

# Ameaças Cibernéticas no Brasil em 2021

Alguns dados e resultados identificados durante a pesquisa para elaboração do relatório.

## PRINCIPAIS RISCOS EM 2021

A quantidade de ataques direcionados aos **usuários finais e suas estações de trabalho** está aumentando exponencialmente e, apesar das proteções de perímetro, estes ataques têm sido eficazes devido à falta de conscientização. Este tem sido percebido como o **elemento mais vulnerável** na proteção das informações das empresas, sendo muito explorado por criminosos como um dos **principais vetores de ataque para a prática do crime de ransomware**.

POSIÇÃO	RISCO
#1	Engenharia Social
#2	Ransomware
#3	Vazamento de Dados
#4	Brechas no Supply-Chain
#5	Ataques à Privacidade

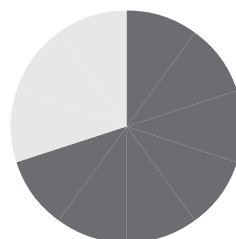
## RANSOMWARE NO BRASIL EM 2020



**3,86mi** ataques de *ransomware* foram realizados em 2020 somente em território nacional.  
(Sonicwall, 2021)

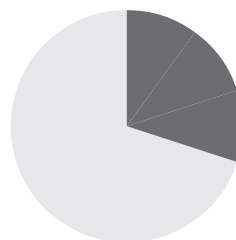
**Acesse a área de conteúdo em nosso website e confira a versão completa !**

## FOCO DO RANSOMWARE



**67%**  
Empresas e Organizações

**46%** das tentativas diárias de *ransomware* na América Latina em 2020 aconteceram no Brasil.  
(Kaspersky, 2020)

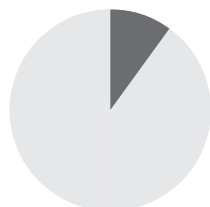


**33%**  
Pessoas Físicas

*Ransomware* foi o método de ataque mais popular em 2020, atingindo, em média, 37% das organizações pesquisadas.  
(Sophos, 2021)

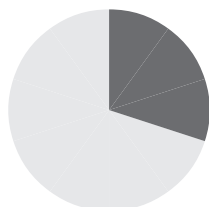
# Alguns números de nossa pesquisa

## FERRAMENTAS DE ACESSO REMOTO



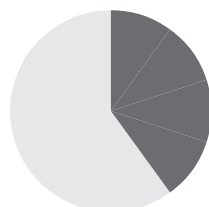
**7%**  
do total das falhas encontradas

## AUMENTO DOS ATAQUES DE PHISHING



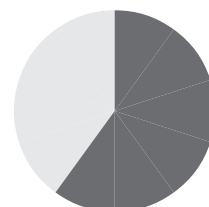
**30%**  
acima da média de crescimento ano anterior

## CRESCIMENTO NA EXPOSIÇÃO DE ACESSO REMOTO



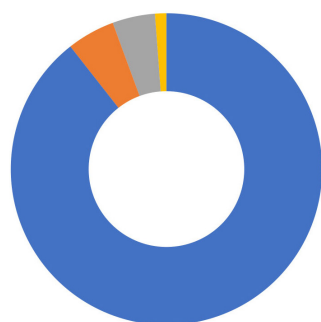
**40%**  
entre 2020 e 2021

## AUMENTO DOS GASTOS COM CIBERSEGURANÇA



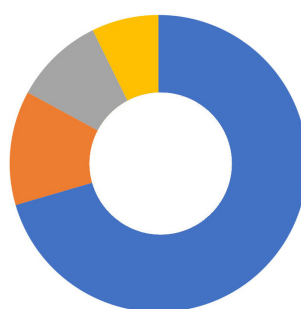
**60%**  
entre 2014 e 2020

## VULNERABILIDADES POR TIPO DE ATIVO



- 89% - Infraestrutura
- 06% - Usuários
- 04% - Compliance
- 01% - Aplicações

## VULNERABILIDADES EM INFRAESTRUTURA



- 70% - Atualização
- 13% - Diversos
- 10% - Compliance
- 07% - Configuração

**70%**  
entre todas as vulnerabilidades detectadas estão relacionadas à falta de atualização de sistemas operacionais e softwares.

**69%**  
entre todas as vulnerabilidades detectadas ainda estão identificadas como pendentes de remediação.

**59%**  
das falhas de infraestrutura têm correção disponível há mais de 1 ano.

**28%**  
das falhas de aplicação estão relacionadas a vazamento de dados.

**27%**  
entre todas as falhas identificadas são corrigidas.

