

Segurança e Auditoria de Sistemas

Fundamentos e Segurança para SI



Prof. Flávio Murilo de Carvalho Leal
Centro Universitário Paraíso

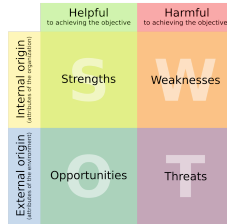
Definição

A Matriz SWOT é uma ferramenta de análise estratégica utilizada para avaliar o ambiente interno e externo de uma organização.

- ▶ Criada por Albert Humphrey (década de 1960).
- ▶ Muito utilizada em planejamento estratégico.
- ▶ Também conhecida como FOFA (Forças, Oportunidades, Fraquezas e Ameaças).

A ferramenta será apresentada como uma opção de ferramenta de planejamento estratégico para o suporte da análise de segurança de sistemas.

SWOT ANALYSIS



- ▶ Ambiente Interno: controlável.
- ▶ Ambiente Externo: não controlável.

Forças (Strengths)

Características internas que representam vantagens competitivas.

Fraquezas (Weaknesses)

Limitações internas que prejudicam o desempenho.

- ▶ Equipe qualificada.
- ▶ Marca consolidada.
- ▶ Tecnologia própria.
- ▶ Boa reputação no mercado.
- ▶ Localização estratégica.

- ▶ Falta de capital de giro.
- ▶ Processos internos ineficientes.
- ▶ Dependência de poucos clientes.
- ▶ Alta rotatividade de funcionários.
- ▶ Infraestrutura defasada.

Oportunidades (Opportunities)

Fatores externos que podem favorecer a organização.

Ameaças (Threats)

Fatores externos que podem prejudicar a organização.

- ▶ Crescimento do mercado.
- ▶ Novas tecnologias.
- ▶ Mudanças favoráveis na legislação.
- ▶ Parcerias estratégicas.
- ▶ Novos nichos de clientes.

- ▶ Crises econômicas.
- ▶ Entrada de novos concorrentes.
- ▶ Mudanças regulatórias desfavoráveis.
- ▶ Avanço tecnológico da concorrência.
- ▶ Instabilidade política.

- ▶ Forças podem ser usadas para aproveitar oportunidades.
- ▶ Forças podem minimizar ameaças.
- ▶ Fraquezas podem impedir o aproveitamento de oportunidades.
- ▶ Fraquezas podem potencializar ameaças.

Estratégia SO (Maxi-Maxi)

Usar forças para aproveitar oportunidades.

Estratégia ST (Maxi-Mini)

Usar forças para reduzir ameaças.

Estratégia WO (Mini-Maxi)

Minimizar fraquezas para aproveitar oportunidades.

Estratégia WT (Mini-Mini)

Minimizar fraquezas e evitar ameaças.

- ▶ **Força:** Equipe altamente qualificada.
- ▶ **Fraqueza:** Baixo investimento em marketing.
- ▶ **Oportunidade:** Crescimento da demanda por soluções digitais.
- ▶ **Ameaça:** Entrada de startups inovadoras.

- ▶ Confundir fatores internos com externos.
- ▶ Listar itens muito genéricos.
- ▶ Não priorizar os fatores mais relevantes.
- ▶ Não transformar análise em estratégia.

- ▶ Simplicidade de aplicação.
- ▶ Visão sistêmica da organização.
- ▶ Base para planejamento estratégico.
- ▶ Facilita tomada de decisão.

- ▶ Pode ser subjetiva.
- ▶ Não estabelece prioridades automaticamente.
- ▶ Não substitui análises quantitativas.
- ▶ Depende da qualidade das informações levantadas.

1. Análise do ambiente (SWOT).
2. Definição de objetivos estratégicos.
3. Formulação de estratégias.
4. Implementação.
5. Monitoramento e controle.

Exemplos no contexto de Sistemas de Informação:

- ▶ **Forças:** equipe capacitada, backups automatizados
- ▶ **Fraquezas:** senhas fracas, sistemas desatualizados
- ▶ **Oportunidades:** novas tecnologias de proteção
- ▶ **Ameaças:** malware, ataques externos, falhas humanas

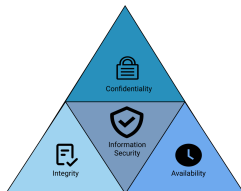
Em grupos, elaborem uma matriz SWOT para:

Em grupos, elaborem uma matriz SWOT para:

Cenário: Sistema acadêmico de uma instituição de ensino.

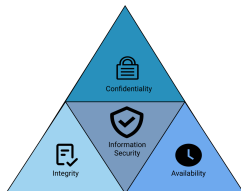
Considerem:

- ▶ Infraestrutura
- ▶ Usuários
- ▶ Dados armazenados
- ▶ Possíveis ameaças



A segurança da informação baseia-se em três pilares:

- ▶ **Confidencialidade**
- ▶ **Integridade**
- ▶ **Disponibilidade**



A segurança da informação baseia-se em três pilares:

- ▶ **Confidencialidade**
- ▶ **Integridade**
- ▶ **Disponibilidade**

Qualquer incidente de segurança afeta um ou mais desses elementos.

Garantia de que a informação é acessada apenas por quem tem autorização.

Garantia de que a informação é acessada apenas por quem tem autorização.

Exemplos:

- ▶ Controle de acesso
- ▶ Criptografia
- ▶ Senhas

Garantia de que a informação não foi alterada indevidamente.

Garantia de que a informação não foi alterada indevidamente.

Exemplos:

- ▶ Hashes
- ▶ Assinaturas digitais
- ▶ Controle de versões

Garantia de que a informação e os sistemas estejam acessíveis quando necessários.

Garantia de que a informação e os sistemas estejam acessíveis quando necessários.

Exemplos:

- ▶ Redundância
- ▶ Backups
- ▶ Proteção contra falhas

Classifiquem os cenários:

- ▶ Queda de servidor
- ▶ Vazamento de dados
- ▶ Alteração indevida de notas

Classifiquem os cenários:

- ▶ Queda de servidor
- ▶ Vazamento de dados
- ▶ Alteração indevida de notas

Pergunta: Qual elemento do CIA foi comprometido?

Ativos são tudo aquilo que possui valor para a organização.

Ativos são tudo aquilo que possui valor para a organização.

Podem incluir:

- ▶ Dados
- ▶ Sistemas
- ▶ Pessoas
- ▶ Equipamentos
- ▶ Processos

Possíveis critérios:

- ▶ Sensibilidade
- ▶ Criticidade
- ▶ Valor estratégico
- ▶ Impacto em caso de perda

Elaborem um mapa mental contendo:

Elaborem um mapa mental contendo:

- ▶ Tipos de ativos
- ▶ Exemplos práticos
- ▶ Riscos associados

Utilizem papel ou ferramenta digital.

Cada grupo assumirá um papel:

Cada grupo assumirá um papel:

- ▶ Administrador de Sistemas
- ▶ Usuário
- ▶ Possível Atacante

Situação:

Situação:

Um sistema corporativo apresentou comportamento anômalo.

Os grupos devem discutir:

- ▶ O que cada papel faria?
- ▶ Quais decisões seriam tomadas?
- ▶ Quais riscos existem?

Discussão coletiva:

Discussão coletiva:

- ▶ Como falhas humanas influenciam a segurança?
- ▶ Tecnologia é suficiente para garantir segurança?
- ▶ Qual a importância de políticas e processos?