

Perspectivas de SegInfo e Proteção de Dados na visão do TCU

Renato Braga
Diretor

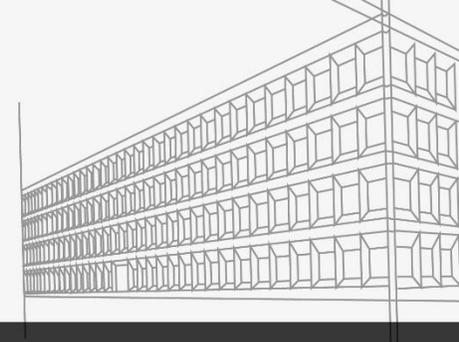
Diretoria de Avaliação de Segurança da Informação

Comissão de Serviços de Infraestrutura do Senado federal

Brasília - DF, 18/5/2023



Ransomware: a ameaça que bate à sua porta



Brasil é líder em ataques de ransomware na América Latina

Especialista faz alerta sobre melhores práticas que podem ajudar a prevenir, detectar, responder e recuperar-se de um ataque de ransomware

Por: Redação, 30/11/2022 às 16h36 - Atualizado em 30/11/2022 às 16h37

<https://www.securityreport.com.br/overview/brasil-e-lider-em-ataques-de-ransomware-na-america-latina/#.ZDa1MHbMKUK>

Brasil é 2º maior país afetado por ataques ransomware em 2022, aponta pesquisa

Por Redação - 7 de novembro de 2022

Já no primeiro semestre de 2022, o Brasil ficou atrás apenas dos Estados Unidos, chegando ao 2º lugar com mais de 19 milhões de casos registrados – pouco mais do dobro dos casos – frente a aproximadamente 136 milhões dos eventos nos EUA.

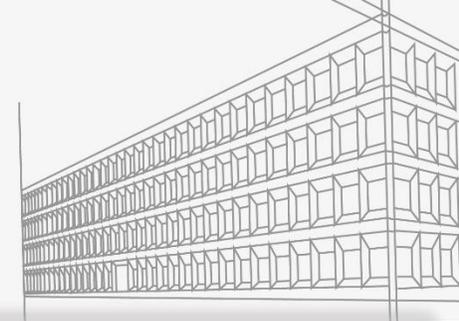
<https://tiinside.com.br/07/11/2022/brasil-e-2o-maior-pais-afetado-por-ataques-ransomware-em-2022-aponta-pesquisa/>

Metade dos ataques de ransomware teve sucesso no Brasil

Segundo o estudo, 58% das empresas brasileiras sofreram uma tentativa de ataque de ransomware no ano passado, com quase metade (46%) sendo bem-sucedido. De forma alarmante, 48% dos ataques de ransomware em períodos diferentes.

<https://www.convergenciadigital.com.br/Seguranca/Metade-dos-ataques-de-ransomware-teve-sucesso-no-Brasil-62669.html?UserActiveTemplate=mobile>

...e a situação só piora!



