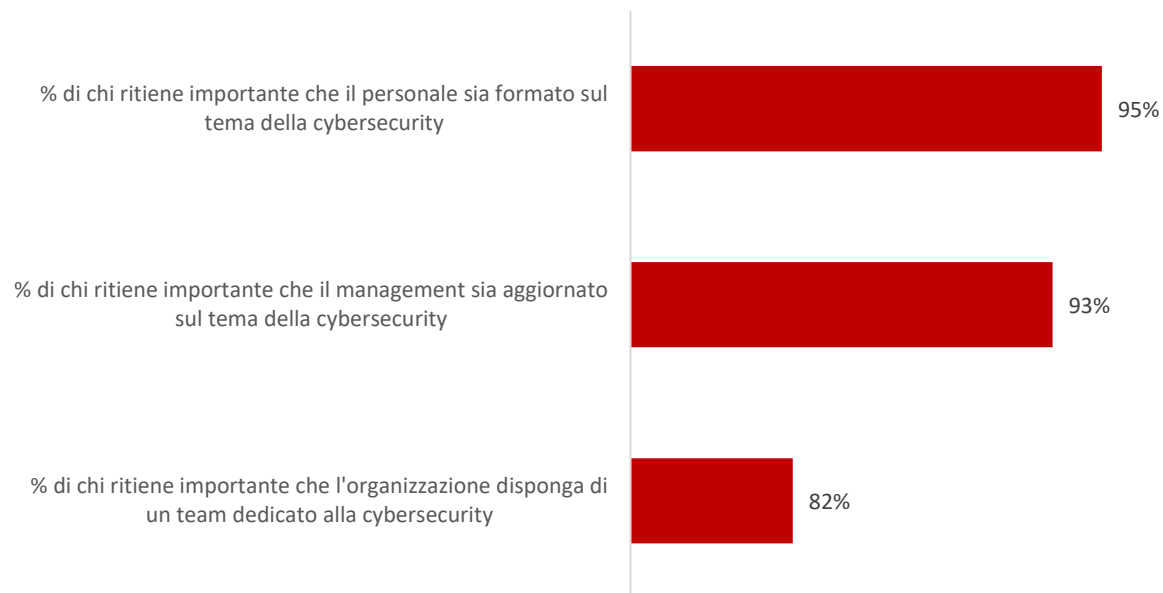
Se molti non conoscono i dettagli del budget, un numero cospicuo di intervistati è a conoscenza del fatto che nella propria organizzazione ci sia o meno un team dedicato alla cybersecurity



# Dall'indagine emerge una diffusa sensibilità a disporre o a potenziare misure e strumenti atti a garantire la sicurezza informatica nella struttura/organizzazione di cui si fa parte

---

% di ingegneri dipendenti favorevoli a particolari misure in materia di cybersecurity

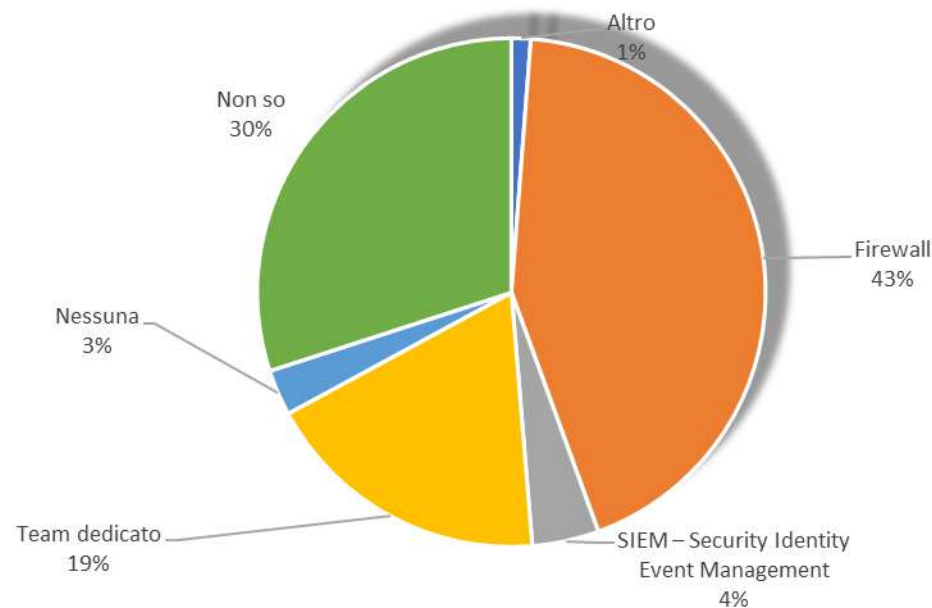


Tutti sono sostanzialmente favorevoli alla formazione continua di tutti e di team specializzati in materia di sicurezza informatica. Diffusa è l'attenzione verso la necessità di disporre di team dedicati alla cybersecurity nella struttura/organizzazione di appartenenza

