DESAFIOS DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM 2023

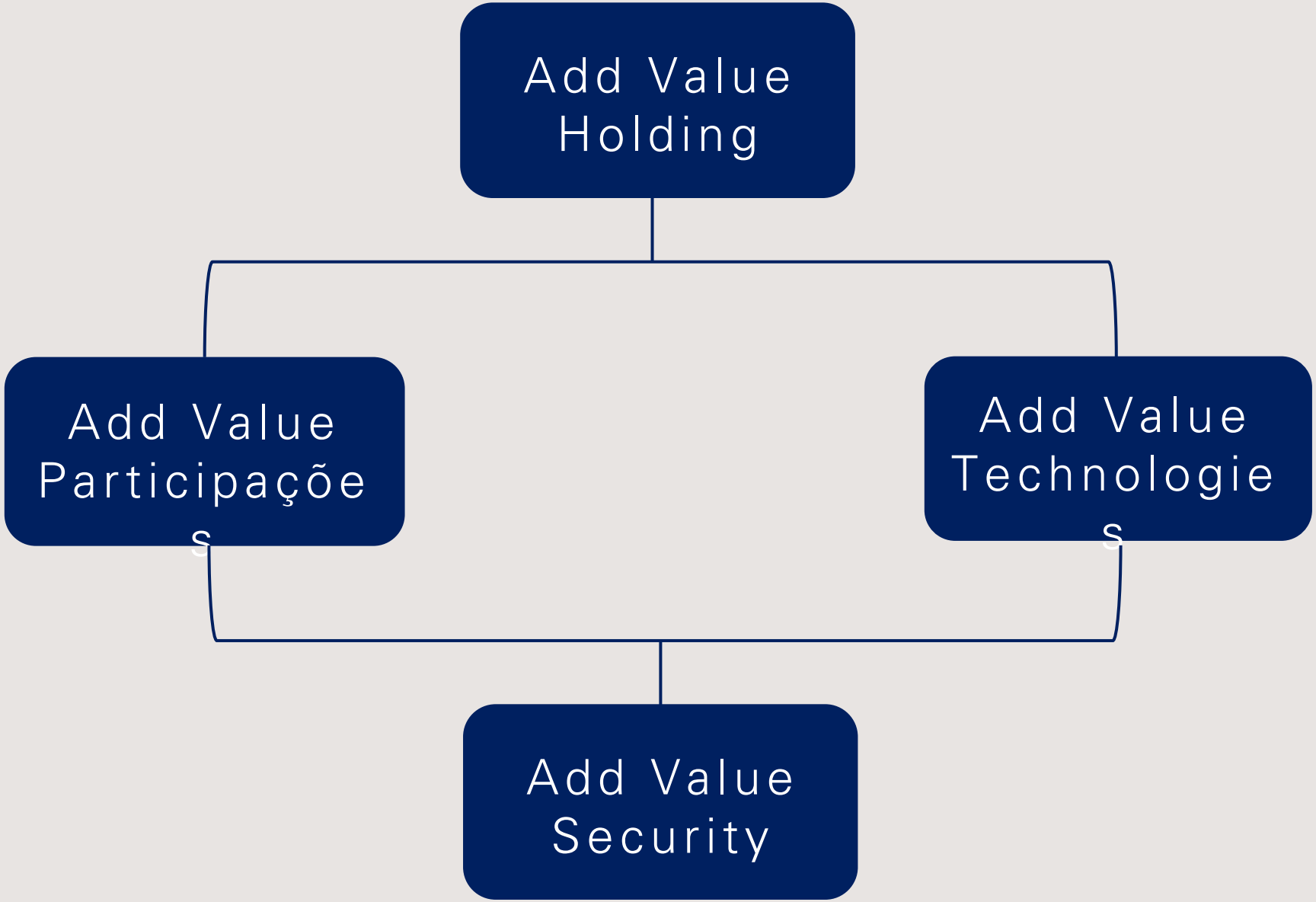
Isabel Silva – Sócia Diretora
Add Value Security

Fonte dos gráficos: Relatório custo de violação de dados 2022 da IBM-

QUEM SOU EU?

- Formada em Administração pela Escola Superior de administração de negócios
- Neta de Italianos
- Mãe de dois filhos
- Cachorreira
- Entusiasta do mundo de segurança da informação e com alguma experiência nesse mundo nele.

NOVA ESTRUTURA ADD VALUE



ABRANGÊNCIA

NACIONAL

Com sua matriz localizada em **São Paulo** e as regionais em **Belo Horizonte**, **Brasília**, **Curitiba**, **Rio de Janeiro** e **Fortaleza**, Somos hoje mais de 100 pessoas, sendo 35% envolvidos em serviços.

COMO FOI 2022 E O QUE NOS ESPERA EM 2023?

Valores analisar os números

Contexto Atual – Incidentes de segurança com repercussão na mídia*

- Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade

IBRASPD

RESULTADOS GLOBAIS DE 2022

- 83% das empresas pesquisadas, tiveram mais de uma violação
- 60% das empresas pesquisam , tiveram aumento de seus preços repassados aos clientes
- 19% das violações ocorreram através de um terceiro contratado
- 19% das violações ocorreram através de credenciais roubas ou comprometidas
- Custo médio global de um ataque de Ransomware foi de US$ 4, 54 milhões, sem contar o custo do resgate

Custo médio de uma violação de dados por país ou região

QUAIS FORAM OS FOCOS DOS ATAQUES EM 2022 E COMO NOS COMPORTAMOS?

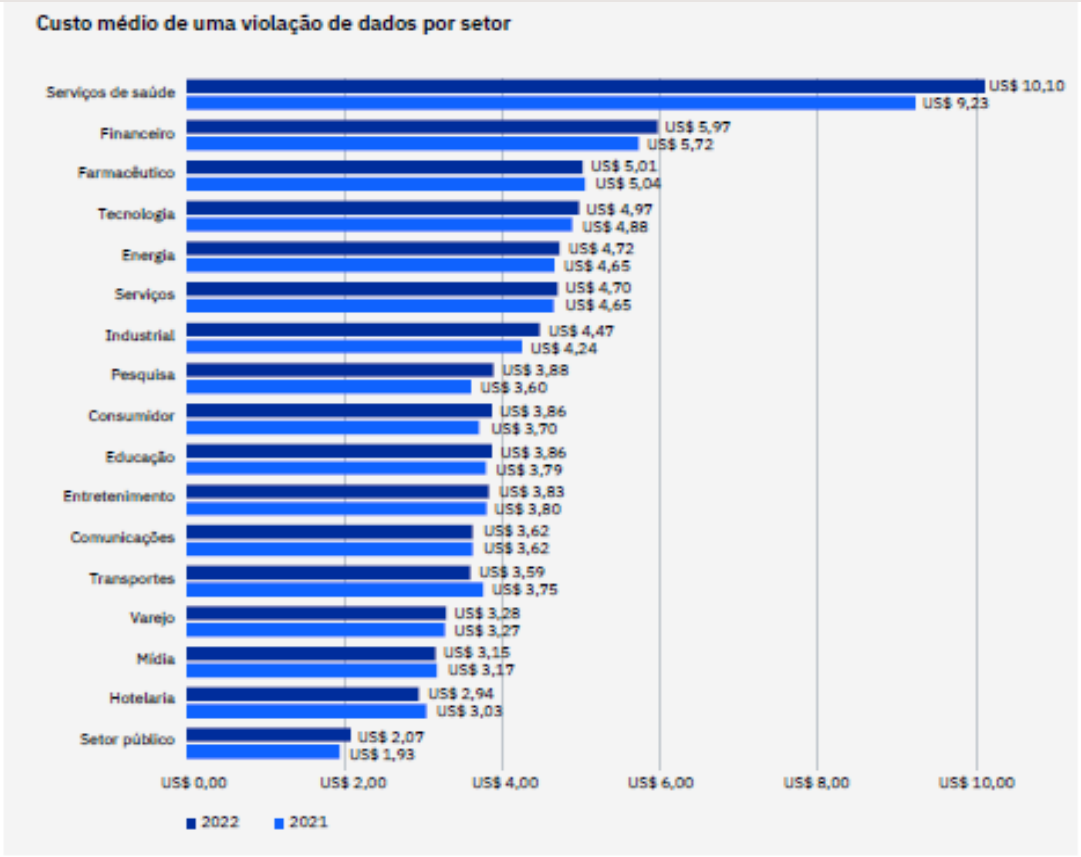
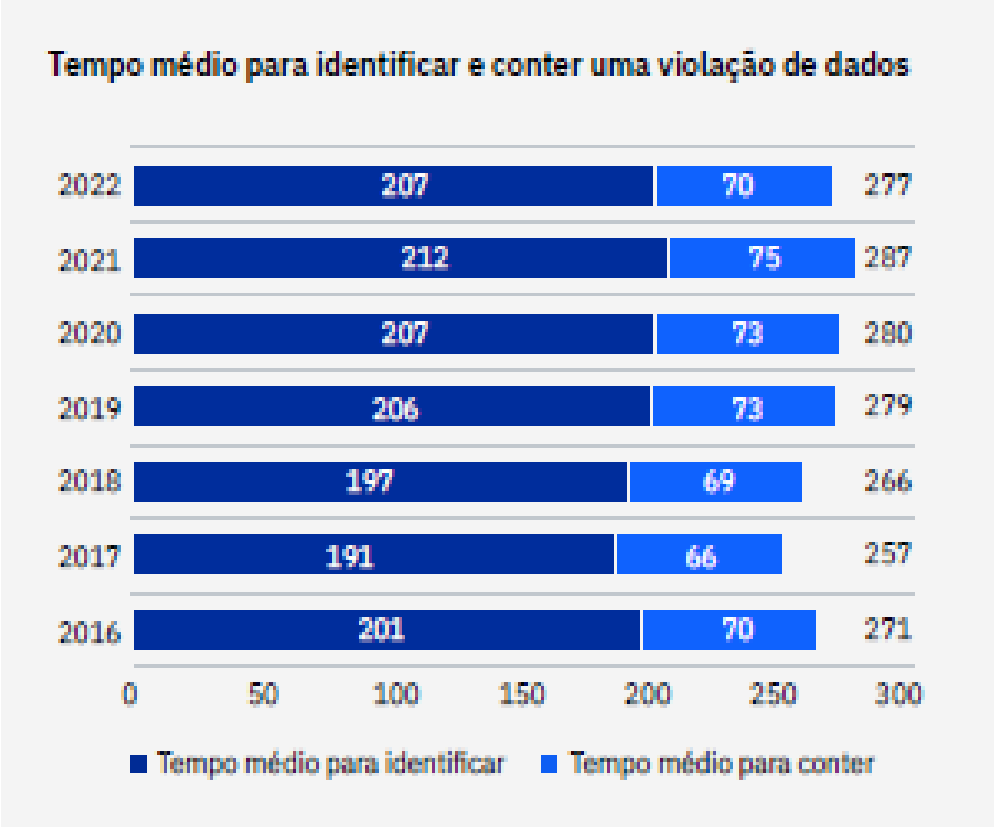


Figura 4: Mensurado em milhões (US$)



VETORES DE ATAQUES

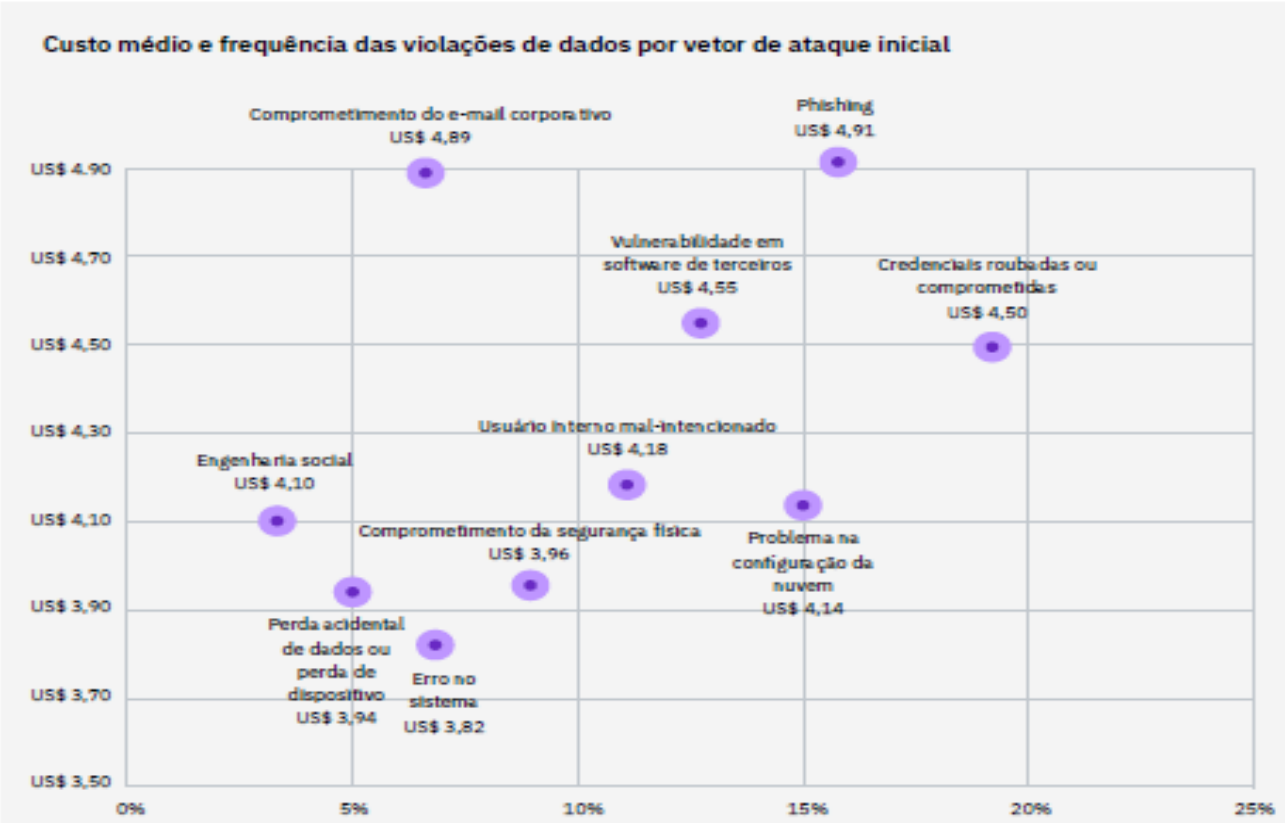


Figura 11: Mensurado em milhões (US$)

TEMPO MÉDIO PARA IDENTIFICARMOS POR VETOR DE ATAQUES

Contra quem estamos lutando?