SOPHOS

Brasil lidera pagamento de resgate de Ransomware

Por: Matheus Bracco, 10/05/2023 às 17h09 atualizado em 12/05/2023 às 15h12

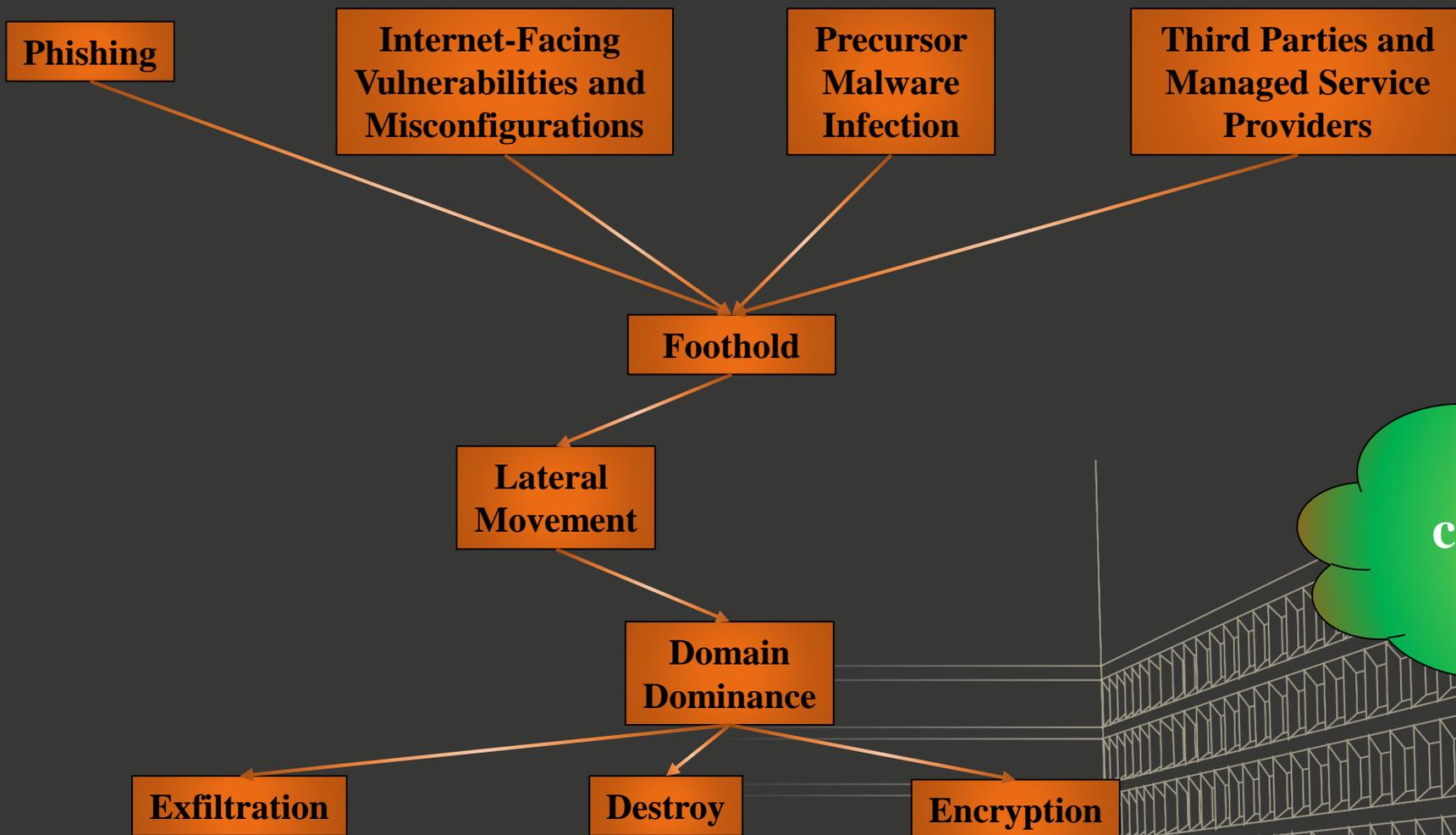
De acordo com estudo elaborado pela **Sophos**, o grande número de extorsões bem-sucedidas no país pode acarretar um aumento nos incidentes envolvendo esse malware, colocando o **Brasil no mesmo patamar de incidentes da Europa e dos Estados Unidos**

https://www.securityreport.com.br/destaques/brasil-lidera-pagamento-de-resgate-de-ransomwre/?utm_campaign=sr_daily_-_100523&utm_medium=email&utm_source=RD+Station#.ZGlrSXbMK3B

The State of Ransomware 2023

Findings from an independent, vendor-agnostic survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries, conducted in January-March 2023.

Anatomia de um ataque *ransomware*

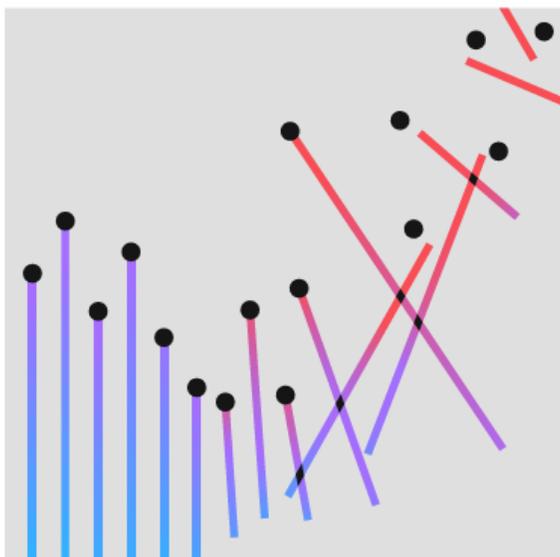


Defesa em camadas é uma necessidade

O que são APT? (Advanced Persistent Threat)

IBM Security

Relatório de custo da violação de dados de 2022



IBM

Tempo médio para identificar e conter uma violação de dados

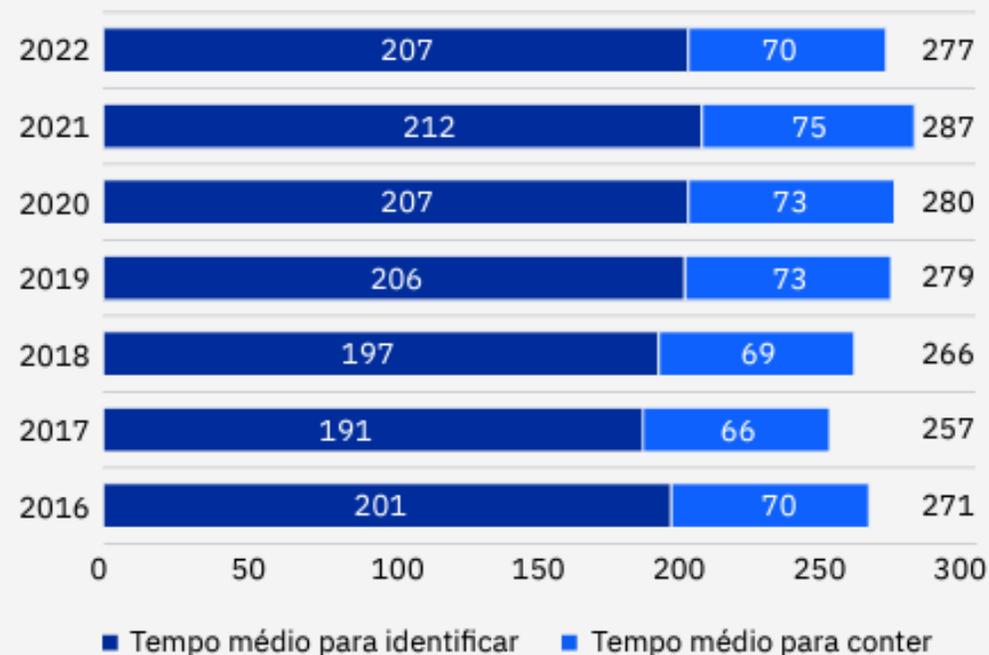


Figura 8: Mensurado em dias

O agente de ameaça não é amador...

APT são organizações bem estruturadas...

- Financiados para custear pessoas, ferramentas e equipamentos

Já é realidade (Ca...

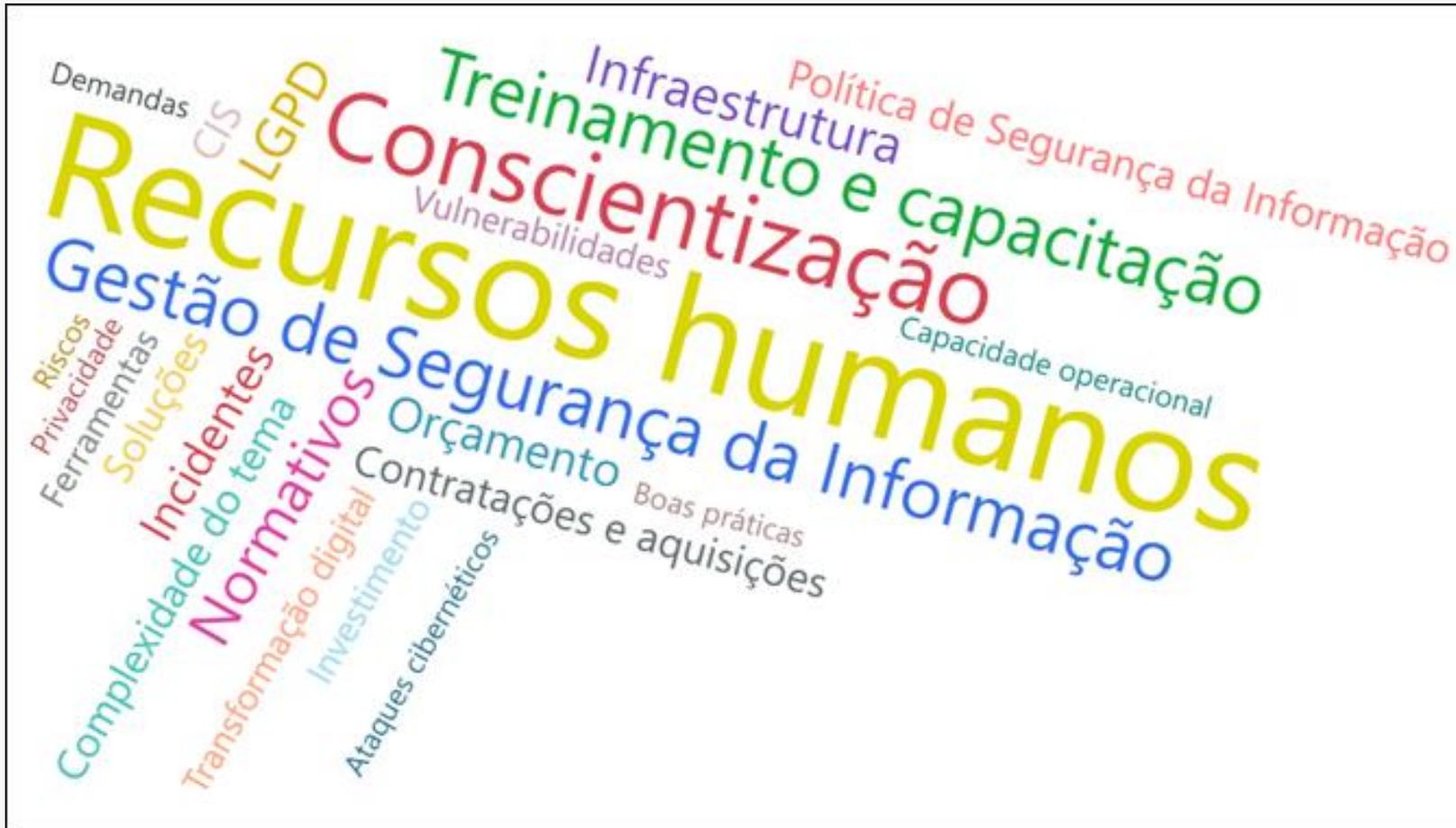
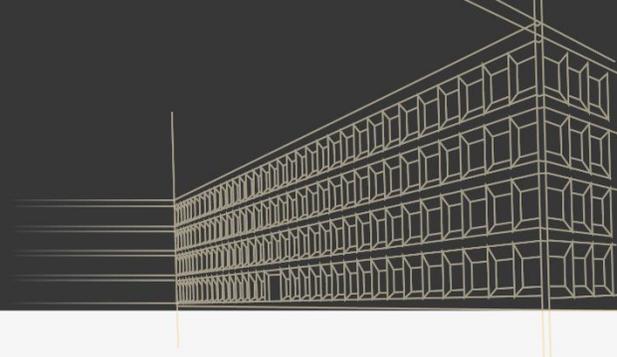
service

um em

Está desequilibrado o "combate" entre atacantes e defensores no mundo digital.

...as, mento e serviços a outras pessoas.

Desafio: Prover pessoal



Diversos acórdãos sobre deficiências em **quantidade e qualificação** de recursos humanos em TI entre 2008 e 2019, em especial Acórdão 1200/2014-Plenário (Rel. Min. Raimundo Carreiro)

Desafio: Implementar Controles Críticos de SI e SCiber

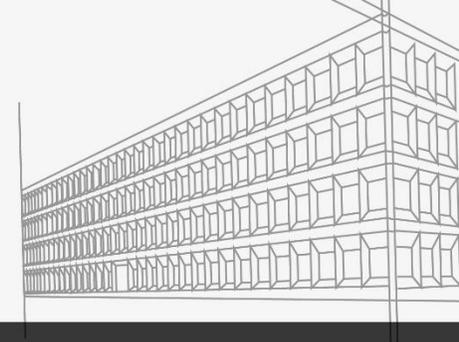
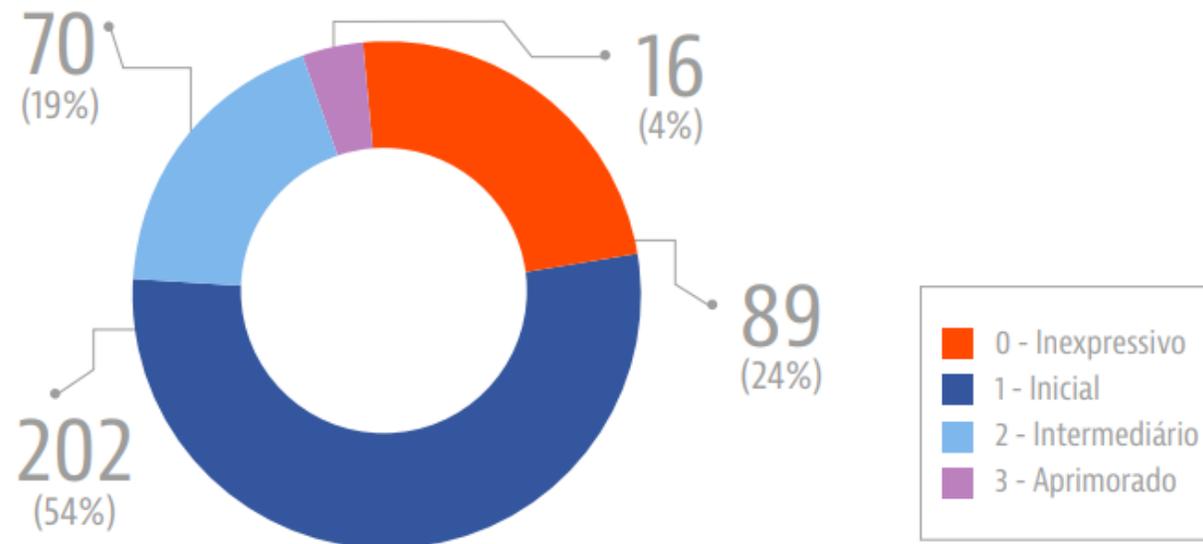


Gráfico 1: Distribuição das organizações em função do nSegCiber

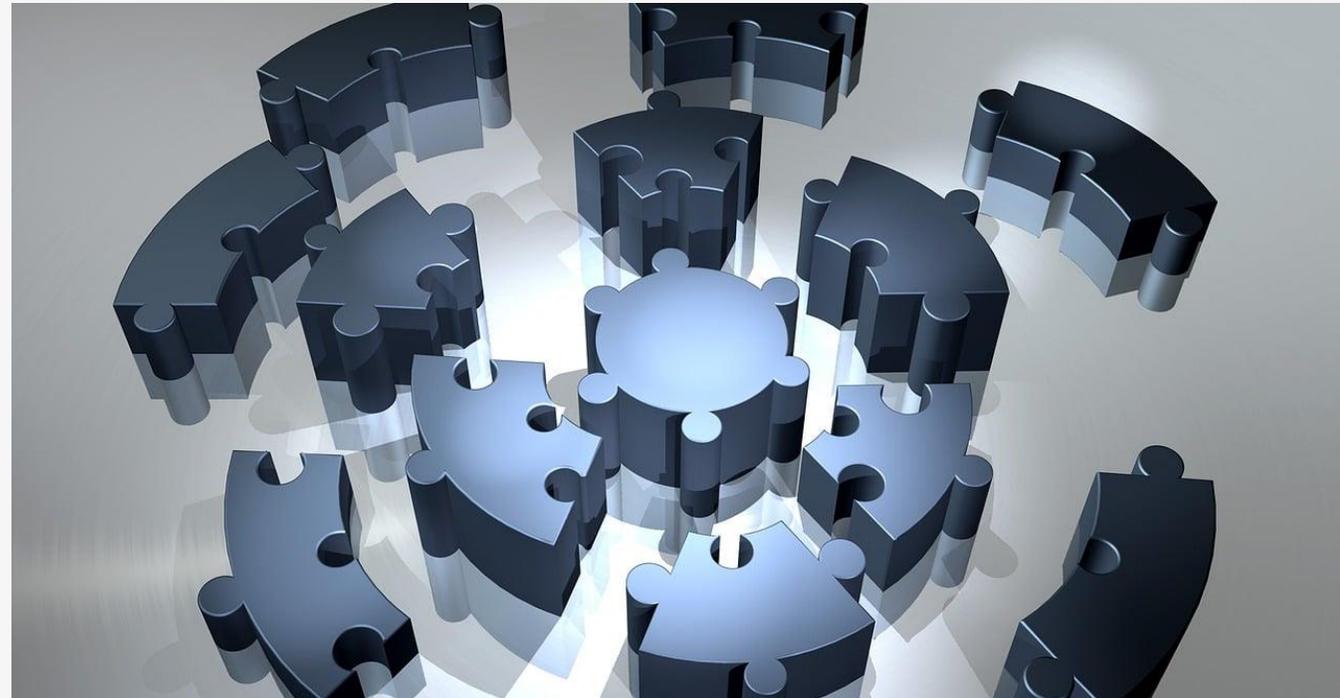


Fonte: Elaboração própria.

Fonte: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E7FF0EF4B0182B8F5CE4A3D8D>, com base no relatório do Acórdão 1.768/2022-Plenário (Rel. Min Vital do Rêgo)

Desafio: Liderança para Governança e Articulação

- Fragmentação
 - PNSI: [Decreto 9.637/2018](#)
 - PNSIC: [Decreto 10.569/2020](#)
 - ENSEC-PJ: [Res-CNJ 396/2021](#)
 - MP: Em estudo
- Lacunas
 - Setor privado
- Sobreposição
 - PNSI: [Decreto 9.637/2018](#)
 - PNSIC: [Decreto 10.569/2020](#)



Fonte:

Fonte: Relatório do Acórdão 4.035/2020-Plenário (Rel.: Min. Vital do Rêgo)

Potenciais desafios: a serem confirmados (PROTEGE-TI 2023)



