



Tempest

ACADEMY

Conference  
2023

# A importância do Blue Team

---

Porque investir na segurança  
defensiva?





Tempest

**ACADEMY**

Conference

**01** Quem sou eu?

**02** O que é segurança?

**03** Porque a segurança é importante?

**04** O que precisamos fazer?

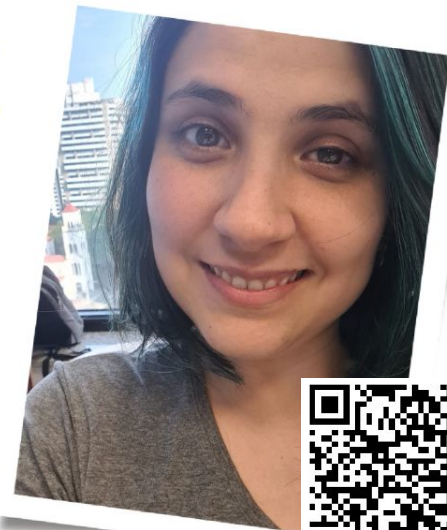


ACADEMY

Conference

# Quem sou eu?

- 32 anos
- Atuo com TI há mais de 15 anos, e com SI há mais de 10
- Já atuei no cliente final, fabricante e consultoria
- Formada em Gestão de TI e Pós em Liderança e Produtividade
- Coordenadora de STM e GV
- Não recuso um café, um whisky ou uma cerveja
- Mãe da Maria Valentina
- Viciada em séries, joguinhos de celular e no caldinho de Recife :)



# Segurança

 Tempest  
**ACADEMY**  
Conference



# Segurança

substantivo feminino

1. Ato ou efeito de **segurar**.
2. Qualidade do que é ou está **seguro**. ≠ INSEGURANÇA
3. Conjunto das ações e dos recursos utilizados para **proteger** algo ou alguém.
4. O que serve para **diminuir os riscos** ou os perigos. = GARANTIA
5. Aquilo que serve de base ou que dá **estabilidade** ou **apoio**. = AMPARO, ESTEIO

"segurança", in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2023, <https://dicionario.priberam.org/seguran%C3%A7a>.

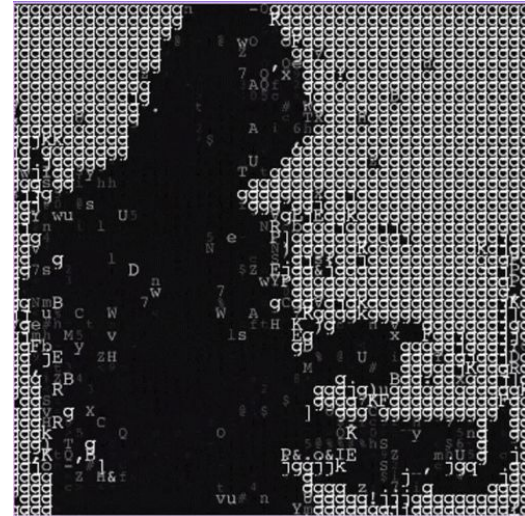


# Teoria das Necessidades Humanas



# Segurança da Informação

Conjunto de ações e estratégias, visando **controlar os riscos e evitar qualquer tipo de ameaça** à integridade, à confidencialidade, à disponibilidade e à autenticidade dos dados da empresa.



# Times de Segurança da Informação\*



\* Atualmente já existem outros times, como Orange Team, White Team, entre outros que podem ser considerados, vamos nos ater a esses para o objetivo dessa apresentação.



# Como vêm a segurança defensiva

 Tempest  
**ACADEMY**  
Conference



# Entretenimento



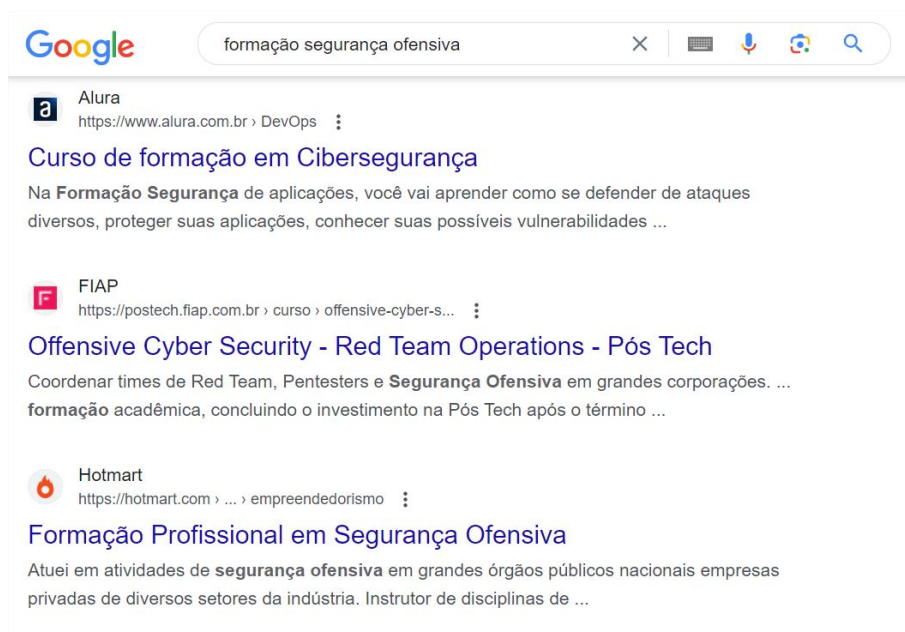
# A defesa

 Tempest  
ACADEMY  
Conference



# Capacitação

## Segurança **Ofensiva**



Google  
formação segurança ofensiva

**Alura**  
https://www.alura.com.br › DevOps

### Curso de formação em Cibersegurança

Na **Formação Segurança** de aplicações, você vai aprender como se defender de ataques diversos, proteger suas aplicações, conhecer suas possíveis vulnerabilidades ...

**FIAP**  
https://postech.fiap.com.br › curso › offensive-cyber-s...

### Offensive Cyber Security - Red Team Operations - Pós Tech

Coordenar times de Red Team, Pentesters e **Segurança Ofensiva** em grandes corporações. ... **formação** acadêmica, concluindo o investimento na Pós Tech após o término ...

**Hotmart**  
https://hotmart.com › ... › empreendedorismo

### Formação Profissional em Segurança Ofensiva

Atuei em atividades de **segurança ofensiva** em grandes órgãos públicos nacionais empresas privadas de diversos setores da indústria. Instrutor de disciplinas de ...

## Segurança **Defensiva**



Google  
formação segurança defensiva

**GAC Cursos Online**  
https://www.gaccursosonline.com.br › loja › catalogo

### Curso Instrutor Multiplicador Direção Defensiva Segurança ...

Curso Instrutor Multiplicador Direção **Defensiva Segurança** no Trânsito · Carga horária: 40 horas · Período de acesso: 60 dias - 24h por dia · Certificação Válido ...  
R\$ 932,00

**GAC Cursos Online**  
https://www.gaccursosonline.com.br › loja › catalogo

### Curso de Direção de Defensiva Segurança no trânsito

Curso de **Formação**, Direção **Defensiva Segurança** no Trânsito. Curso 100% Online através de Vídeo Aula, Emissão do Certificado Válido em Todo Território ...  
R\$ 163,00

**STARSEC**  
https://www.starsec.com.br

### STARSEC – Curso de Formação de Vigilantes RJ

O Curso de Direção **Defensiva** é essencial para quem pretende aproveitar a condição de possuir habilitação. ... Atuando na **formação** Desde 2008. Preparando os ...

# Com o que precisamos lidar



## Origem dos incidentes:

- 43% hacking
- 27% malwares
- 16% erro ou mal uso
- 14% outras categorias

# Com o que precisamos lidar

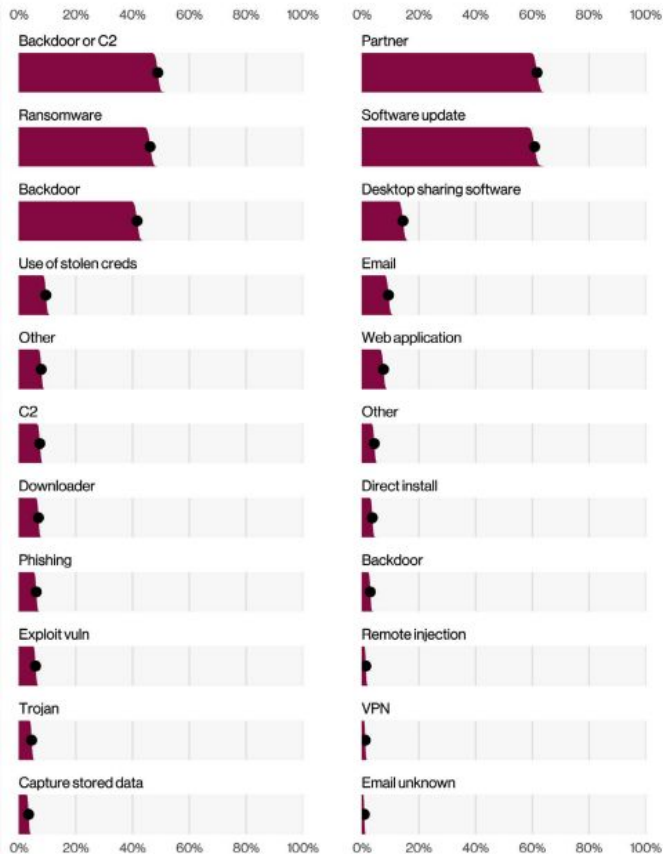


Figure 35. Top Action varieties in System Intrusion incidents (n=5,212)

Figure 36. Top Action vectors in System Intrusion incidents (n=3,403)

Tudo isso envolve:

- Definição da **estratégia** de segurança
- Aplicação de **correções**
- **Configurações** adequadas das ferramentas
- **Conscientização**
- Identificação de cenários legítimos x **maliciosos**

# Porque somos importantes

## Ataque hacker em Dallas interrompe serviços da polícia e bombeiros

Caso envolveria ransomware, um tipo de ataque no qual hackers embaralham dados e imobilizam redes até que um pagamento de extorsão seja feito

Por Da Redação  
4 Maio 2023, 18h04

<https://veja.abril.com.br/mundo/ataque-hacker-em-dallas-interrompe-servicos-da-pc>



## Hackers causaram prejuízos a cerca de 25% das empresas brasileiras em 2022, diz pesquisa

A varejista Americanas perdeu R\$ 1 bilhão em vendas após sofrer um ataque hacker em 2022; estudo foi divulgado pela empresa de segurança Proofpoint.

<https://g1.globo.com/tecnologia/noticia/2023/03/08/hackers-causaram-prejuizos-a-cerca-de-25-das-empresas-brasileiras-em-2022-diz-pesquisa.ghtml>. Acesso em 11/nov/23.

## Brasil é o 2º país mais vulnerável a ataques de hackers, diz relatório

Empresa de cibersegurança bloqueou 85,6 bilhões de ameaças de hackers no primeiro semestre de 2023 e Brasil está como um dos alvos principais

<https://exame.com/future-of-money/brasil-e-o-2o-pais-mais-vulneravel-a-ataques-de-hackers-diz-relatorio/>. Acesso em 16/nov/23.

# Porque somos importantes

Apenas **30%** dos incidentes são identificados pelas equipes internas.

Incidentes revelados pelos atacantes custaram **US\$ 1 milhão** a mais.


Fonte: IBM

Violações com identificação e contenção **> 200 dias** custaram em média **23% a mais**.

Fonte: IBM



# O que ninguém sabe...

 Tempest

**ACADEMY**

Conference

## ... é quanto a empresa economiza.

**Cidade de Dallas vai gastar US\$ 8,5 milhões para mitigar ataque**

<https://www.cisoadvisor.com.br/cidade-de-dallas-vai-gastar-us-85-milhoes-para-mitigar-ataque/>. Acesso em 14/nov/23.

**Custo de vazamento de dados no Brasil é de R\$ 6,2 milhões**

<https://www.securityreport.com.br/media-de-custo-de-vazamento-de-dados-no-brasil-oscila-para-r-62-milhoes-em-2023/>. Acesso em 15/nov/23.

**Custos de vazamentos de dados são repassados por empresas aos consumidores**

<https://canaltech.com.br/seguranca/custos-de-vazamentos-de-dados-sao-repassados-por-empresas-aos-consumidores-221729/>. Acesso em 15/nov/23.

# Os custos de um incidente são muitos

## Custos Diretos

- ✓ Indisponibilidade
- ✓ Consultoria de SI
- ✓ Hora extra
- ✓ Ressarcimento
- ✓ Multas
- ✓ Extorsão

## Custos Indiretos

- ✓ Imagem da marca
- ✓ Valor da marca
- ✓ Confiabilidade
- ✓ Diminuição de clientes
- ✓ Controles de segurança
- ✓ Ações judiciais

Segundo a **pesquisa\*** da IBM:

US\$ 4,45  
milhões

custo médio da violação de dados

51%

das organizações planejam aumentar os investimentos

\* Analisou 553 empresas que sofreram violações de dados, entre mar/22 e mar/23, contemplando 16 países e 17 setores.

# O que precisamos fazer?

Fator humano aparece em 82% dos casos

Muitos CTOs não tem uma **comunicação clara**

**Conscientização**

**Automação / Inteligência Artificial**

108 dias a menos para identificação

Redução de US\$ 1,76 milhões nos custos

31,6% a menos no custo

US 3,84 milhões X US\$ 5,28 milhões

**Redução de Complexidade**

**Segurança por design / Segurança por padrão**

**Zero Trust**

O básico bem feito

NÃO EXISTE BALA DE PRATA!

**Resposta a Incidente**

54 dias a menos para resolução

Redução de US\$ 1,49 milhões nos custos

Repita depois de mim...

 Tempest  
**ACADEMY**  
Conference

Lembrete  
Lembrete  
L  
L  
L  
L  
Lembrete  
Lembrete

Segurança  
defensiva  
importa!


Ciente



# Obrigada!

## Bora bater um papo?



 Tempest

**ACADEMY**

Conference



Tempest

ACADEMY

Conference

2023





**ACADEMY**

Conference

# Clique para adicionar um título

---

Clique para adicionar texto



Tempest

**ACADEMY**

Conference



# Clique para adicionar um título



Clique para adicionar texto

Clique para adicionar texto

# Clique para adicionar um título





**ACADEMY**

Conference

Clique para adicionar texto

Clique para adicionar texto



**ACADEMY**

Conference

Clique para  
adicionar um título

Clique para adicionar texto

# Clique para adicionar um título

 Tempest

**ACADEMY**

Conference

Clique para adicionar texto

# Clique para adicionar um título

 Tempest

**ACADEMY**

Conference

Clique para adicionar texto

Clique para adicionar texto

# Clique para adicionar um título

 Tempest

**{ACADEMY}**

Conference