Quem são os Hackers?

- Quadrilhas extremamente organizadas
- Utilizando tecnologias avanças
  - IA
  - ChatGPT

O que eles buscam?

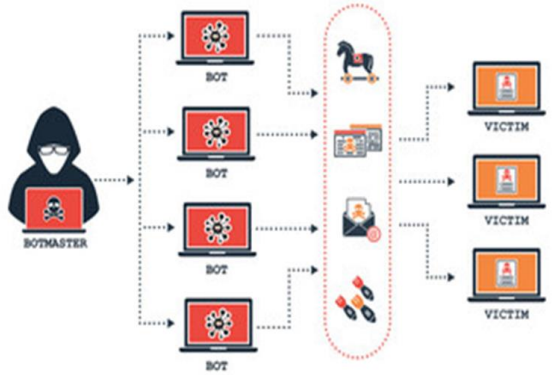
- Informações que possam ser vendidas
- Resgates

Com qual objetivo?

- Abastecer o crime organizado
- Guerras
- Redes direcionadas a violência

Como eles agem?

- Atráves de falhas humanas e tecnologicas, acessam nossas redes e instalam o malware/virus
  - Engenharia social
  - Senhas fracas
  - Acesso liberados voluntariamente
  - Acesso a links ou sites indevidos
  - Informações indevidamente compartilhadas
  - Atualização de software ou aplicações não realizados



O que é um Ransomware?

- O ransomware é um malware (programa malicioso) de extorsão – do estilo cavalo de troia – capaz de bloquear seu computador/banco de dados e, depois, exigir resgate para desbloqueá-lo. Daí seu nome (“ransom”, em inglês, significa resgate).
- Ao entrar num dispositivo, o malware pode bloquear o acesso ao sistema operacional ou criptografar arquivos. Geralmente, os cibercriminosos exigem dinheiro de resgate das vítimas para liberarem seus computadores.

Quais os tipos de Ransomware?

- Hoje temos mais de 25 tipos de Ransonware
  - Alguns dos mais utilizados
    - Crypto ransomware
    - Locker ransomware
    - Bad Rabbit
    - B0r0nt0k
    - CryptoWall
    - Doxware
    - Medusa

ANALISANDO ESSE CENÁRIO, O QUE ESPERAR DE 2023?

Não precisamos nos desesperar

GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Como direcionar nossas iniciativas?

Qual meu cenário atual?

Eu sei quais são os meus gaps?	Quanto eu tenho de orçamento?	Tenho visibilidade de tudo o que ocorre em minha rede?	Minha empresa tem consciência dos riscos que corremos?
Faço treinamento para meus usuários?	Consigo corrigir as vulnerabilidades de minha rede ou aplicações?	Minha equipe de TI consegue aplicar todos os patchs?	Como controlo o meu legado?

Identificando meus gaps

Definição do escopo

Assessment baseado em um framework de segurança

Analise dos riscos

Criação de um plano de ação

Envolvendo de todas as equipes incluídas no escopo

Envolvimento da gestão

SI tem que fazer parte do negócio

Segurança da informação e seus pilares:

Pessoas

Processos

Tecnologias

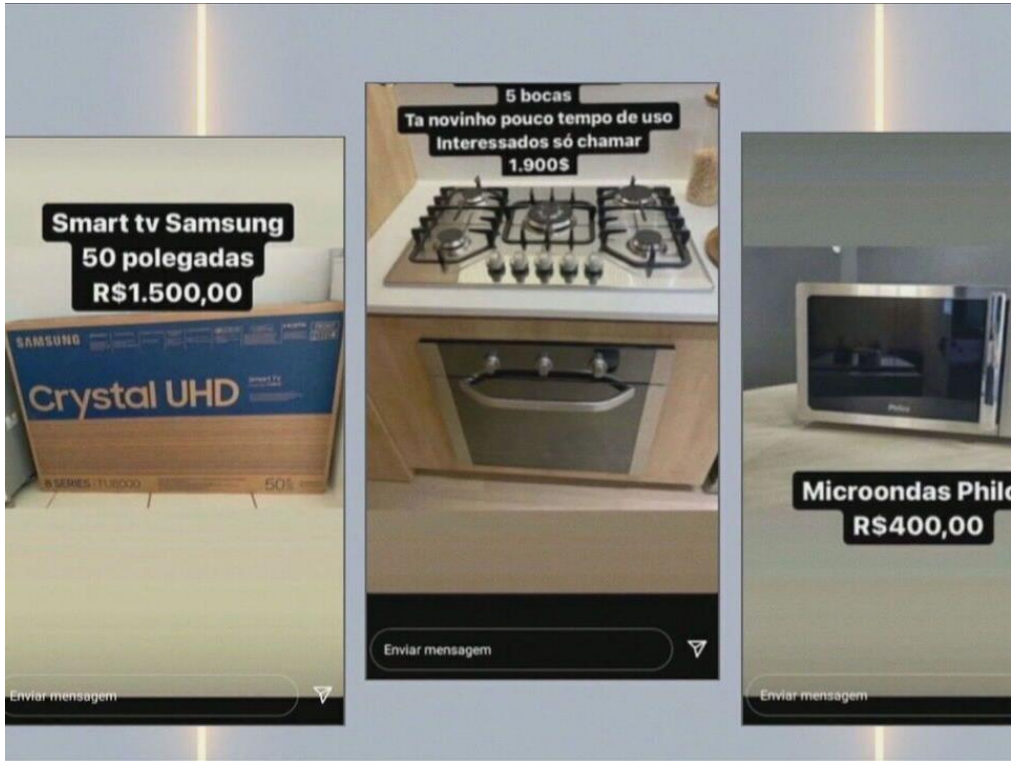
addvalue security

Pilar: Pessoas e a Engenharia Social

- Engenharia social é uma **técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados**.