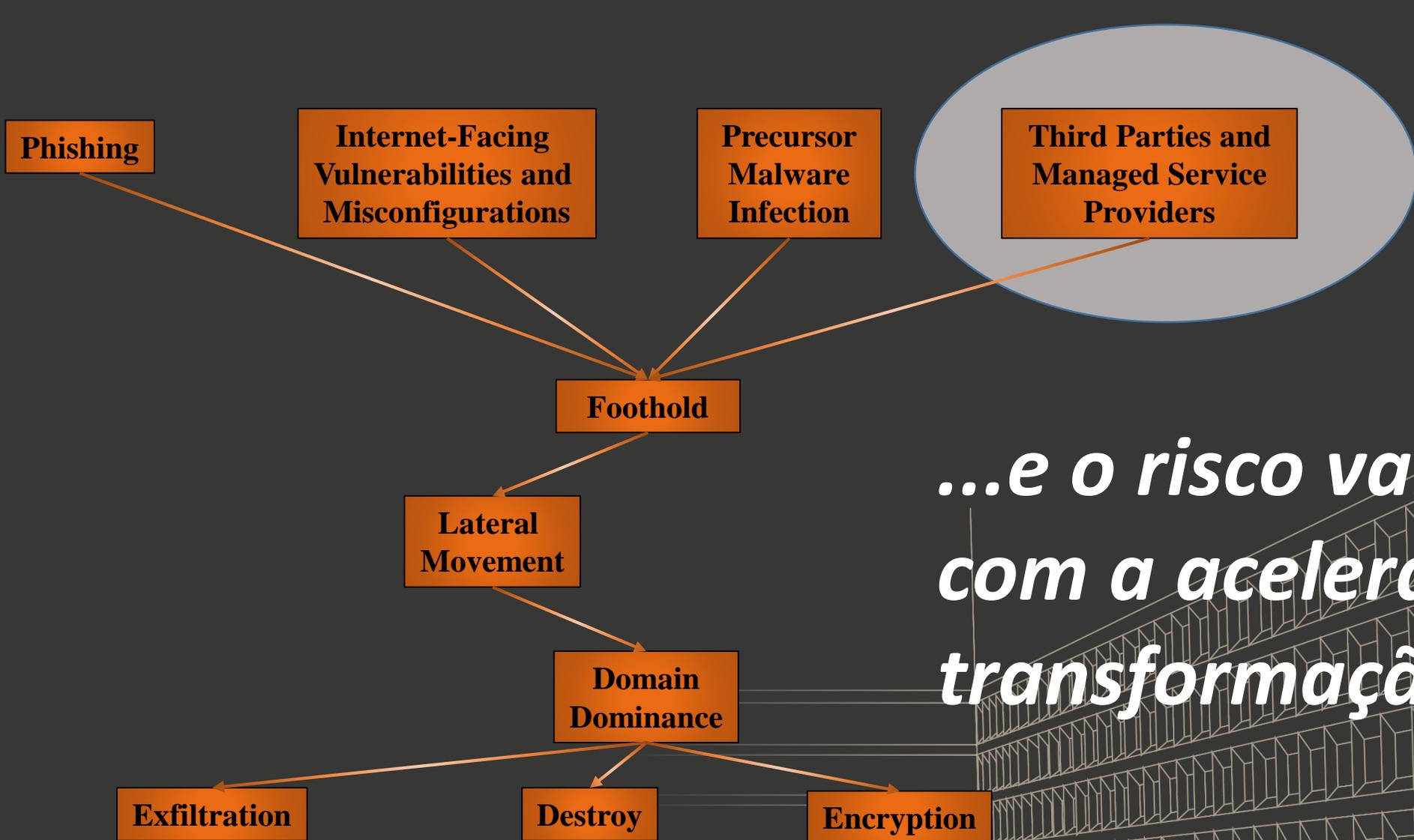
Implementação efetiva de
controles técnicos



Incorporar visão de
segurança ofensiva à defesa



AA liderar a Gestão de Riscos
de Segurança da Informação



...e o risco vai aumentar com a aceleração da transformação digital!

Segurança da Informação é responsabilidade coletiva



- APF: Administração Pública Federal
- AP: Administração Pública (3 esferas)
- IC: Infraestrutura Crítica

*Segurança da informação é tema que deve ser
priorizado na agenda de todo ESTADO
que deseje ser soberano.*

Reflexão

Obrigado!

audti@tcu.gov.br

Comissão de Serviços de Infraestrutura do Senado federal

Brasília - DF, 18/5/2023