Se tuttavia dagli aspetti di carattere più generale si ritorna all'ambito tecnico, il numero di chi conosce con esattezza la situazione in materia di cybersecurity nella propria organizzazione diventa piuttosto esiguo. Ben il 30% degli intervistati non sa che tipo di tecnologia è utilizzata dalla propria struttura per garantire la sicurezza informatica. Nel 43% è utilizzato un semplice Firewall

---

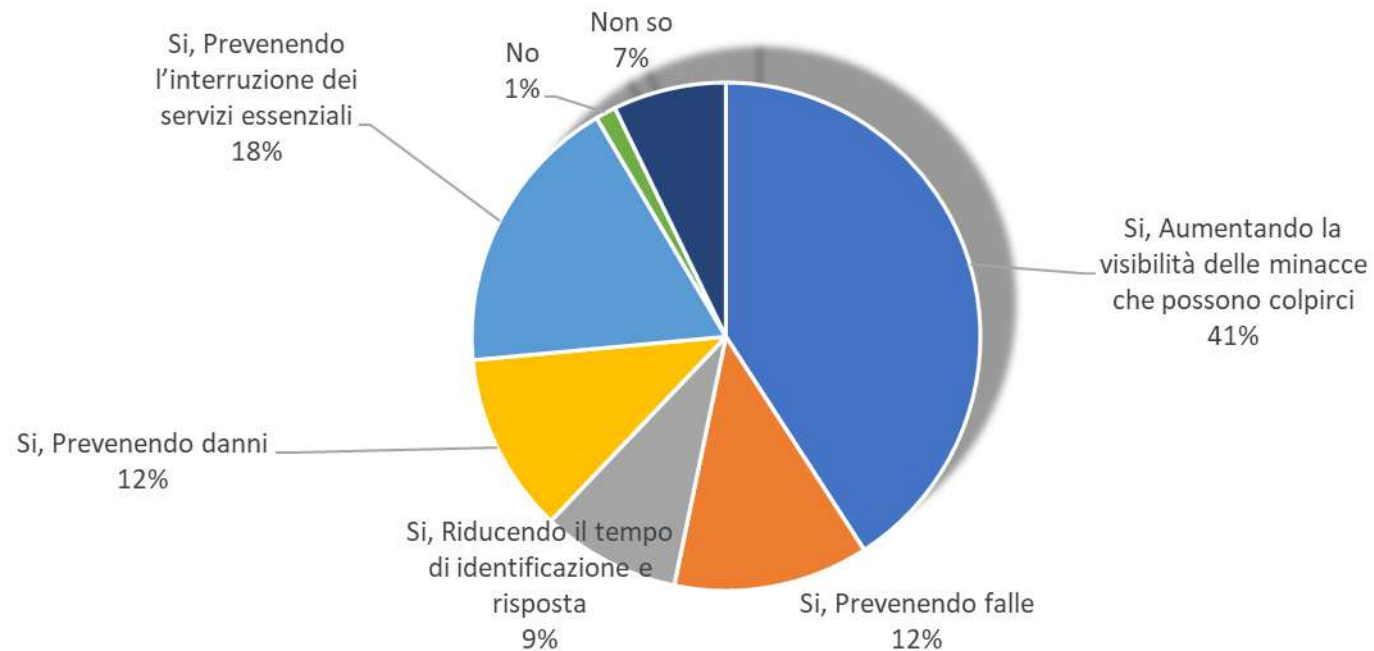
Tecnologie/modelli organizzativi utilizzati in azienda/ente di appartenenza per la cybersecurity



# Effetti determinati dalla presenza di un team dedicato alla cybersecurity (la presenza di un team è stata indicata dal 19% degli intervistati)

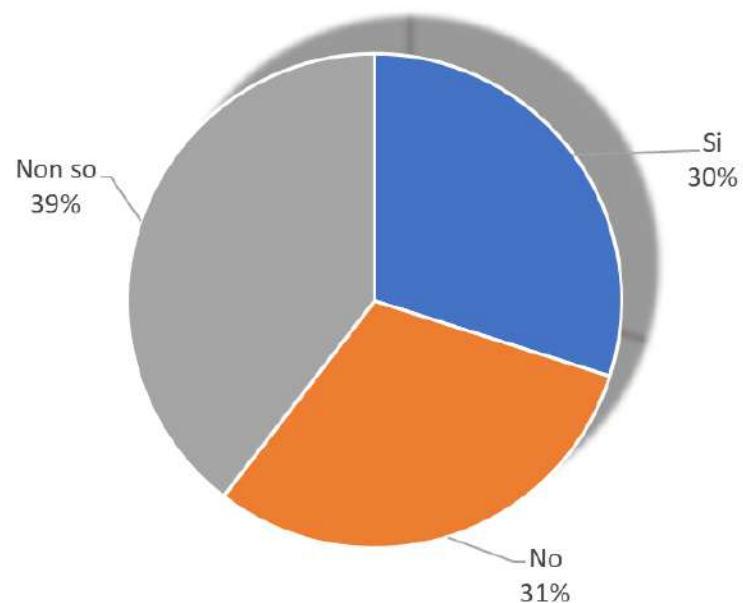
---

Il ricorso a team dedicati alla cybersecurity ha migliorato il livello di sicurezza informatica in ambito lavorativo?

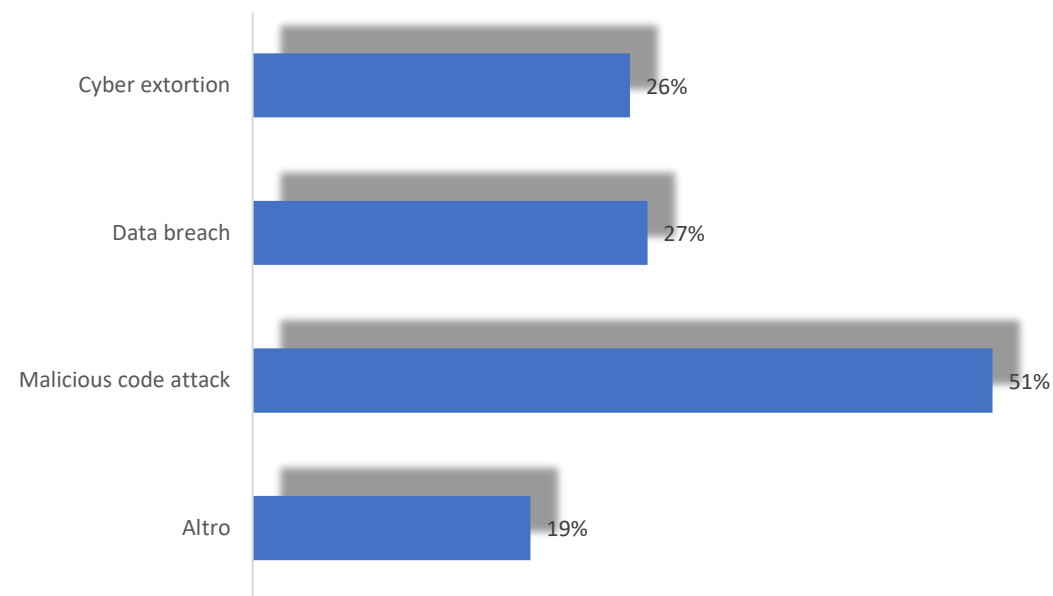


# Attacchi informatici negli ultimi 5 anni

Negli ultimi 5 anni la Sua azienda/Ente ha subito attacchi informatici?



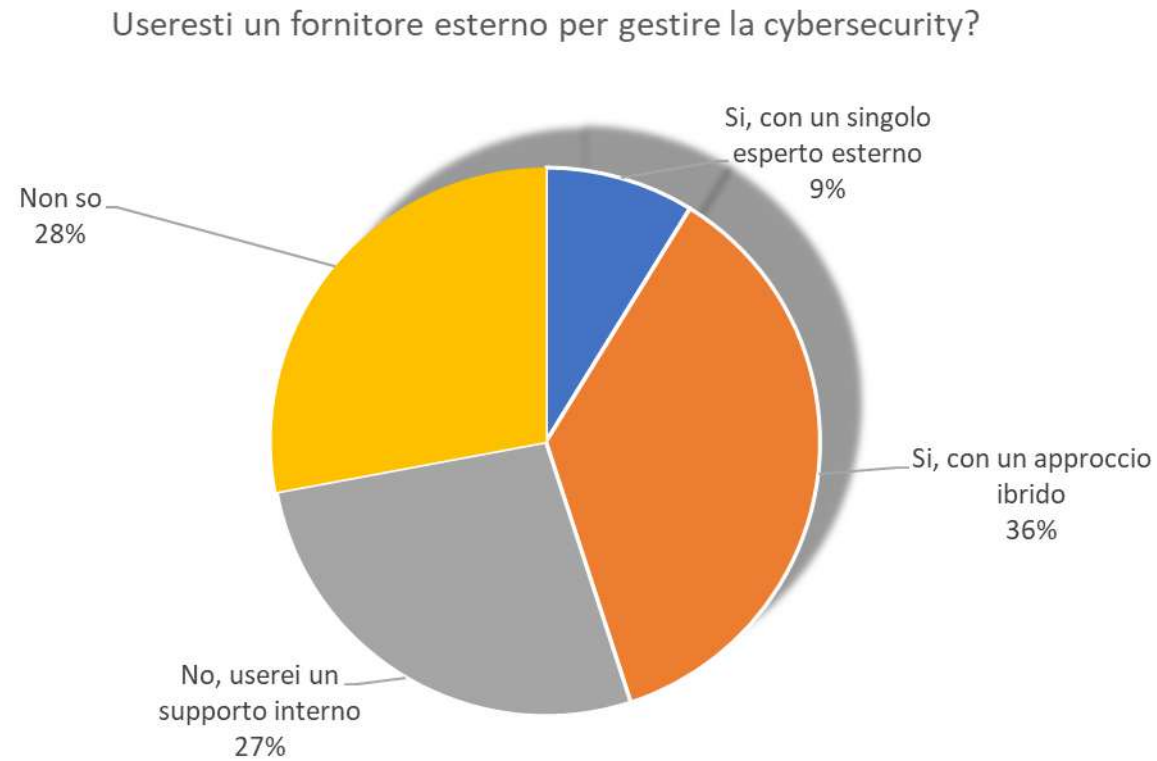
Tipi di attacchi informatici subiti dall'azienda/ente di appartenenza negli ultimi 5 anni