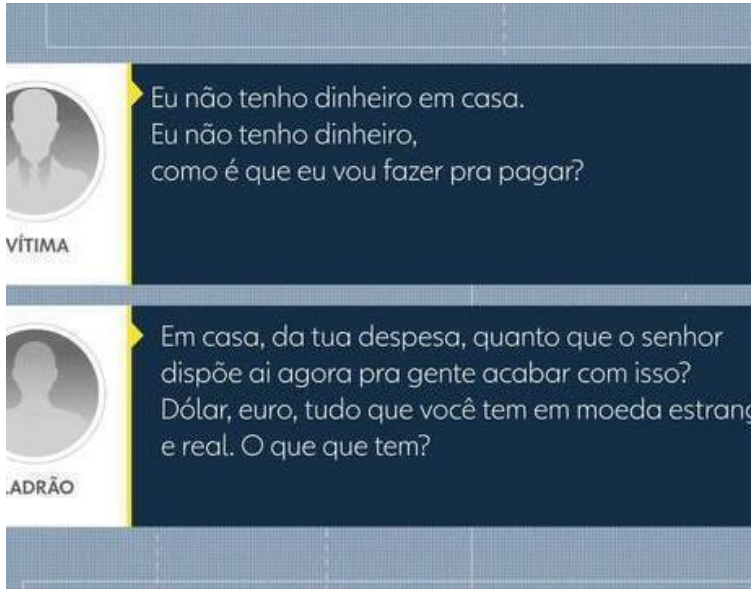
- Por meio da engenharia social, os criminosos cibernéticos usam a interação humana para manipular o usuário a divulgar informações confidenciais. Como a engenharia social **se baseia na natureza humana e nas reações emocionais**, os invasores utilizam várias táticas para tentar enganá-lo online e off-line.

    - Medo
    - Ganancia
    - Curiosidade


Smart tv Samsung
50 polegadas
R$1.500,00
SAMSUNG
Crystal UHD
5 bocas
Ta novinho pouco tempo de uso
Interessados só chamar
1.900$
Enviar mensagem
Microondas Philc
R$400,00
Enviar mensagem
Enviar mensagem


4h
dando casal de
amigos
uitas coisas a
venda
4h
Pessoal, um casal de amigos estão se mudando e precisam vender os móveis. Irei postar algumas coisas deles
Preço de desapego!
Chama no chat
4h
Ps5 1 tera com 2 controles
3.000$
Possui caixa e nota
Tudo funcionando perfeitamente e sem nenhum detalhe


12 min
GALERA, NOS PRÓXIMOS STORIES ESTAREI POSTANDO PRA UMA AMIGA ALGUNS ELETRODOMÉSTICOS E ELETRÔNICOS NO PREÇO SUPER ACESSÍVEL, TODOS OS PRODUTOS COM GARANTIA E NOTA FISCAL!!! (MINHA AMIGA ESTÁ DE MUDANÇA DE PAÍS E ESTÁ VENDENDO AS COISAS DELA).
10 h
IPhone 11 Pro Max 2
Meses de uso 512gb Na garantia
Valor 2.500


Eu não tenho dinheiro em casa.
Eu não tenho dinheiro,
como é que eu vou fazer pra pagar?
VÍTIMA
Em casa, da tua despesa, quanto que o senhor dispõe ai agora pra gente acabar com isso?
Dólar, euro, tudo que você tem em moeda estran
e real. O que que tem?
ADRÃO

Redes sociais

- Quais são os perigos:
  - Exposição excessiva
  - Informações pessoais expostas
  - Fotos comprometedoras
  - Exposição de crianças
  - Fake news

Como me proteger nas redes sociais?

- Não exponha informações confidenciais
  - Onde trabalha
  - Onde mora
  - Endereço de eventos
  - Telefones
  - Escola dos filhos
- Seja seletivo em aceitar seguidores
- Configure a rede como privada
- Não compartilhe informações sem checar
- Bloqueie imediatamente contas falsas
- Controle quem pode acessar suas informações

Como me proteger nas redes sociais?

- Coloque senha fortes
- Cuidado com contas que darão acesso a outras
- Não acesse links que você não conhece ou enviados por pessoas que você não conhece
- Cuidado com presentes ou facilidades
- Use todas as configurações de segurança oferecidos pelas redes sociais
- Lembre-se, eles podem unir várias informações suas para utilizar no golpe
- Nada cai do céu

Cuidados com a sua senha

Não compartilhe as suas senhas

- Caso necessite compartilhar, altere logo em seguida

Troque periodicamente (90 dias)

Não utilize senhas fáceis

- Datas de aniversário
- Nome do animal de estimação

Coloque sempre caracteres $*@

Não deixem anotados em cadernos, papéis

- Existem aplicativos que podem controlar as senhas
- Duplo fator de autenticação

Não utilizem a mesma senha para todos os aplicativos ou redes sociais

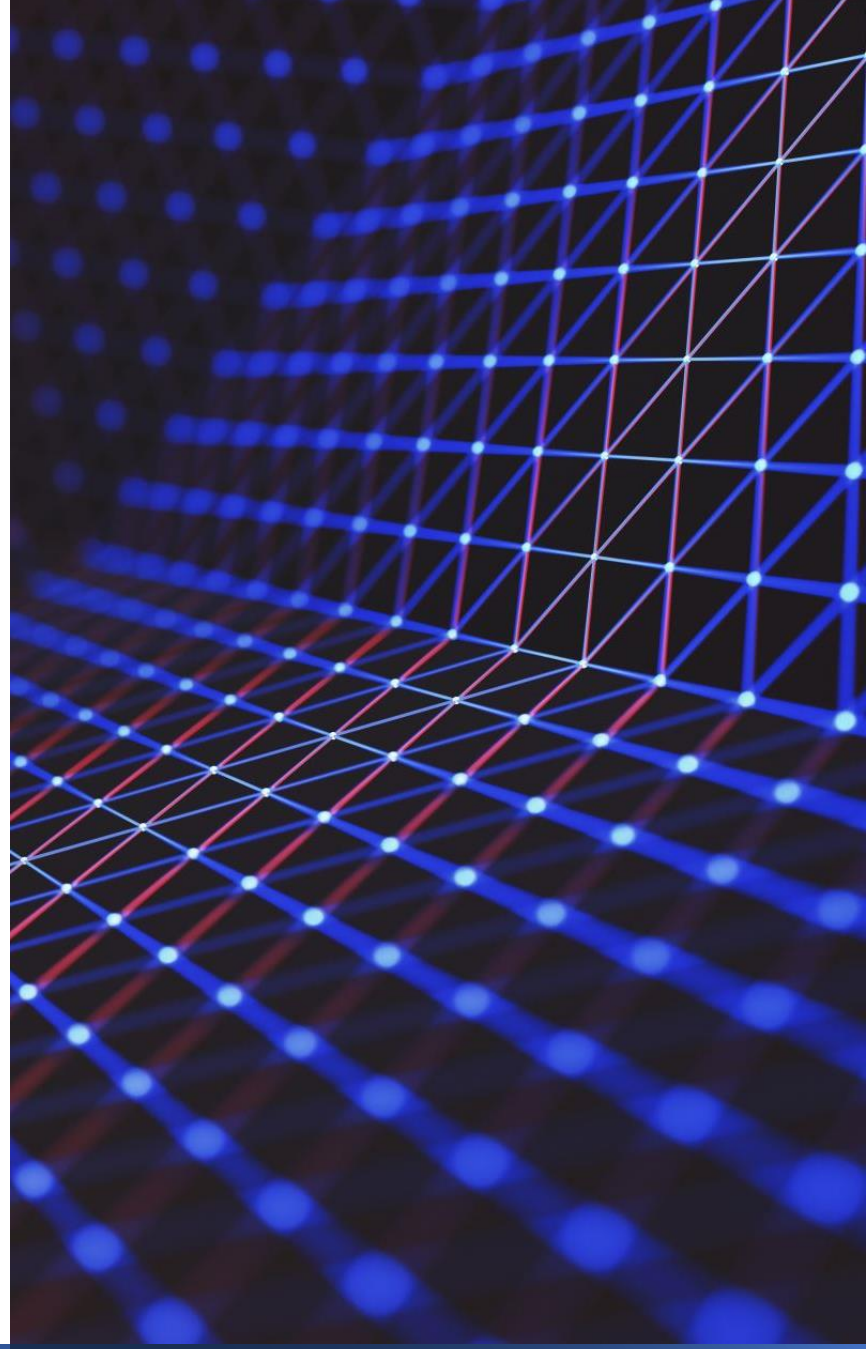
Como controlar engenharia social como gestor?

- Treinamento, Treinamento e Treinamento
- Ferramentas que possam identificar BEC, Phising
- Fazer com que o usuário entenda a importância dele
- Campanhas de conscientização
- Envolvimento de todos os gestores

addvalue security

Como todos podem colaborar ?

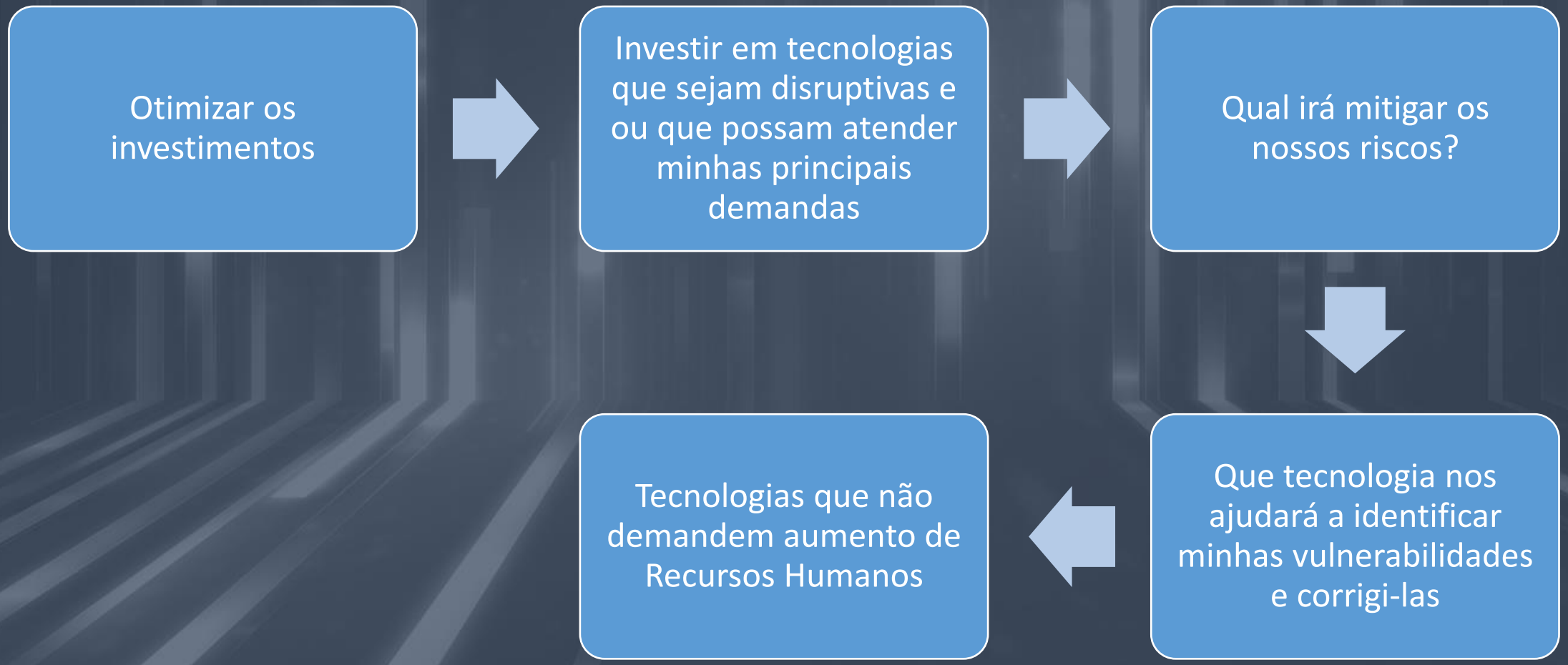
Façam todos os treinamentos determinados pela equipe de segurança/RH.	Não acessem links enviados através de emails sem validar a criticidade	Troquem as senhas de acordo com a politica da empresa	Sigam os processos determinados
Estejam sempre atualizados sobre a política de segurança da empresa	Não fale sobre a empresa em suas redes sociais (deixe que a empresa administre as redes sociais da empresa)	Não compartilhem informações sobre o andamento da empresa, projetos, tecnologias, informações industriais.	Evitem comentários sobre a empresa em locais públicos
Não acessem a rede da empresa em wi-fi inseguros, sem controles de acessos	Não permitam que terceiros acessem a rede da empresa, sem autorização.	Não utilizem os computadores da empresa para jogos, redes sociais ou sites públicos sem autorização	Não eliminem qualquer item de segurança de seus computadores que acessem a rede da empresa



Pilar - Processos

- Politica de segurança da informação
  - Base para qualquer gestão de SI
- Controle de acessos (quem acessa e o que acessa)
  - Físicos ou lógicos
- Troca de senhas (periodicidade)
- Sites acessados
- Informações enviadas com segurança
- O que pode ser compartilhado ou não

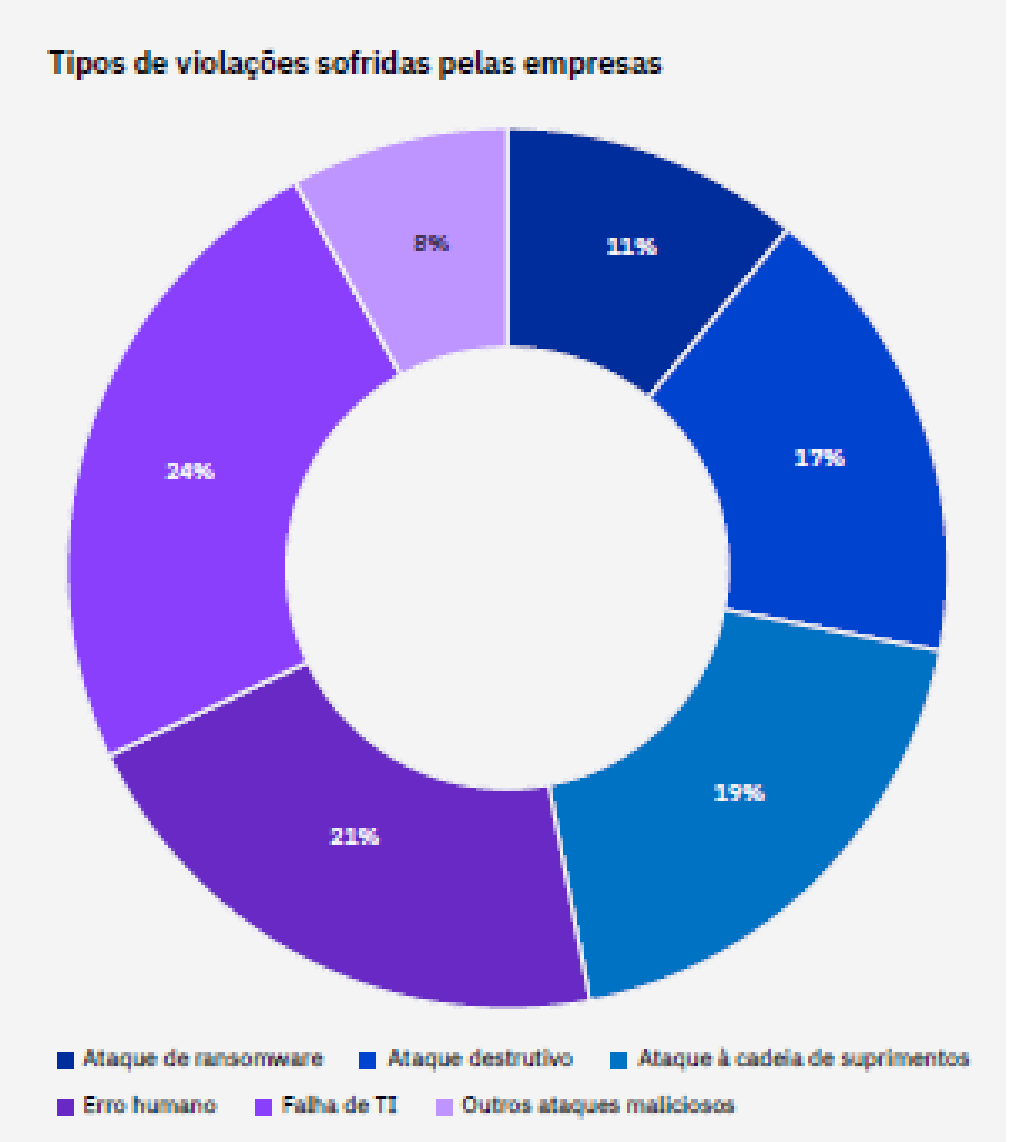
Pilar tecnologia- Em que devemos investir?



O que os números nos dizem sobre em que investir?

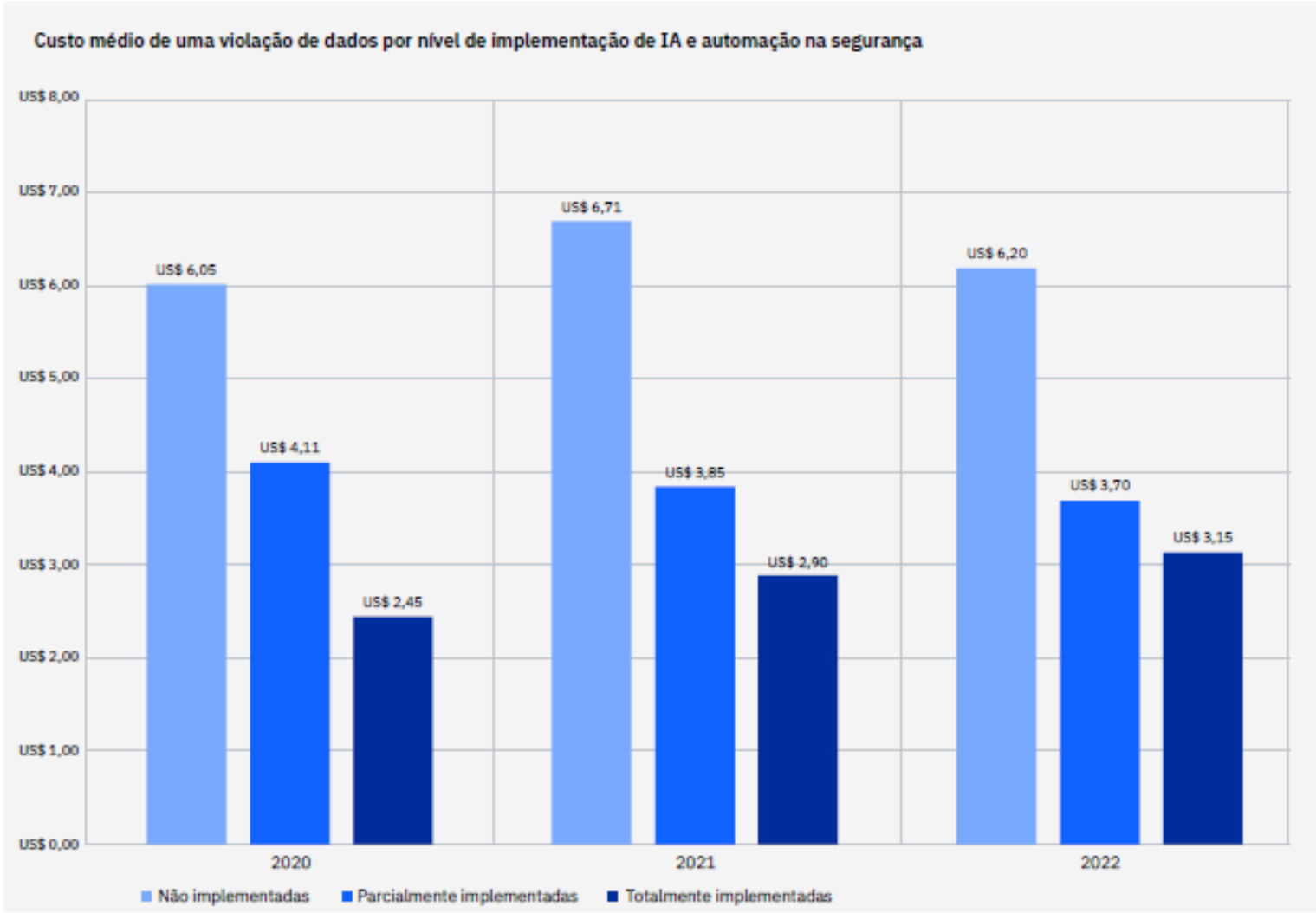
- Ransonware foi o ataque que mais cresceu nos ultimos anos
- Falha em TI, que basicamente refere-se a vulnerabilidade/ou patchs não aplicados, segue sendo o principal fonte de ataques com erros humanos

Tudos isso nos mostra mais uma vez que pessoas, processos e tecnologias são o caminho.



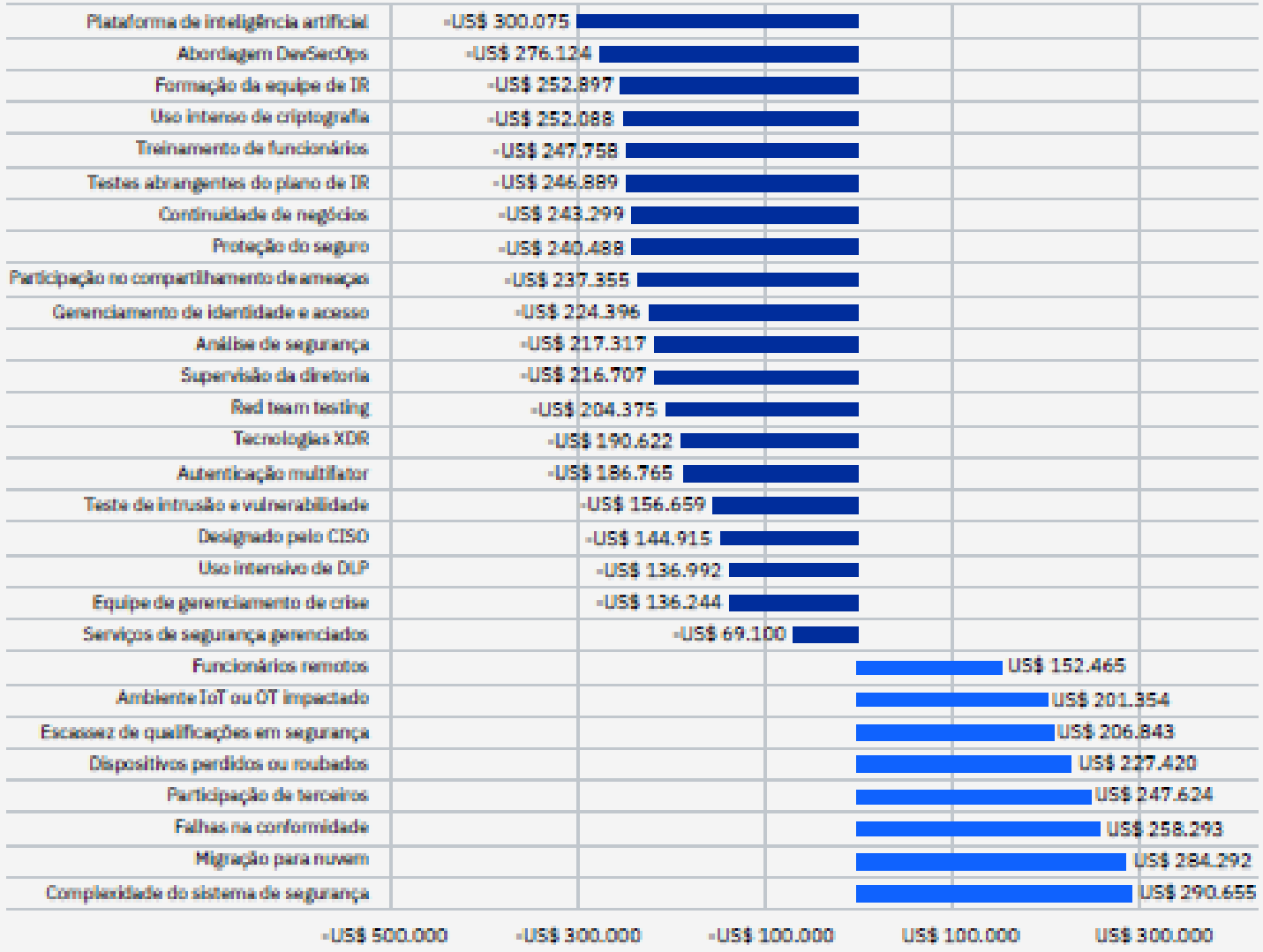
addvalue security

Investimento em IA segue sendo o melhor caminho

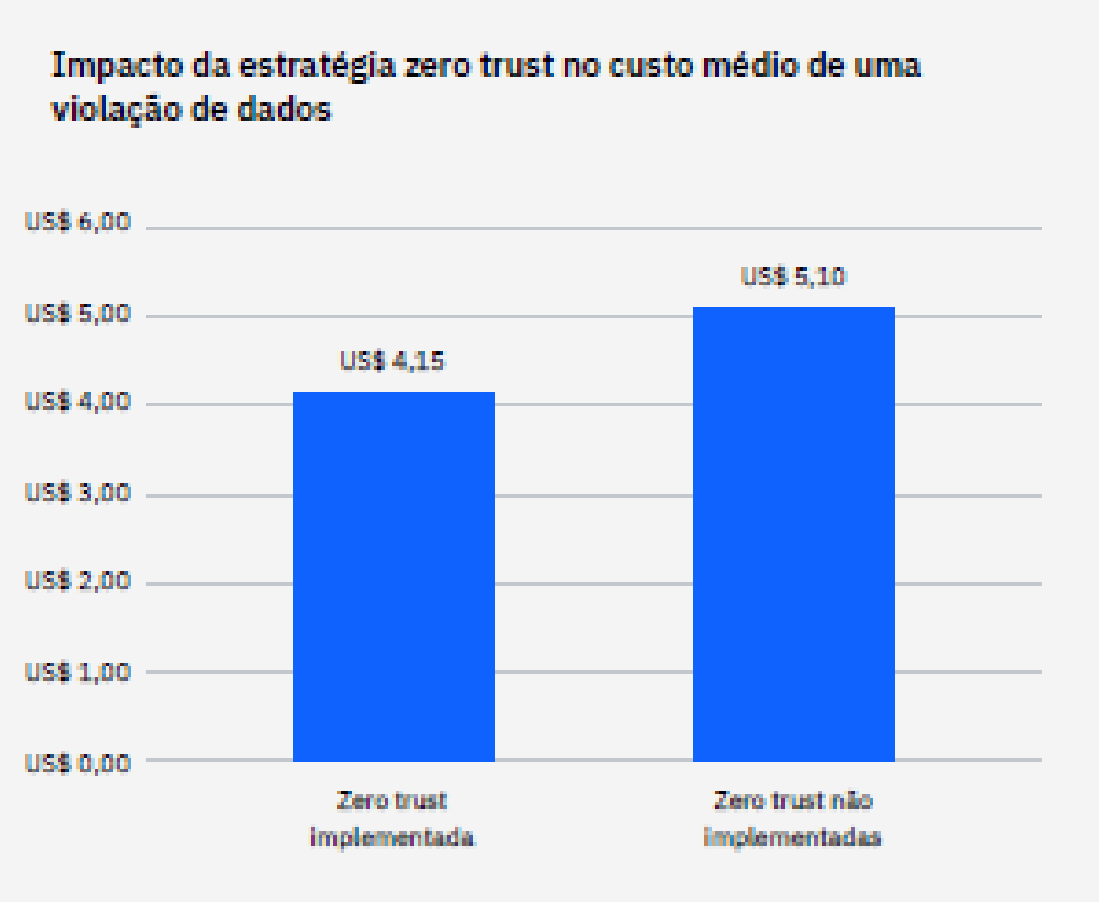


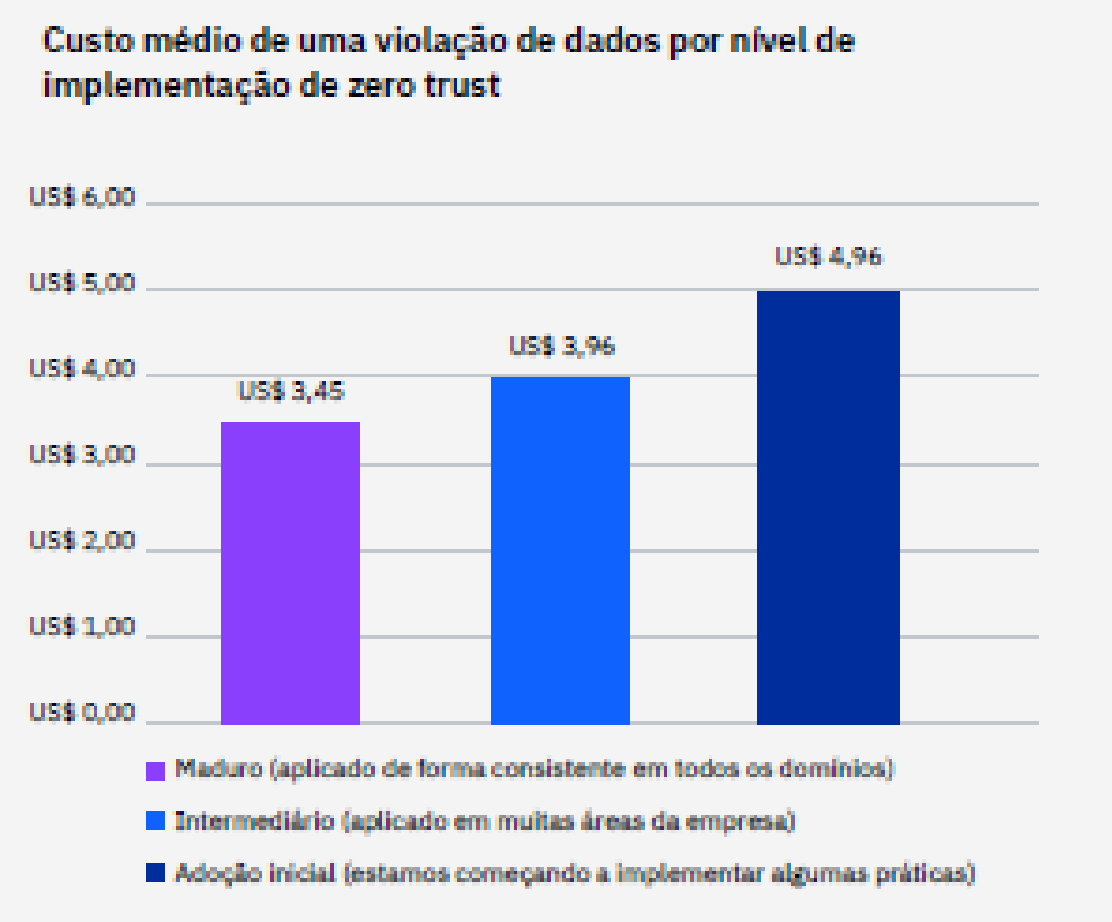
addvalue security

Impacto de fatores-chave no custo médio total de uma violação de dados



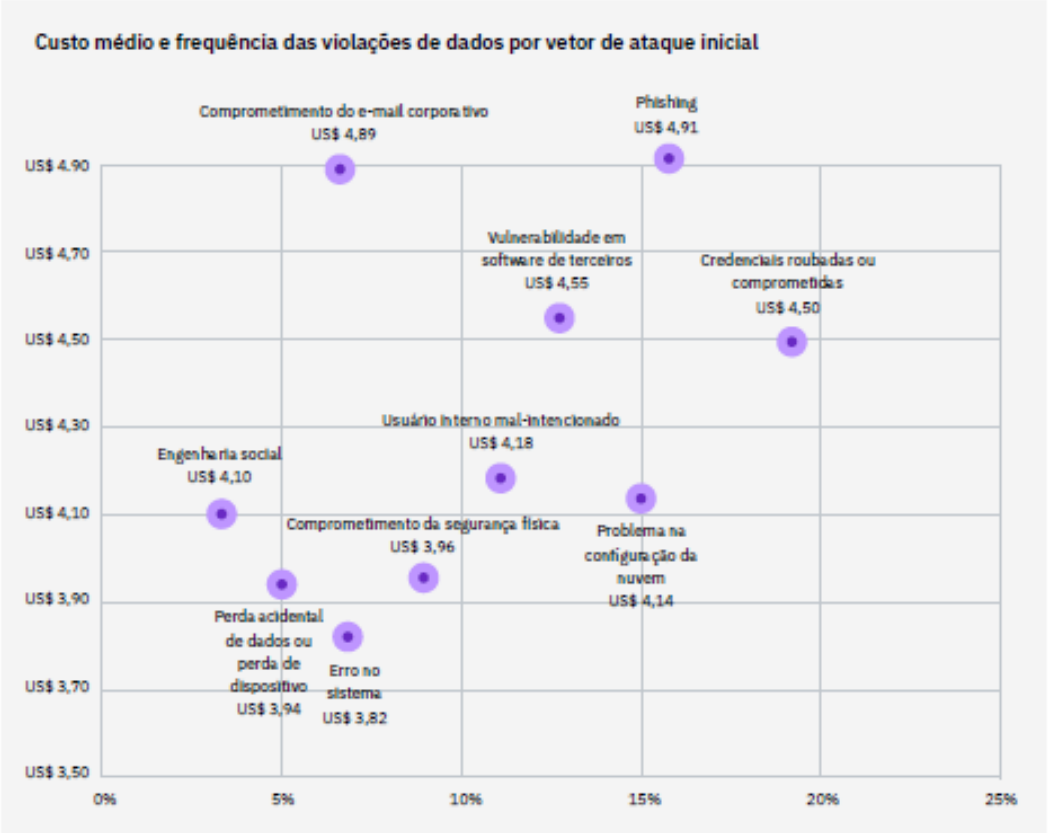
O Conceito Zero Trust- Uma estratégia





Analisando os vetores de ataques

- Tecnologia para segurança dos emails são fundamentais
  - US$ 9,9 milhões de custo médio por violação
- Gestão de vulnerabilidade
  - Fundamental na gestão de SI
- Engenharia social classificada entre as principais violações



Qual o nosso papel como gestores de SI?

Conscientizar a empresa/órgão da atual situação

- Não queira assumir tudo

Criar um plano de segurança da informação para aumentar a maturidade

Alinhamento total com TI

Exigir que a politica de segurança da informação seja criada e aplicada

Estar sempre atualizado com o que está acontecendo no mercado

- Muitas vezes não precisamos reinventar a roda

Quebrar alguns paradigmas

Investir na tecnologia correta para as suas necessidades

Criar um programa constante de treinamentos

Orçamento de SI deve ser direcionado as suas necessidades anuais e plano de ação

Tolerância Zero a falta de segurança

O desafio é de todos nós!

Muito obrigada pela oportunidade.

Nossos contatos

- Isabel Silva
  - Isabel.silva@addvalue.com.br
    - 11 99160 5315
- Pablo Gazitua
  - Pablo.Gazitua@addvalue.com.br
    - 85 98143 8080
- Ronald Studart
  - Ronald.Studart@addvalue.com.br
    - 85 99985 7500