



# PID Cyber Check

10/03/2023

Report nazionale

Italia

## Descrizione del report

Questo rapporto fornisce informazioni ottenute attraverso un questionario sull'autovalutazione del rischio informatico. Il sondaggio è disponibile sul sito web dell'Osservatorio sulla cybersecurity.

L'obiettivo principale dell'indagine è fornire uno strumento semplice e veloce per l'autovalutazione del rischio informatico.

Lo strumento richiede due tipi di input: informazioni sulle misure di sicurezza e informazioni sugli asset chiave dell'impresa. Una volta forniti tutti gli input, lo strumento stima le perdite annuali previste per ogni minaccia rilevata e una totale.

L'indagine prevede domande a scelta multipla, suddivise in 7 categorie.

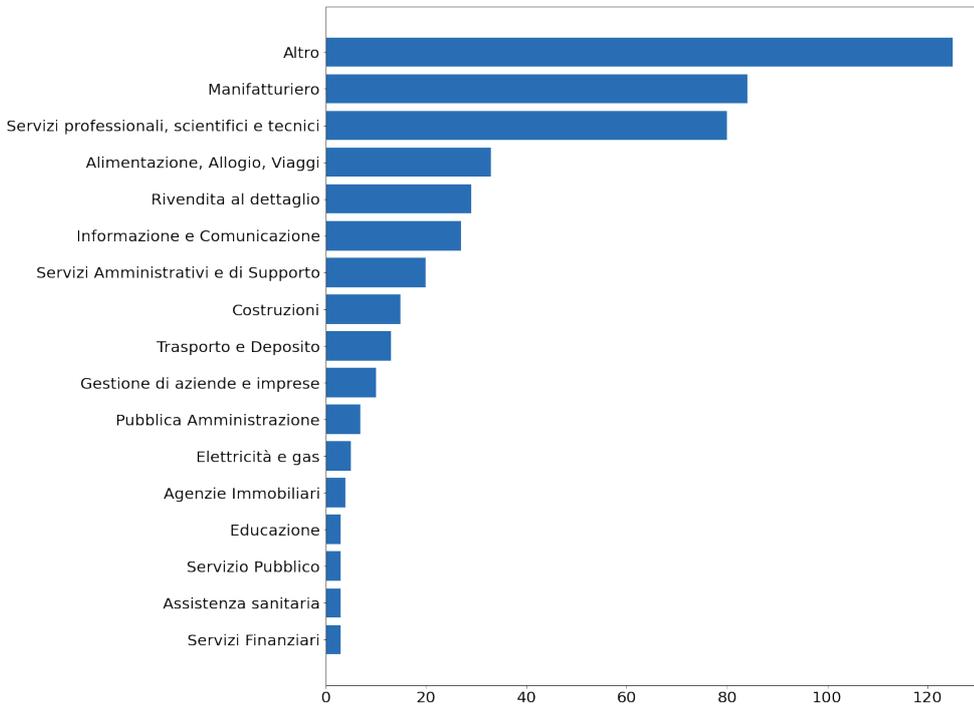
Per ogni domanda, riportiamo la distribuzione delle risposte tra tutte le scelte possibili.

# 464

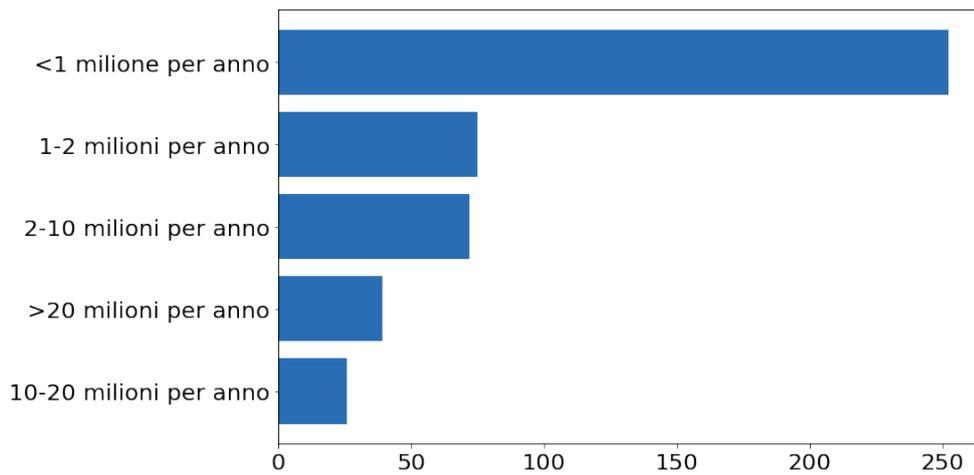
Hanno partecipato al sondaggio

# Informazioni sulle aziende

Settore:

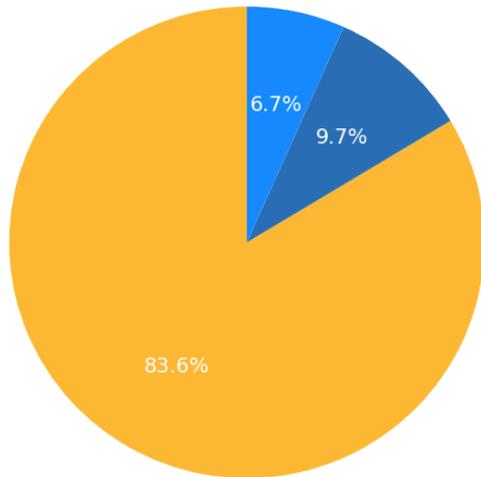


Fatturato:

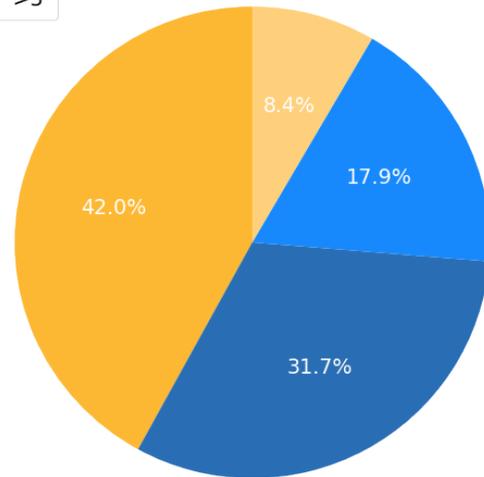
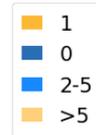


# Struttura dell'azienda

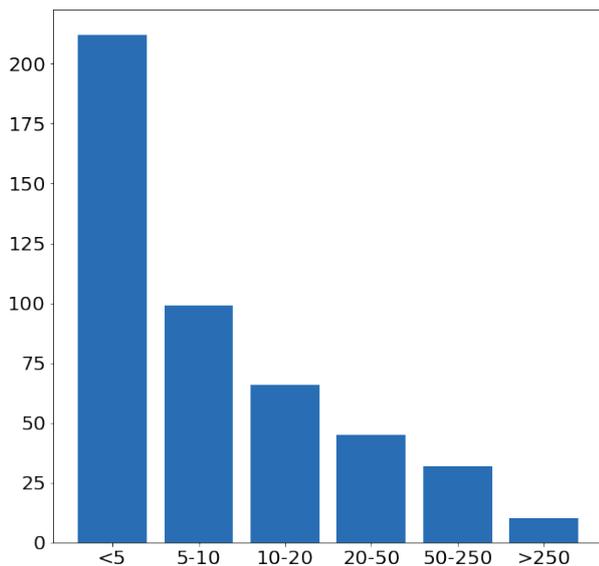
La sua azienda possiede una rete IT:



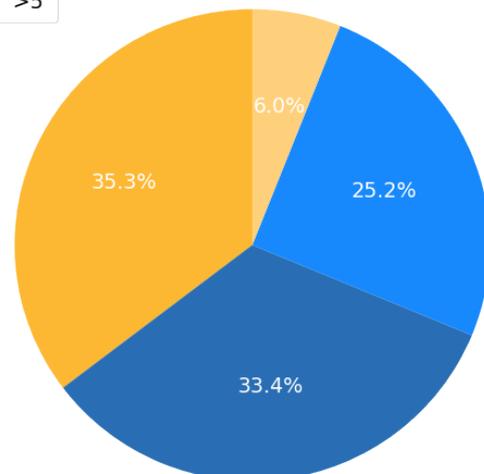
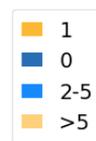
Server:



Computer Tradizionali:



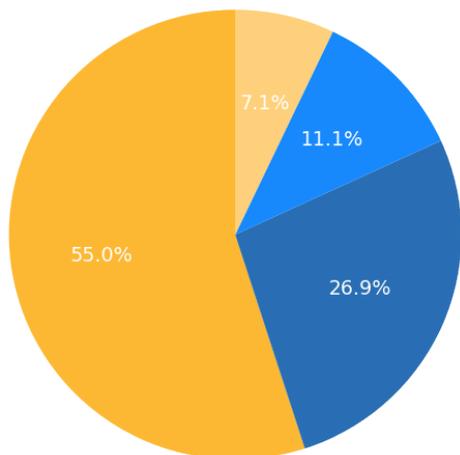
Servizi Cloud:



# Tipi di risorse dati

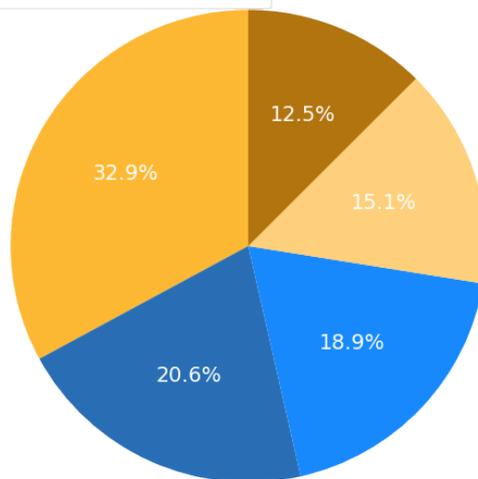
## Informazioni del cliente:

- Informazioni personali identificabili (nome, codice fiscale, indirizzo, sesso, ecc.);
- Informazioni finanziarie (dettagli delle carte di credito, cronologia degli acquisti, ecc.);
- Informazioni sanitarie personali (stato di salute, storia delle malattie, prescrizioni, ecc.);
- Nessuno dei precedenti;

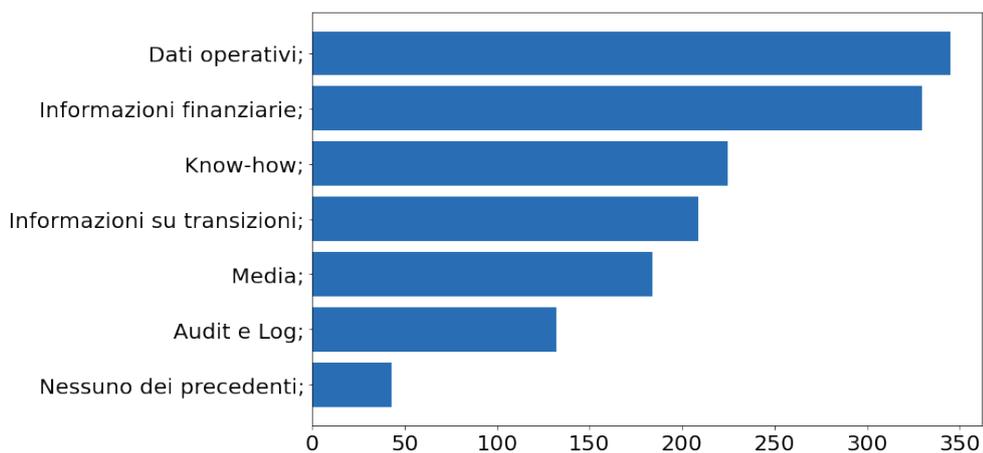


## Informazioni di altre aziende partner:

- Nessuno dei precedenti;
- Informazioni sui clienti del partner;
- Informazioni sulle transazioni;
- Record finanziari;
- Know-how;



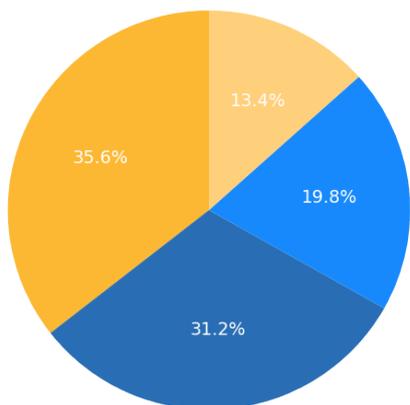
## Informazioni dell'azienda:



# Protezione informatica : Managment

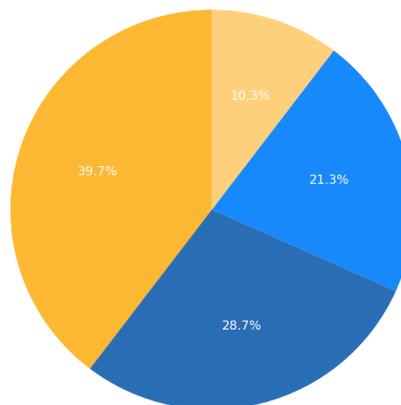
La sua azienda ha formalmente definito delle politiche di sicurezza:

- Sì, le politiche sono definite e il personale responsabile è a conoscenza di esse;
- No
- Sì, tutti i dipendenti ne sono a conoscenza (vengono informati all'inizio del loro impiego);
- Sì, tutti i dipendenti hanno familiarità con esse e lo staff responsabile assicura che vengano seguiti;

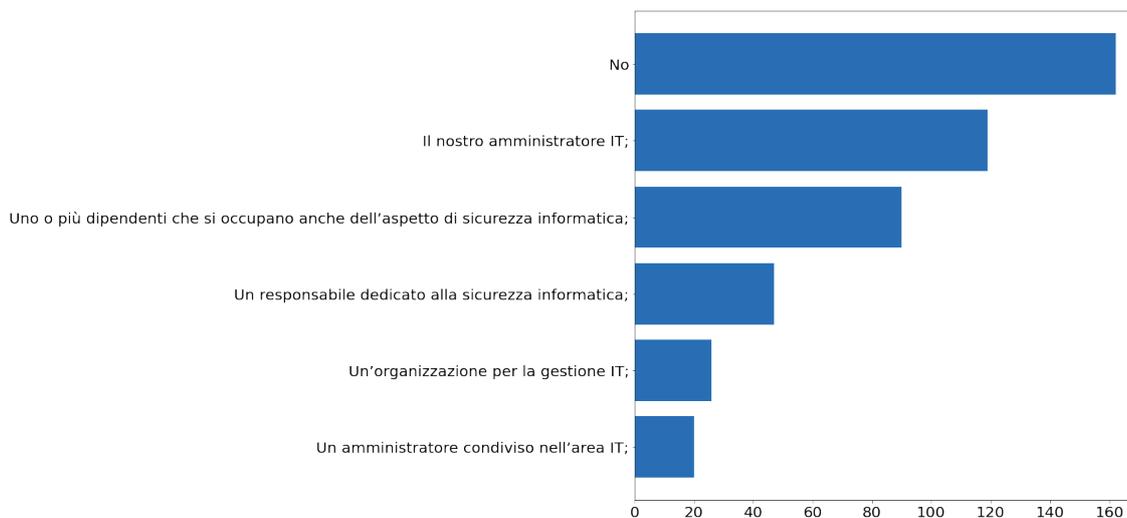


La sua azienda ha formalmente definito delle politiche sui dispositivi mobili (supponendo che la risposta precedente sia Sì):

- I dispositivi mobili possono connettersi liberamente alla rete, presupponendo che vengano fornite le credenziali corrette;
- Solo i dispositivi mobili dell'azienda (configurati e gestiti dal personale IT interno) possono connettersi alla rete aziendale;
- Tutti i dispositivi mobili possono connettersi liberamente alla rete
- Tutti i dispositivi mobili sono obbligati a soddisfare le politiche dell'azienda;



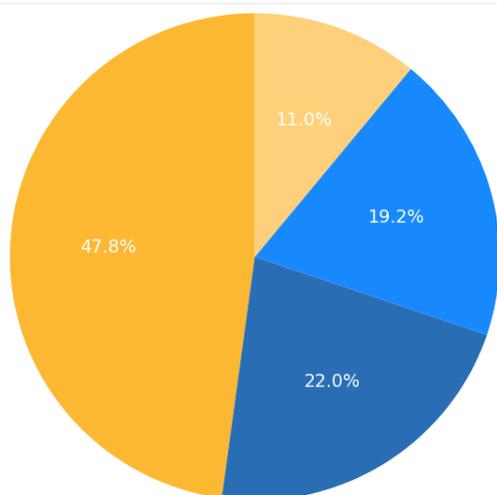
La sua azienda ha una persona ufficialmente responsabile della sicurezza informatica (colui/colei che distribuisce il budget per la sicurezza informatica, stabilisce gli obiettivi strategici e definisce le politiche di sicurezza, ecc.):



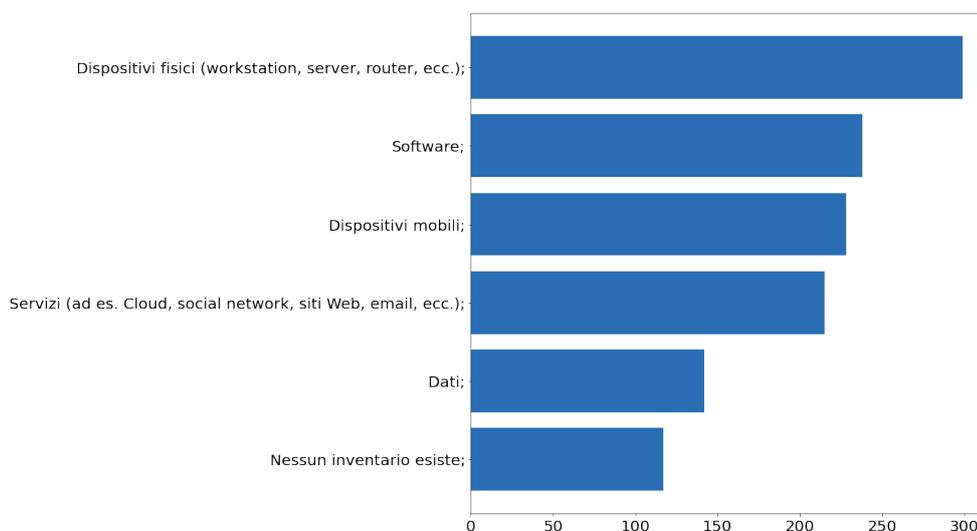
## Protezione informatica : Domande non tecniche

Qual è il livello di consapevolezza da parte dei suoi dipendenti della sicurezza informatica nella sua azienda (scelte multiple consentite):

- Nessuno dei precedenti;
- I dipendenti leggono (e firmano un documento speciale) sulle politiche di sicurezza informatica;
- Vengono effettuate attività speciali di formazione sulla sicurezza informatica organizzate dall'azienda;
- Vengono effettuati corsi di formazione sulla sicurezza informatica da una ditta esterna;

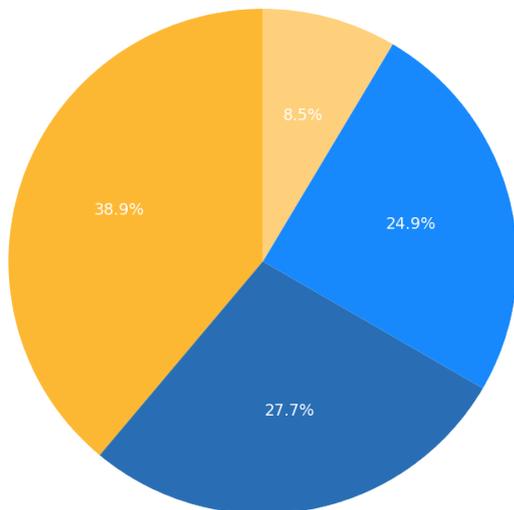


Quali beni sono inclusi in un inventario mantenuto dalla sua azienda: (scelte multiple consentite)



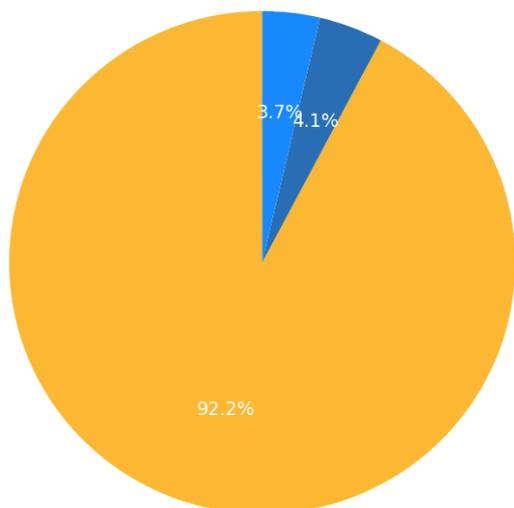
## In che modo l'accesso fisico ai locali dell'azienda è protetto e controllato (scelte multiple consentite)

- Uffici. L'accesso agli uffici principali è severamente vietato ai visitatori esterni se nessuno dei presenti è all'interno;
- Perimetro. L'accesso all'area è sorvegliato dall'addetto alla reception;
- La stanza del server è bloccata e solo il personale responsabile ha accesso ad essa;
- L'accesso di visitatori esterni non è monitorato.



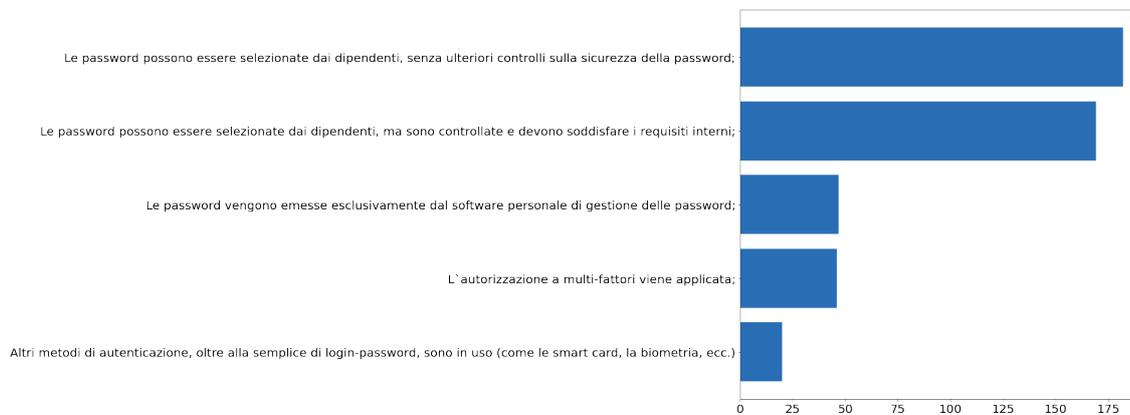
## L'organizzazione ha un certificato di sicurezza informatica: (scelte multiple consentite)

- Nessuna
- Altro
- Si (ISO 270XX, (N)CSF, Cobit)



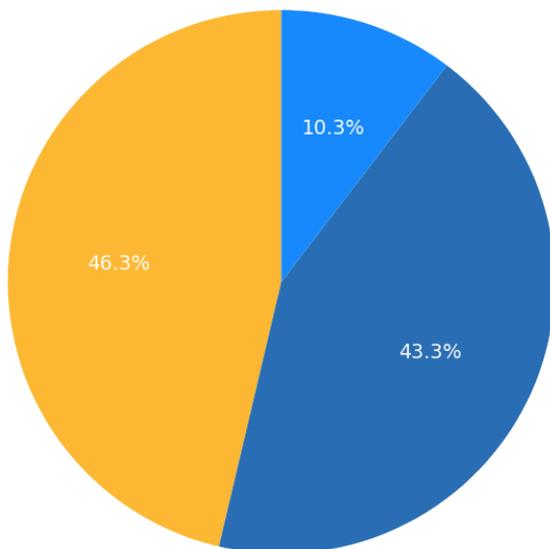
# Protezione informatica : Access Control

Politiche di gestione della password e dell'identità:



Qual è la procedura per garantire l'accesso alle risorse informative:

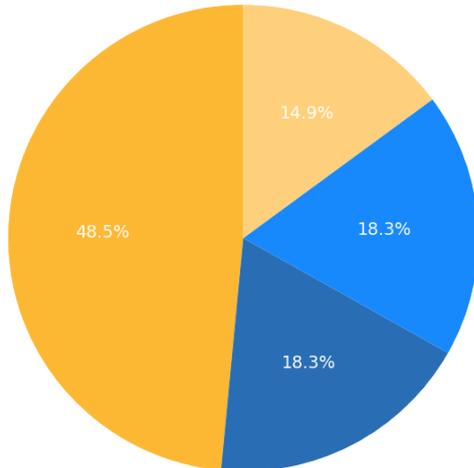
- Non esiste una procedura particolare. L'accesso è concesso quando è necessario;
- L'accesso è concesso per quanto riguarda il lavoro svolto dal dipendente e solo per quello;
- Esiste una procedura formale per garantire l'accesso e la revoca al dipendente;



## Protezione informatica : Domande tecniche

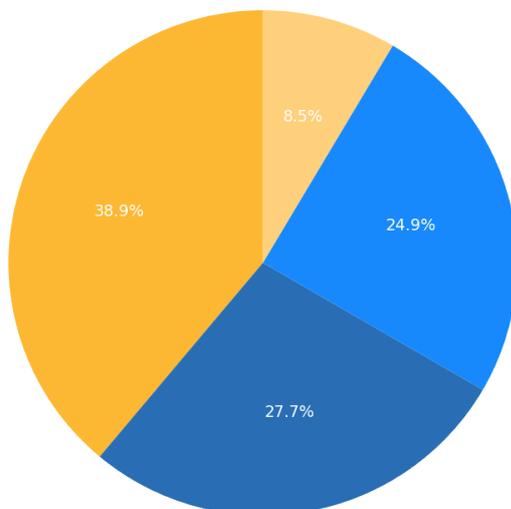
Come viene protetto l'accesso remoto alle risorse informative:

- I dati vengono crittografati con un protocollo di sicurezza (HTTPS, TLS, SSL, ecc.) o inviati tramite una VPN;
- Non è consentito l'accesso remoto;
- I dati inviati non vengono criptati;
- Questo è gestito direttamente dall'amministratore IT;

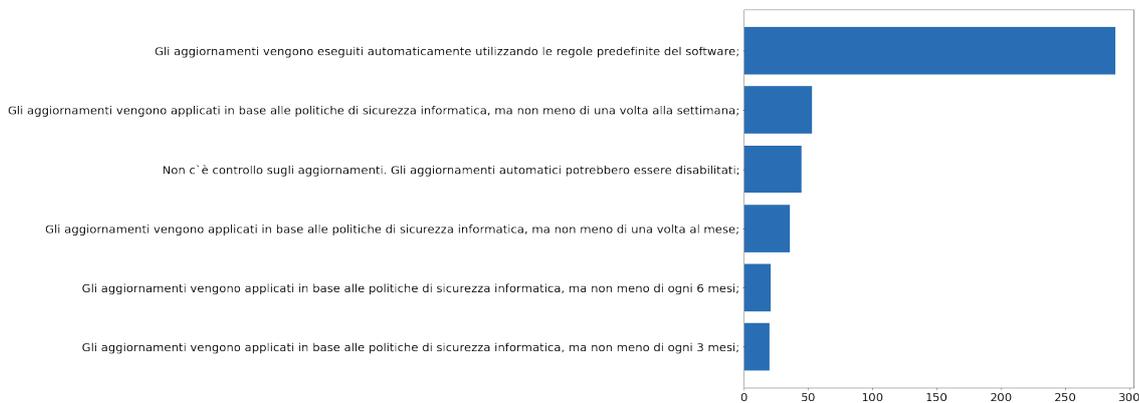


Quali meccanismi di protezione di rete sono implementati: (scelte multiple consentite)

- Uffici. L'accesso agli uffici principali è severamente vietato ai visitatori esterni se nessuno dei presenti è all'interno;
- Perimetro. L'accesso all'area è sorvegliato dall'addetto alla reception;
- La stanza del server è bloccata e solo il personale responsabile ha accesso ad essa;
- L'accesso di visitatori esterni non è monitorato.

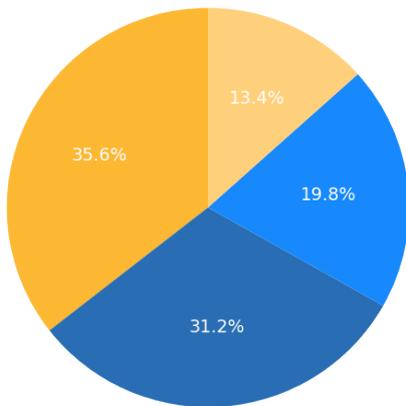


Con quale frequenza aggiorna i suoi sistemi (inclusi sistemi operativi, servizi Web, browser, database, ecc.):



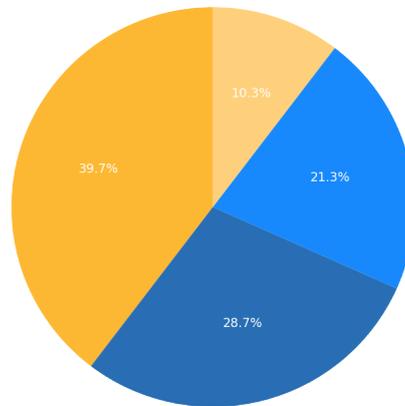
La sua azienda ha formalmente definito delle politiche di sicurezza:

- Sì, le politiche sono definite e il personale responsabile è a conoscenza di esse;
- No
- Sì, tutti i dipendenti ne sono a conoscenza (vengono informati all'inizio del loro impiego);
- Sì, tutti i dipendenti hanno familiarità con esse e lo staff responsabile assicura che vengano seguiti;



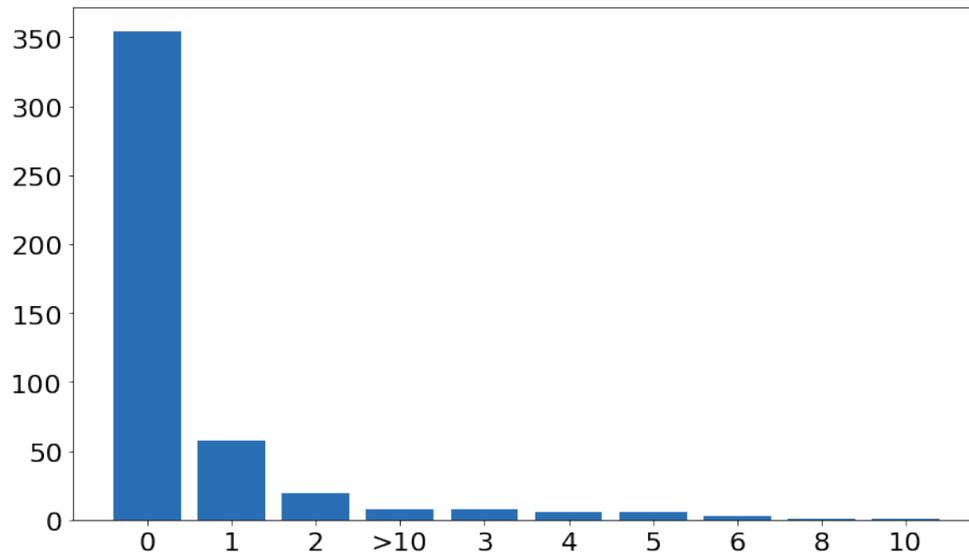
La sua azienda ha formalmente definito delle politiche sui dispositivi mobili (supponendo che la risposta precedente sia SI):

- I dispositivi mobili possono connettersi liberamente alla rete, presupponendo che vengano fornite le credenziali corrette;
- Solo i dispositivi mobili dell'azienda (configurati e gestiti dal personale IT interno) possono connettersi alla rete aziendale;
- Tutti i dispositivi mobili possono connettersi liberamente alla rete
- Tutti i dispositivi mobili sono obbligati a soddisfare le politiche dell'azienda;

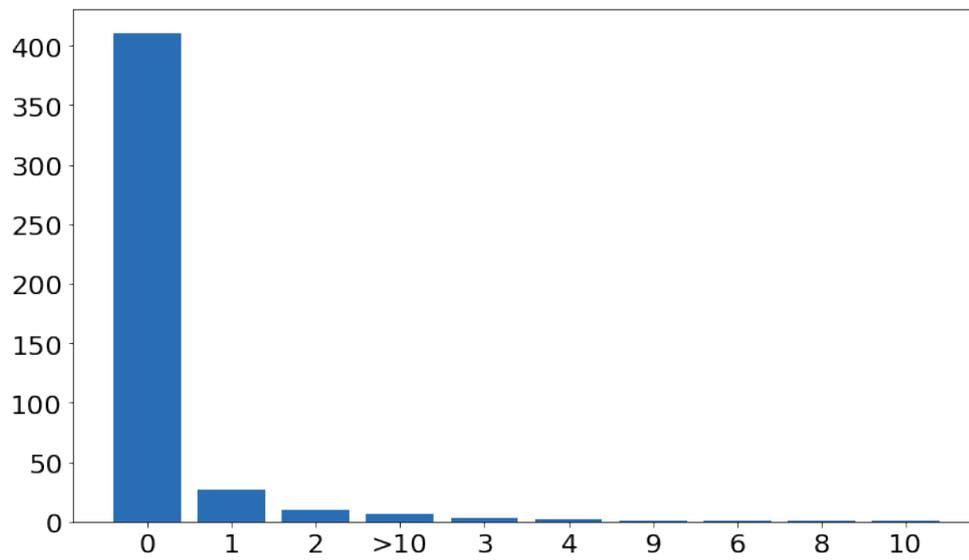


# Attacchi

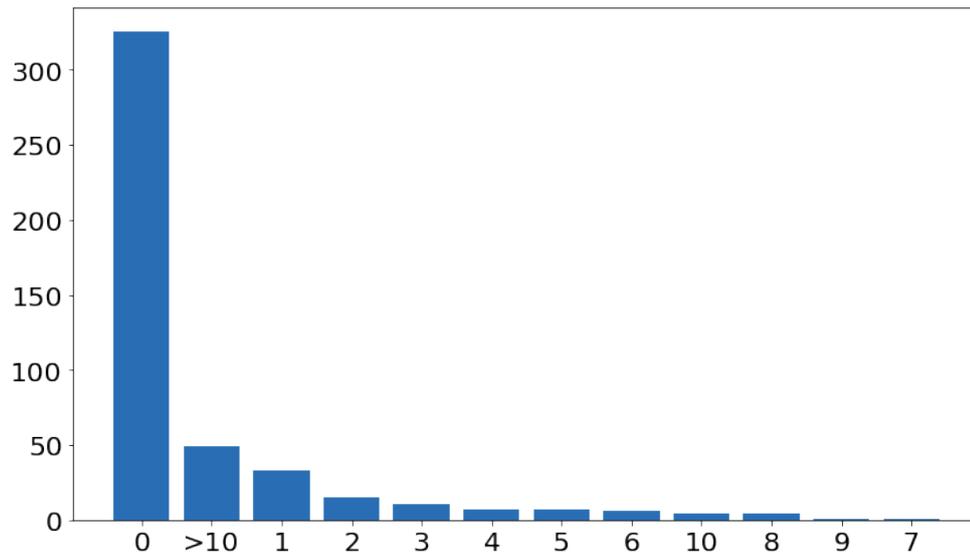
Malware / Hacker



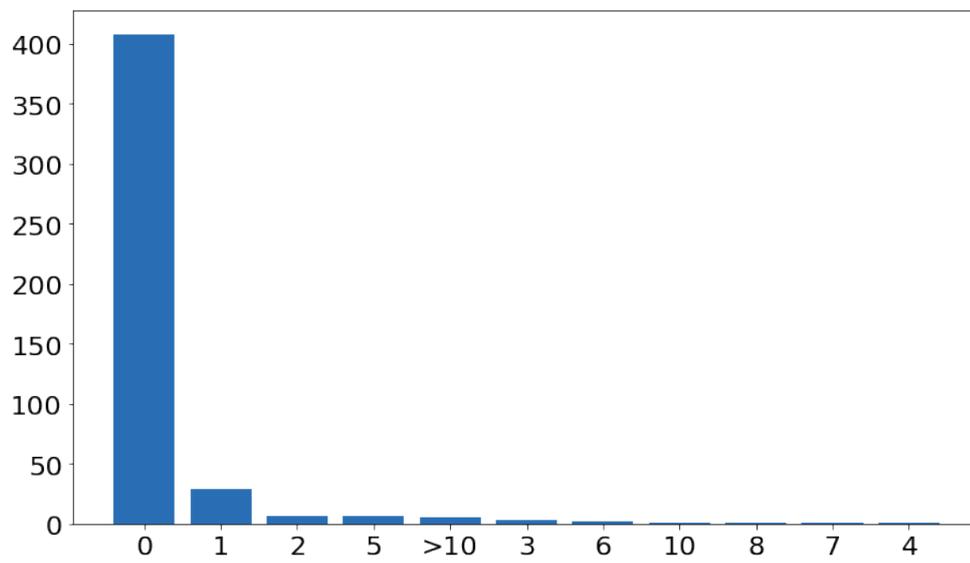
Ransomware



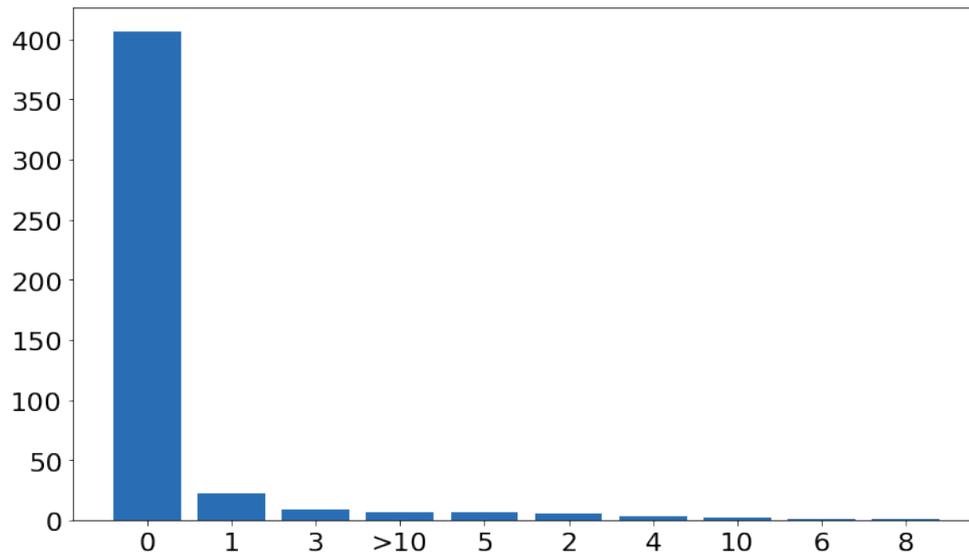
## Phishing



## Web application attacks



## Comportamento scorretto dei dipendenti



## Numero di altri incidenti registrati:

