



Segurança da Informação: Fatores Humanos e Neuro Cognitivos

ABOUT ME



[linkedin.com/in/thaispedrosog](https://www.linkedin.com/in/thaispedrosog)



thais.pedroso@gmail.com

Formação:

- ✓ **Tecnóloga em Gestão de Redes de Computadores e Internet – UNINOVE**
- ✓ **MBA em Gestão de Segurança da Informação – FIAP**
- ✓ **Cursando pós – graduação em Neurociência e Desenvolvimento - FAAP**

Background:

- ✓ **21 anos como profissional de Segurança da Informação e Auditoria de TI/Cyber no setor bancário (Brasil e Exterior).**
- ✓ **Especialista em Prevenção a Lavagem de Dinheiro, Gestão de Continuidade de Negócios e Gestão de Riscos de Cybersecurity.**

Certificações:

- ✓ **ISFS | ISMAS ISO/IEC 27002; COBIT 2019; ITIL V3; CSFPC™v.1.0; ISO/IEC 27001 Internal Auditor - I27001IA;**
- ✓ **CAMS Certified Anti-Money Laundering Specialist; Information Systems Auditing, Controls and Assurance - The Hong Kong University of Science and Technology; Audi TI - IIA**

Membro:

- ✓ **Instituto de Defesa Cibernética**
- ✓ **The Institute of Internal Auditors**

Agenda

1. Introdução
2. Perspectivas de crescimento/investimentos em Cybersegurança
3. Incidentes Cibernéticos
4. O fator humano na Segurança da Informação
5. Cérebro Humano e Viéses inconscientes
6. Evitando Golpes Digitais



Introdução



Processos

- Políticas;
- Diretrizes;
- Procedimentos, etc.

Pessoas

- Treinamentos;
- Conscientização

Tecnologia

- Controles técnicos;
- Ferramentas (firewall, antivírus, sistema de controle de acessos, etc.)

Perspectivas de crescimento/investimentos em Cybersegurança

Segurança cibernética: a perspectiva do investimento

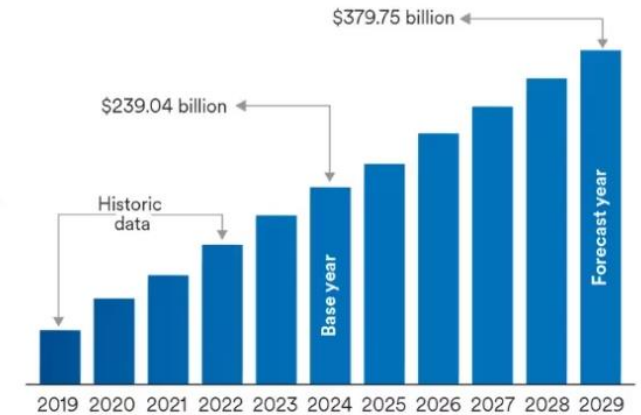
A demanda por segurança cibernética cresceu enormemente nos últimos anos, com gastos previstos para ultrapassar US\$ 200 bilhões em 2024. Mas uma abordagem seletiva para investir no setor continua sendo essencial.

Global cyber security market

Market size overview

9.7%

Global market
CAGR
2024 – 2029

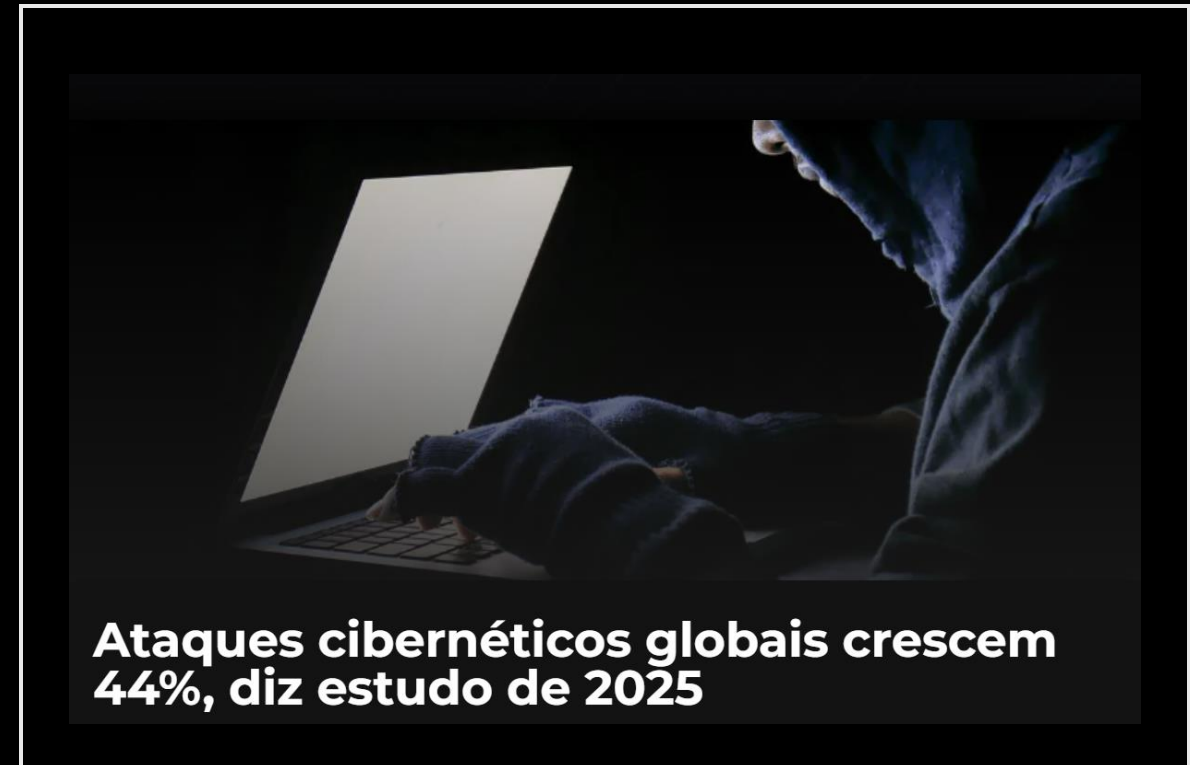


Fonte: <https://www.schroders.com/en/global/family-offices/insights/cyber-security-the-investment-perspective/>

Incidentes Cibernéticos



<https://minutodaseguranca.blog.br/brasil-e-o-2o-no-ranking-de-paises-mais-atacados/>



<https://ibsec.com.br/ataques-ciberneticos-globais-crescem-44-diz-estudo-de-2025/>

SEGURANÇA

Erro humano contribuiu para 95% das violações de dados em 2024, revela pesquisa

Alguns dos maiores ciberataques de 2024 começaram com falhas de funcionários de grandes empresas



André Luiz Dias Gonçalves
15/03/2025, às 16:00



Fonte: Getty Images

Polícia Civil prende em SP suspeito de ataque hacker ao sistema que liga bancos ao PIX

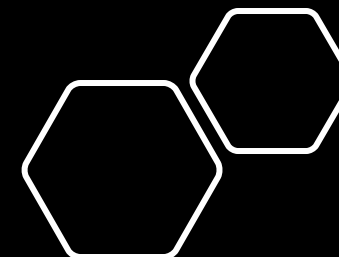
Segundo os investigadores, ele é funcionário de uma empresa que conecta bancos menores aos sistemas PIX do BC e deu aos hackers a senha ao sistema sigiloso.

Por Bruno Tavares, * TV Globo e g1 SP — São Paulo
04/07/2025 07h46 · Atualizado há 3 meses

BC informa ataque hacker contra C&M Software, que interliga bancos aos seus sistemas e ao PIX

Incidente permitiu acesso indevido a contas de reserva de pelo menos seis instituições financeiras. A Polícia Federal (PF) deve abrir um inquérito para investigar o caso.

Por Redação g1 — São Paulo
02/07/2025 11h30 · Atualizado há 3 meses



O Fator
Humano na
Segurança da
Informação...

... é o elo mais frágil!



Principais ataques cibernéticos

Vetores que dominaram 2025



BEC / Spear-Phishing

57% dos ataques

T1566.002 - Spearphishing Link



Erro humano

46% dos ataques

T1204 - User Execution



Exploits de vulnerabilidade

31% dos ataques

T1190 - Exploit Public-Facing App



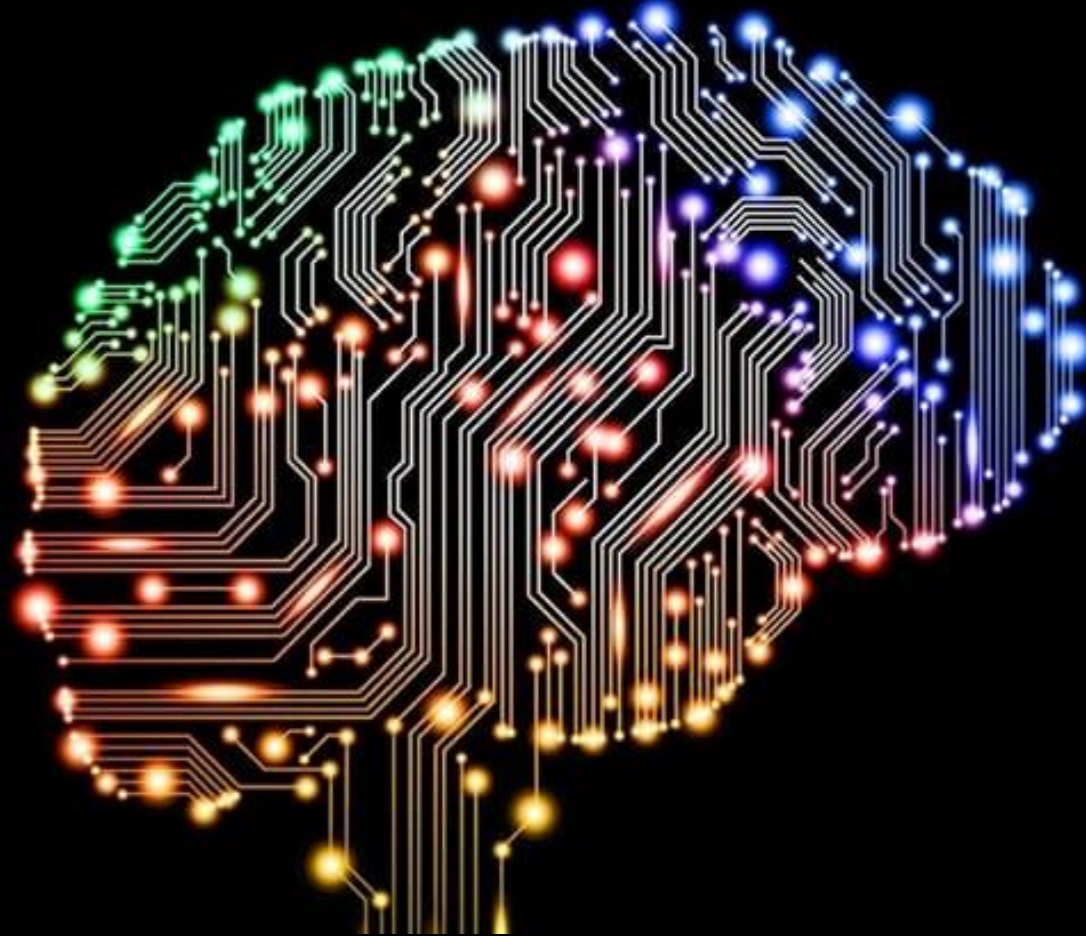
Ransomware

24% dos ataques

T1486 - Data Encrypted for Impact

Fonte: Hiscox Cyber Readiness Report 2025

Segurança das Informações e o Comportamento humano



O Cérebro Racional: Córtex Pré-Frontal

Córtex Pré - Frontal



- Tomada de decisões
- Cognição
- Foco e Concentração
- Planejamento estratégico
- Avaliação de sucesso ou fracasso
- Memória e aprendizagem
- Senso crítico, avaliação das consequências
- Regula os impulsos automáticos emocionais
- Gerenciar emoções

O Cérebro Emocional: Sistema Límbico



- Recebe as informações sensoriais
- Regula processos emocionais e comportamento
- Motivações e recompensas
- Processamento das nossas interações sociais
- Participa da formação das memórias e experiências emocionais
- Reação ao ambiente (luta e fuga)
- Sistema nervoso autônomo (pressão arterial, frequência cardíaca, temperatura, sono, fome, sede)
- Hormônios endócrinos e sexuais

Tomada de decisão: O conflito Interno

Por: Daniel Kahneman

**Sistema 1 -
Rápido
(Emocional e
Impulsivo)**



**Sistema 2 - Lento
e Analítico
(Racional)**

Viéses Cognitivos e Heurísticas

O que são Viéses Cognitivos?

São padrões de pensamentos que distorcem julgamentos e decisões, influenciando nosso modo de pensar de forma inconsciente.

Função das Heurísticas

Heurísticas são atalhos mentais que simplificam problemas complexos, porém podem gerar erros sistemáticos em decisões.



Viés atencional: Distração

- **Clique impulsivo em links e anexos maliciosos**
Durante momentos de pressa ou multitarefa, é comum clicar em links sem verificar a origem.
- **Inserção de credenciais em sites falsos**
Ao tentar resolver algo rapidamente, usuários digitam senhas em páginas sem checar veracidade
- **Erros operacionais em ambientes corporativos**
Funcionários distraídos podem enviar arquivos confidenciais para destinatários errados ou compartilhar dados em canais inseguros.
- **Uso de dispositivos pessoais em ambientes públicos**
A distração em locais como cafés, aeroportos ou transporte público pode levar ao uso de Wi-Fi inseguro ou à exposição da tela

Viés da Urgência

- **Phishing com senso de emergência**

Mensagens como “Sua conta será bloqueada em 1 hora!” ou “Pagamento pendente — evite multa!”.

- **Manipulação emocional por engenharia social**

Frases como “Ajude agora ou perderemos tudo!” ou “Seu chefe precisa disso imediatamente!” ativam o viés de urgência.

- **Erros operacionais em ambientes corporativos**

Funcionários pressionados por prazos podem ignorar etapas de segurança.

Envio de arquivos confidenciais para destinatários errados, uso de canais não seguros.



Viés de Confirmação ou Autoridade

- **Phishing baseado em medo**

Mensagens como “Sua conta será encerrada”, “Você será multado” ou “Detectamos atividade suspeita” ativam o medo.

- **Golpes que simulam autoridade**

Criminosos se passam por bancos, órgãos públicos, empresas ou até superiores hierárquicos.

- **Manipulação emocional por engenharia social ou pressão hierárquicas**

O medo de punição, perda de acesso ou exposição pública leva a decisões precipitadas.





Ganância

- **Phishing com promessas de ganho fácil**

Golpistas exploram a ganância oferecendo prêmios, investimentos milagrosos ou oportunidades exclusivas. Exemplos: “Você ganhou um iPhone!”, “Retorno de 300% em 7 dias!”.

- **Engenharia social baseada em recompensas e Pirâmides Financeiras**

Criminosos manipulam o desejo por status, dinheiro ou vantagem.

Usam frases como: “Acesso antecipado”, “Desconto secreto”, “Oferta limitada”, Plataformas falsas de investimento ou criptomoedas prometem lucros irreais.

- **Ataques internos motivados por lucro**

Funcionários ou ex-colaboradores podem vender informações sigilosas ou facilitar invasões.

Curiosidade

- **Phishing com títulos intrigantes**

“Veja quem te bloqueou”, “Fotos vazadas”, ou “Você foi mencionado!”

- **Downloads disfarçados de conteúdo exclusivo**

Arquivos rotulados como “documento secreto”, “planilha de bônus” ou “manual interno” podem conter vírus

- **Curiosidade técnica em ambientes corporativos**

Funcionários explorando sistemas, acessando áreas restritas ou testando scripts sem autorização.



Evitando Golpes Digitais

-  Cuidado com ligações telefônicas e por vídeo
-  Desconfie de Ofertas e Urgências
-  Verifique Antes de Compartilhar
-  Use autenticação em dois fatores (2FA)
-  Não utilizem redes Wi-Fi Públicas
-  Atualize seus dispositivos e apps
-  Crie senhas fortes e únicas
-  Treinamento Anti-Phishing

Evitando os viesés cognitivos

-  Treine sua atenção digital
-  Reconheça seus próprios vieses
-  Adote rotinas de atenção plena: pausas conscientes, foco em uma tarefa por vez.
-  Exercite a análise: Estou usando a emoção e impulso ou aplicando um modelo mental eficiente?
-  Busque autoconhecimento e percepção das próprias emoções
-  Cuidado com o excesso de redes sociais!

Dúvidas?

Fontes Bibliográficas

Matérias:

<https://www.schroders.com/en/global/family-offices/insights/cyber-security-the-investment-perspective/>

<https://www.visualcapitalist.com/wp-content/uploads/2018/03/18-cognitive-bias-examples.html>

<https://alemdoroteiro.com/2017/04/26/major-lista-de-vieses-cognitivos-que-voce-ja-viu-provavelmente>

<https://leaderdecision.com/pt/vieses-cognitivos-heurísticas/>

<https://positivepsychology.com/cognitive-biases/>

<https://www.nationalgeographicbrasil.com/ciencia/2023/02/como-o-uso-das-redes-sociais-pode-afetar-o-cerebro>

Livros:

KAhneman, Daniel. *Rápido e devagar: duas formas de pensar*. Tradução de Cássio de Arantes Leite. Rio de Janeiro: Objetiva, 2012.

MOORE, Fabricio. *Psicologia da Confiança: estratégias práticas para superar a insegurança*. [local de publicação]: [editora], 2025.



Obrigada!!!