Molti intervistati sarebbero disposti ad un fornitore esterno per gestire la sicurezza informatica, ma prevalentemente con approccio ibrido. Più di un quarto però non esternalizzerebbe il servizio

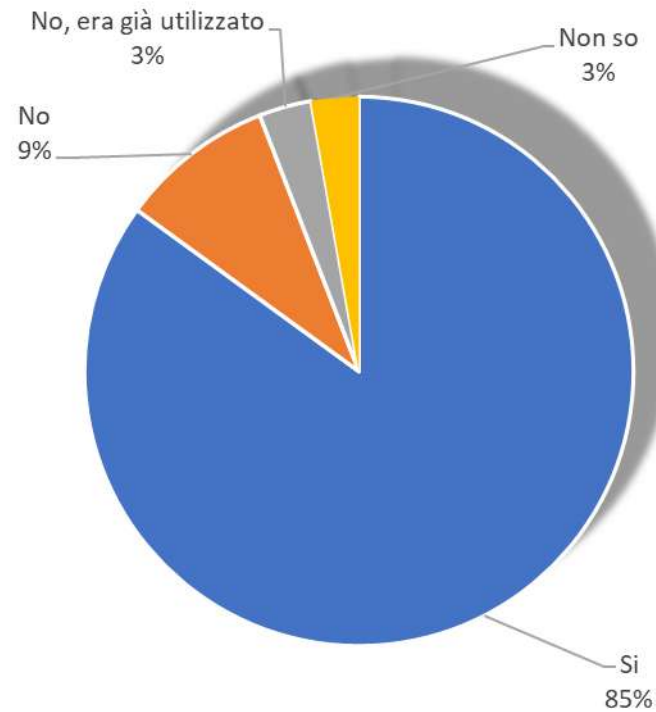
---



Il remote working è diventato una pratica estremamente diffusa, imponendo di ripensare anche il tema della sicurezza informatica

---

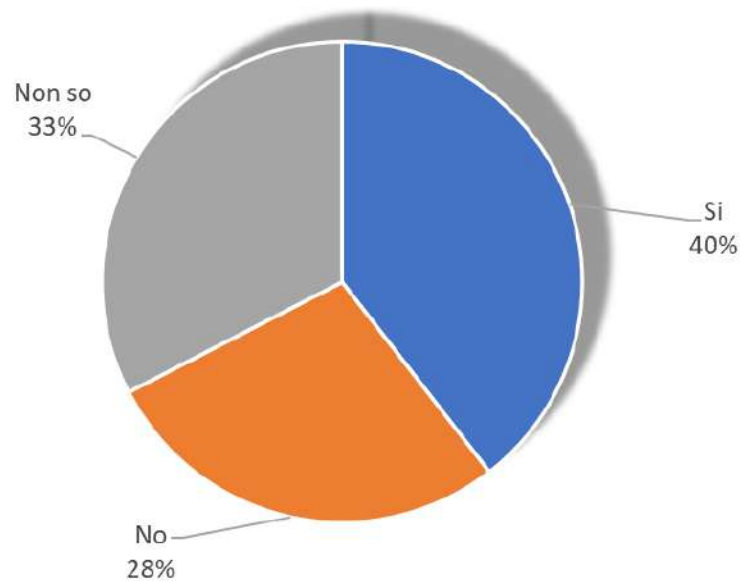
Nell'ultimo anno nella azienda/ente si è ricorso al remote working?



# Il remote working tuttavia ha anche stimolato in molti casi l'innalzamento del livello di attenzione nei confronti del tema della cybersecurity

---

Se si è fatto ricorso al remote working sono state necessarie misure di adeguamento alla cybersecurity?



Se si fa ricorso al remote working, lo si ritiene sicuro?

