ISTITUTO DI INFORMATICA E TELEMATICA

# PID Cyber Check

10/03/2023

## Report nazionale

# Italia

## Descrizione del report

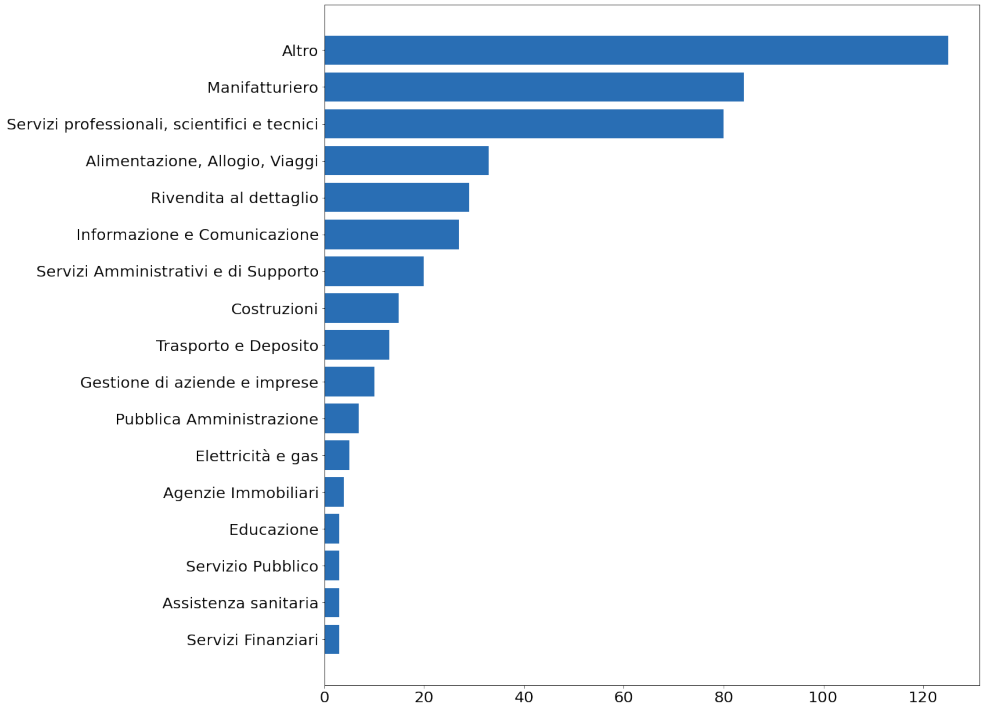
Questo rapporto fornisce informazioni ottenute attraverso un questionario sull'autovalutazione del rischio informatico. Il sondaggio è disponibile sul sito web dell'Osservatorio sulla cybersecurity.
L'obiettivo principale dell'indagine è fornire uno strumento semplice e veloce per l'autovalutazione del 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**

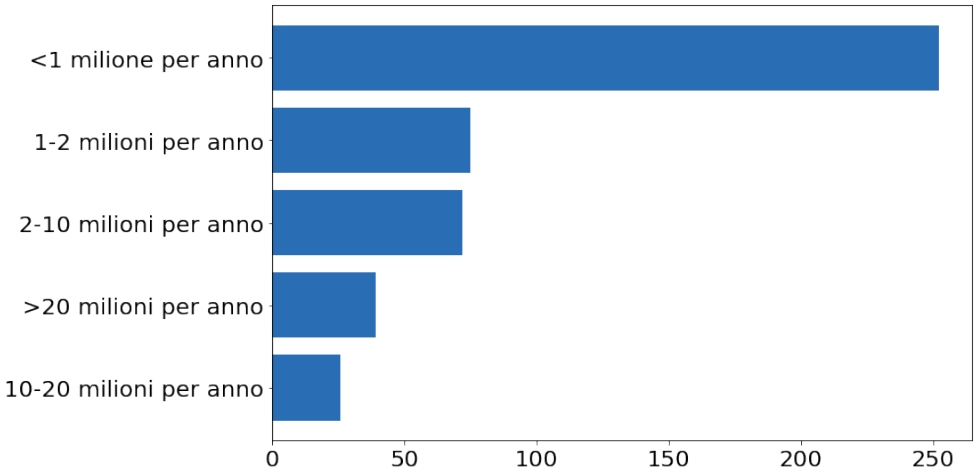
Hanno partecipato al sondaggio

# Informazioni sulle aziende

## Settore:

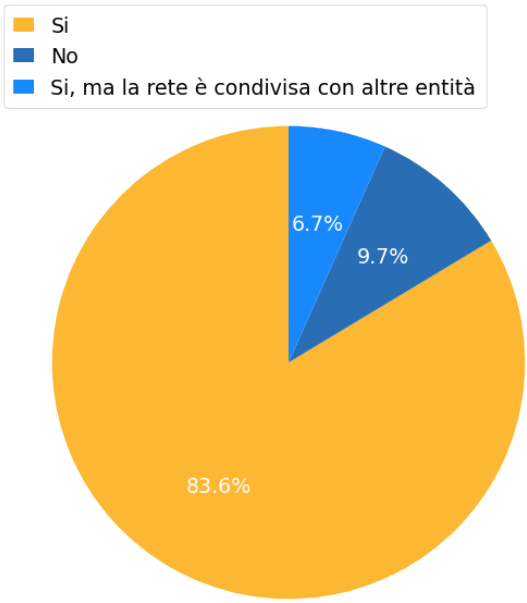



## Fatturato:

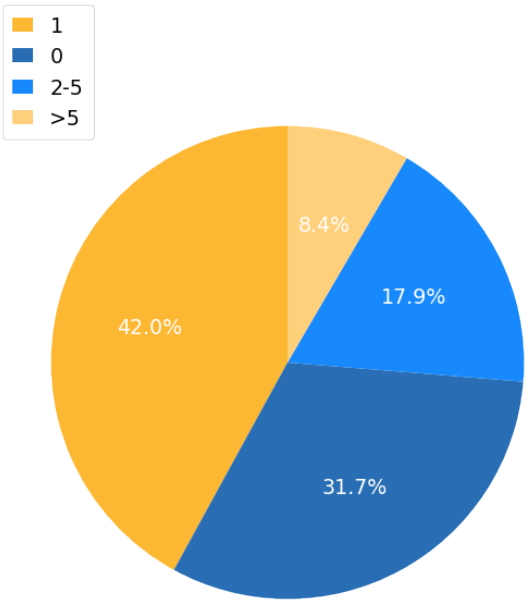


# Struttura dell'azienda

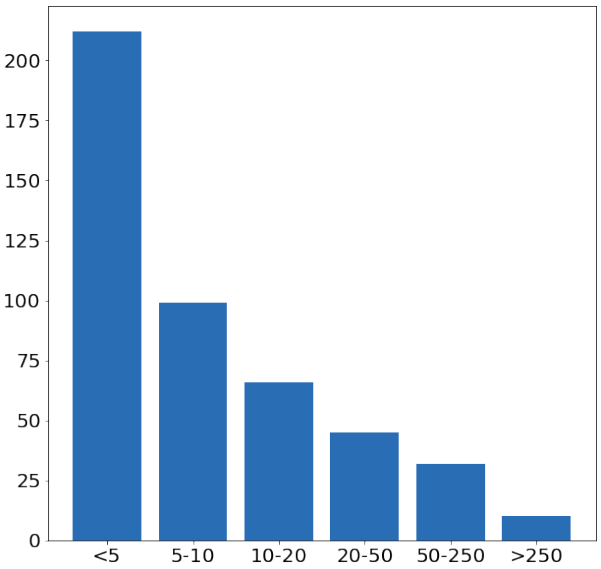
La sua azienda possiede una rete IT:



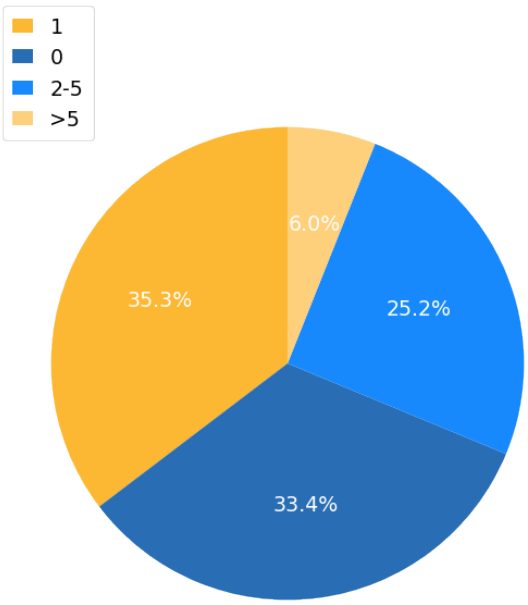

Server:




Computer Tradizionali:

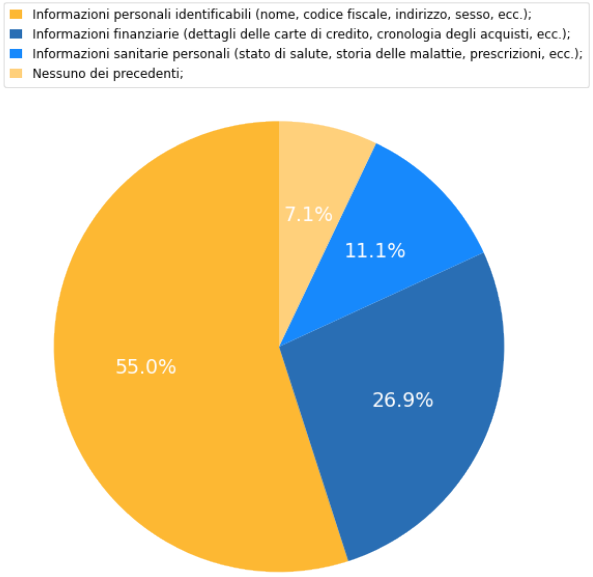



Servizi Cloud:

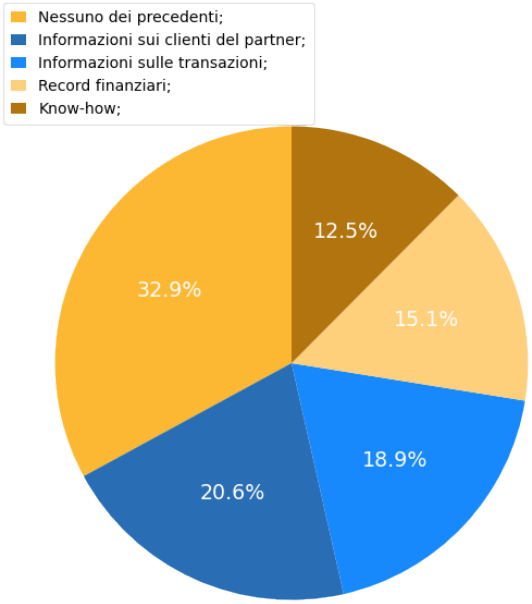


# Tipi di risorse dati

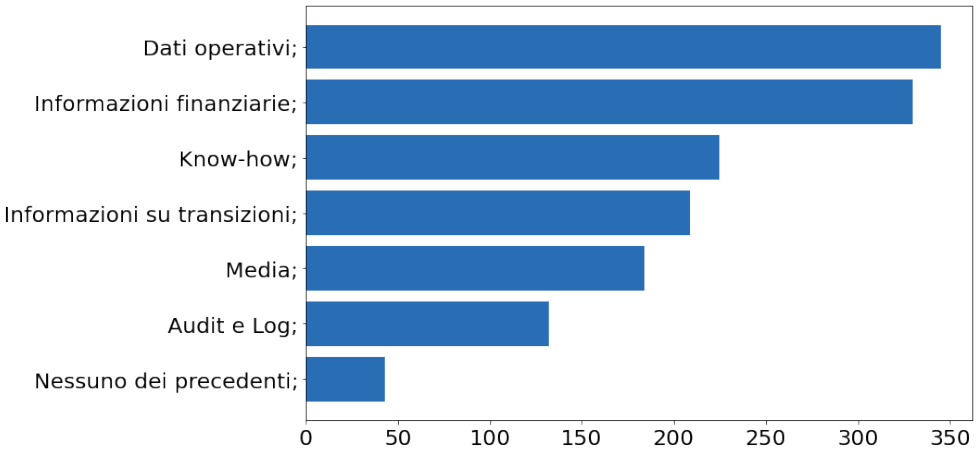
Informazioni del cliente:




Informazioni di altre aziende partner:

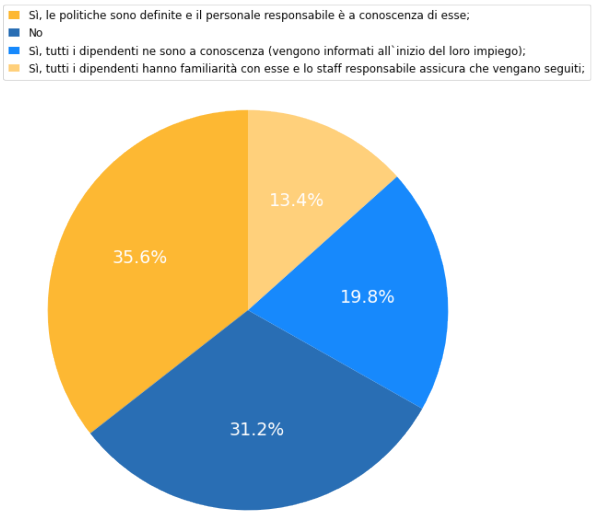



Informazioni dell'azienda:

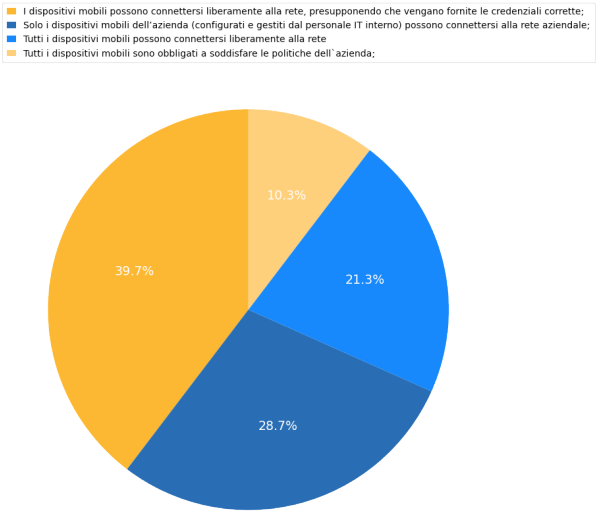


# Protezione informatica : Managment

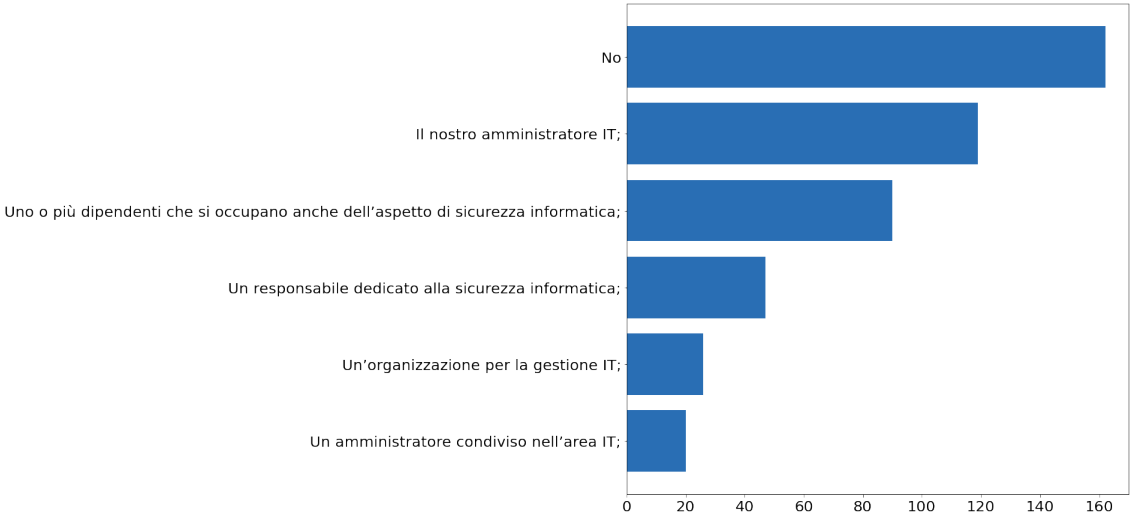
La sua azienda ha formalmente definito delle politiche di sicurezza:




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

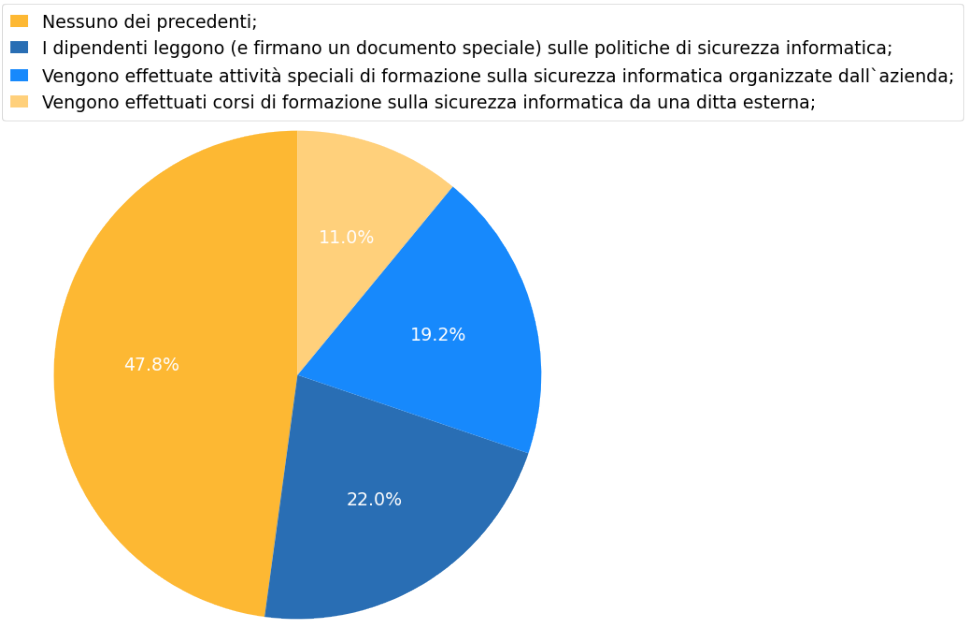



La sua azienda ha una persona ufficialmente responsabile della sicurezza informatica (colui/colei che distribuisce il budget per la sicurezza informatica, stabilisce gli obiettivi strategici e definisce le politiche di sicurezza, ecc.):

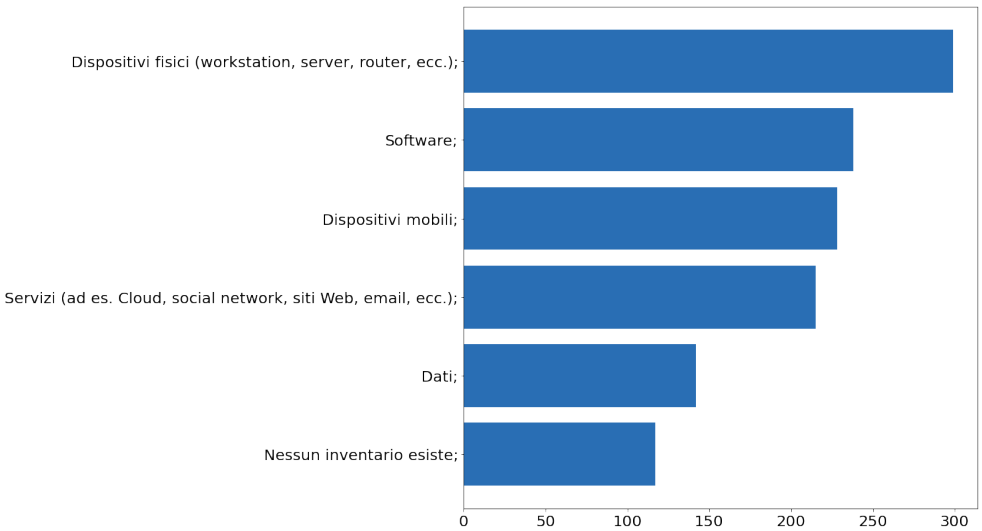


# Protezione informatica : Domande non tecniche

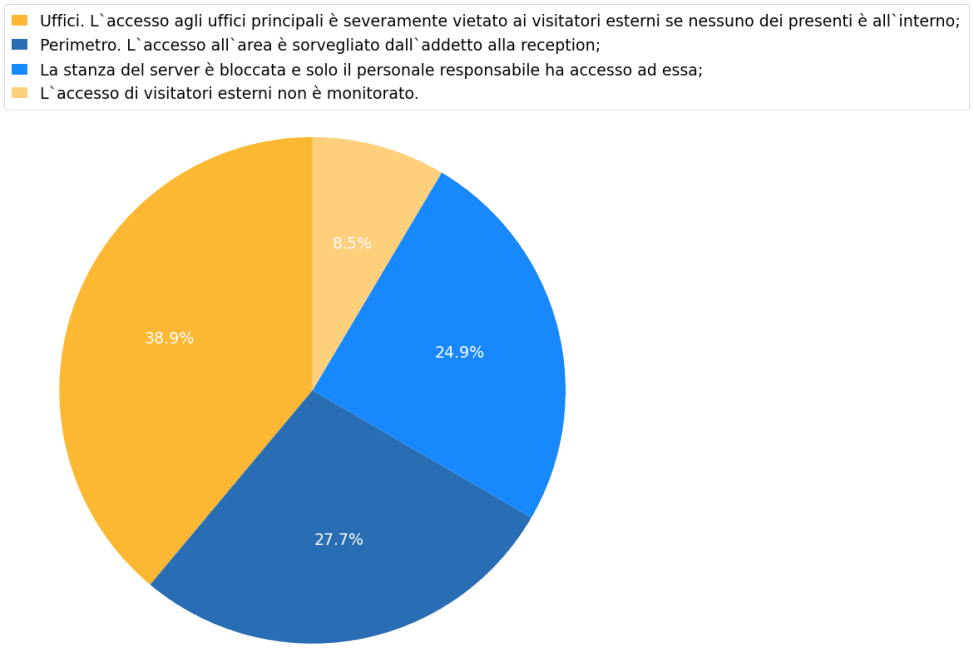
Qual è il livello di consapevolezza da parte dei suoi dipendenti della sicurezza informatica nella sua azienda (scelte multiple consentite):



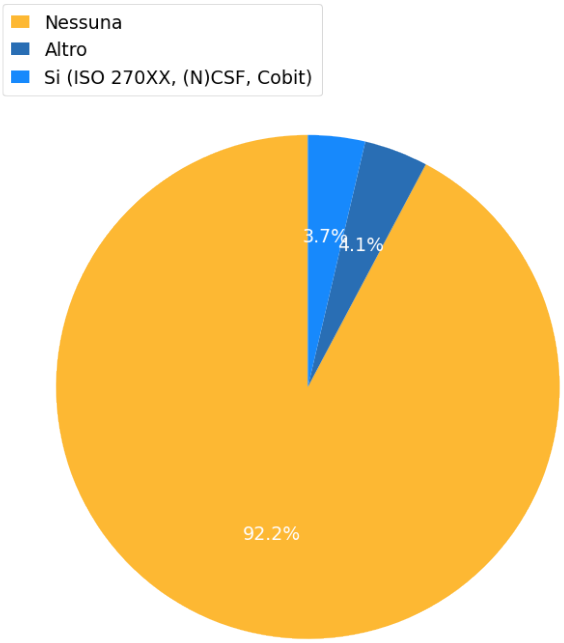

Quali beni sono inclusi in un inventario mantenuto dalla sua azienda: (scelte multiple consentite)



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

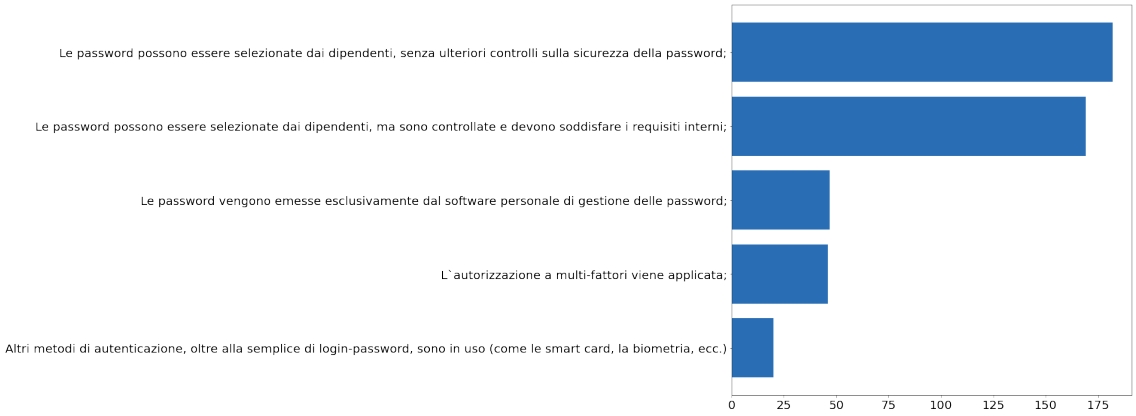



## L'organizzazione ha un certificato di sicurezza informatica: (scelte multiple consentite)

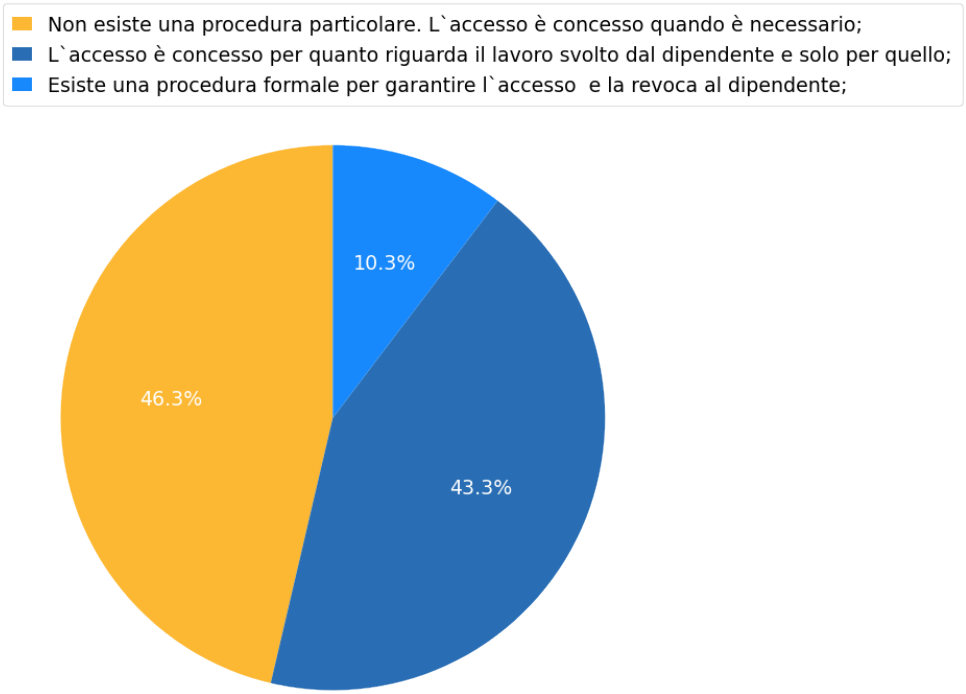


# Protezione informatica : Access Control

## Politiche di gestione della password e dell'identità:

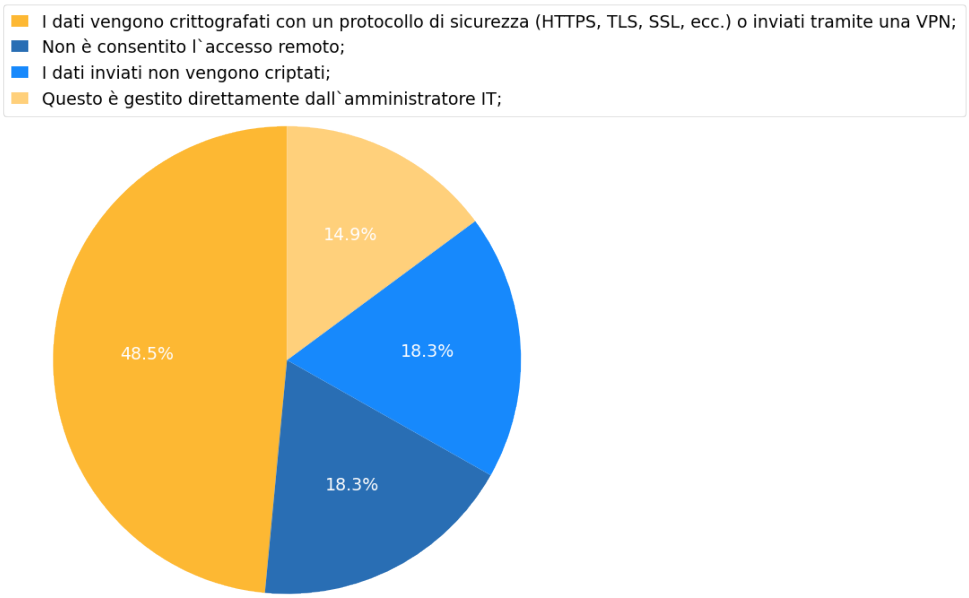



## Qual è la procedura per garantire l'accesso alle risorse informative:

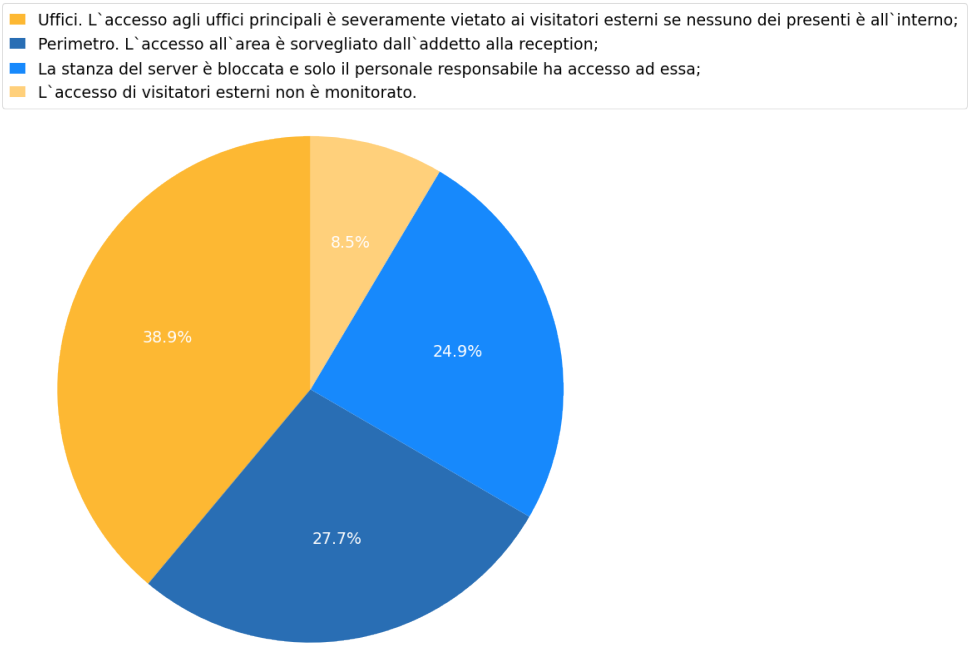


# Protezione informatica : Domande tecniche

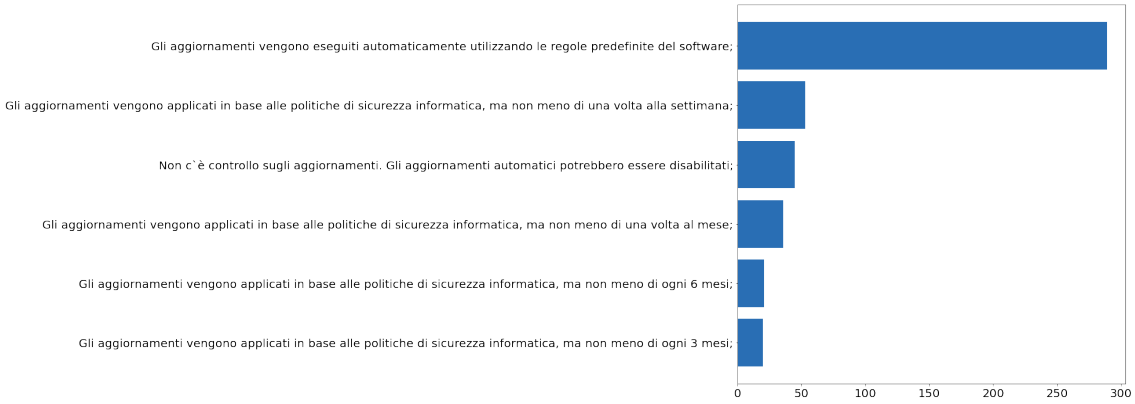
## Come viene protetto l'accesso remoto alle risorse informative:



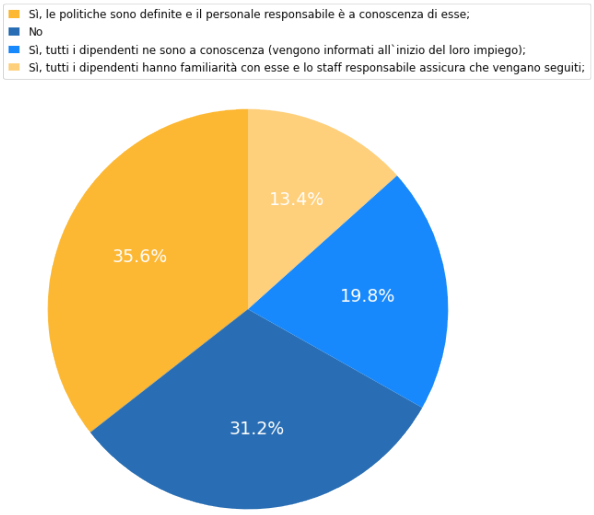

## Quali meccanismi di protezione di rete sono implementati: (scelte multiple consentite)



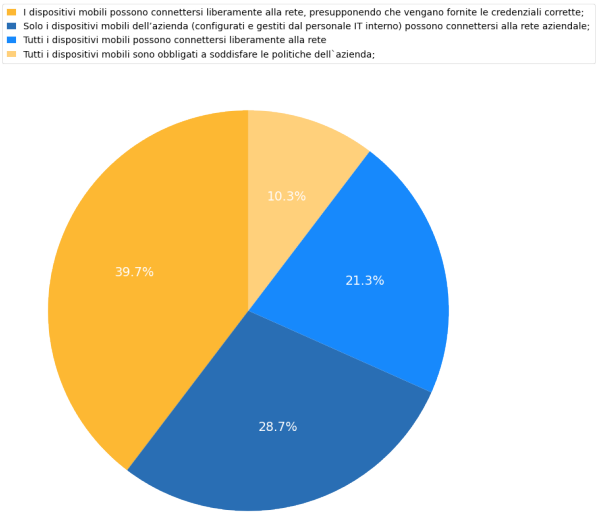
Con quale frequenza aggiorna i suoi sistemi (inclusi sistemi operativi, servizi Web, browser, database, ecc.):




La sua azienda ha formalmente definito delle politiche di sicurezza:

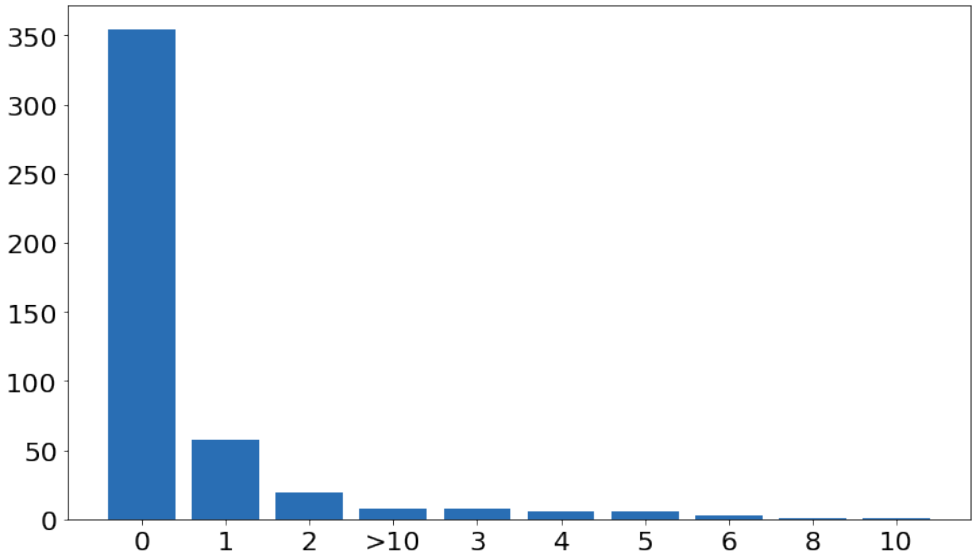



La sua azienda ha formalmente definito delle politiche sui dispositivi mobili (supponendo che la risposta precedente sia SI):

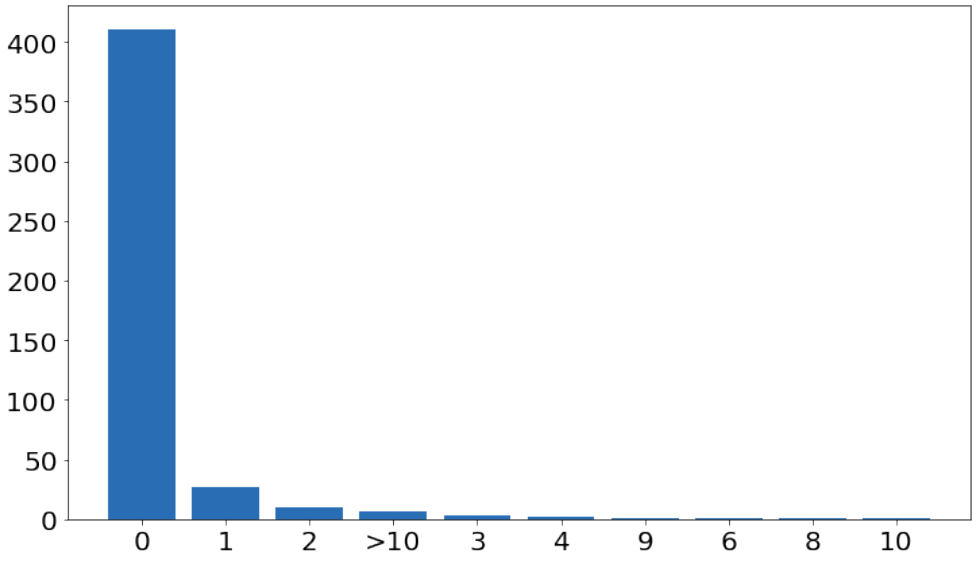


# Attacchi

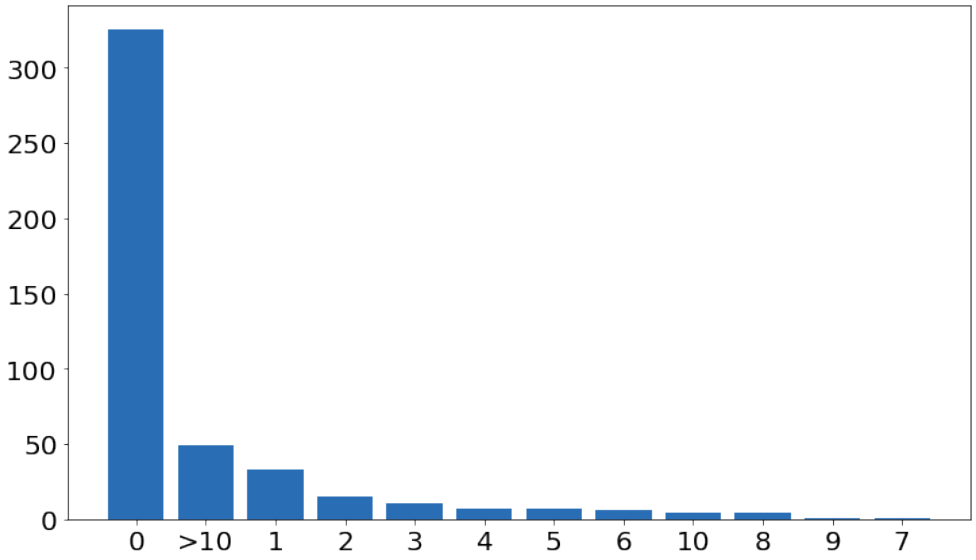
## Malware / Hacker



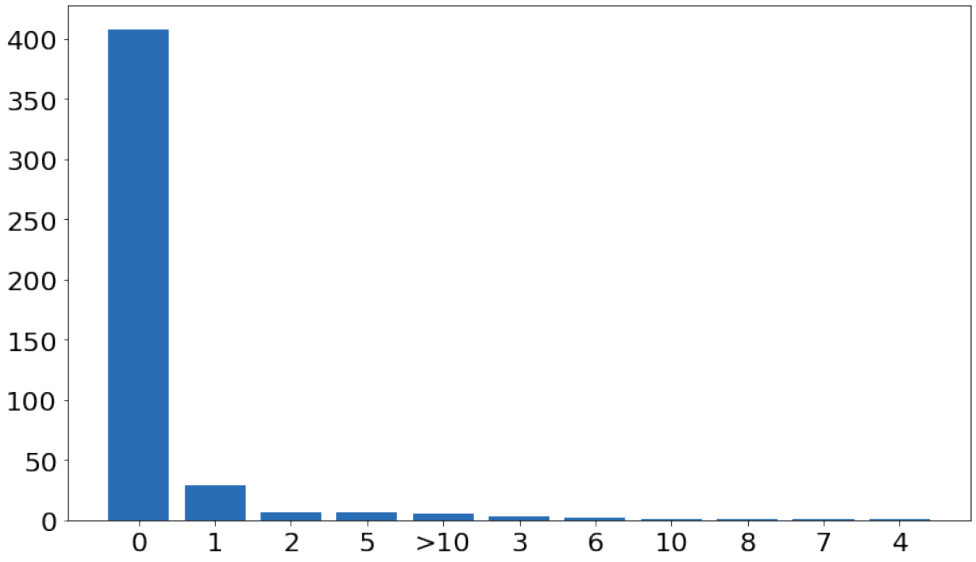

## Ransomware



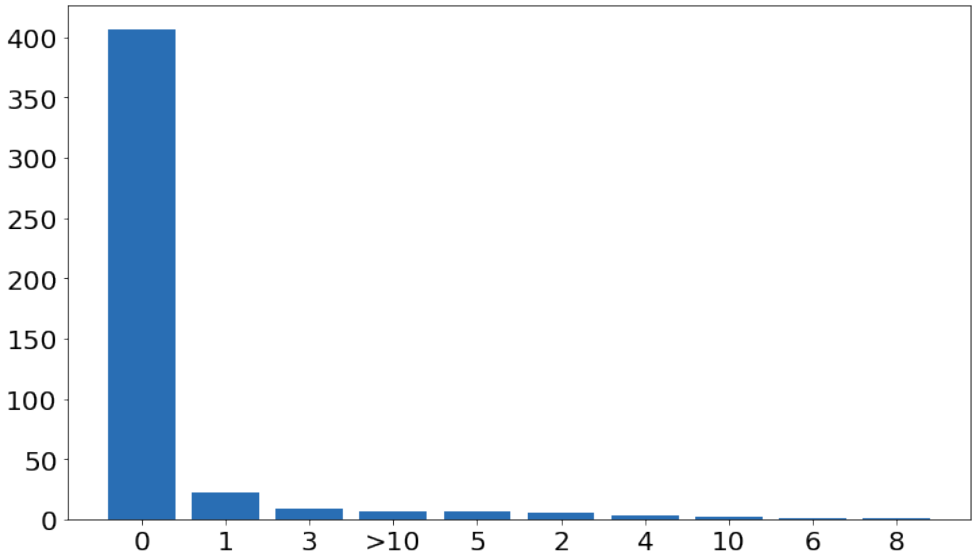
Phishing




Web application attacks



Comportamento scorretto dei dipendenti




Numero di altri incidenti registrati: