TÉCNICO LISBOA

Calculating Business Impact Assessment of Cyber-Threats

Diogo Martins Alves

Orientador: Prof. Dr. António Manuel Raminhos Cordeiro Grilo

Co-Orientador: Eng. Filipe Miguel Marcos Apolinário

Dissertação para a obtenção do grau de Mestre em

Engenharia Eletrotécnica e de Computadores

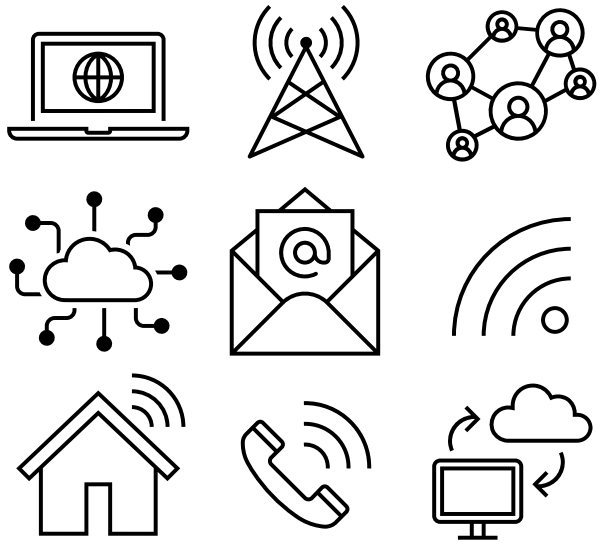
Novembro 2021

Estrutura da Apresentação


Introdução
Revisão de Literatura
Solução Proposta
Avaliação
Conclusão

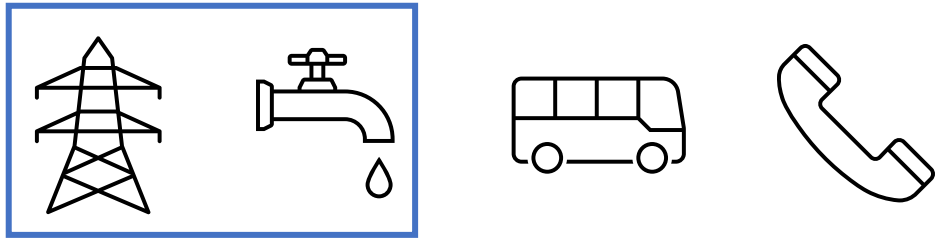
MOTIVAÇÃO

Tecnologias da Informação e Comunicação (TICs)



Risco de ataques informáticos

Infraestruturas Críticas



Efeitos em Cascata

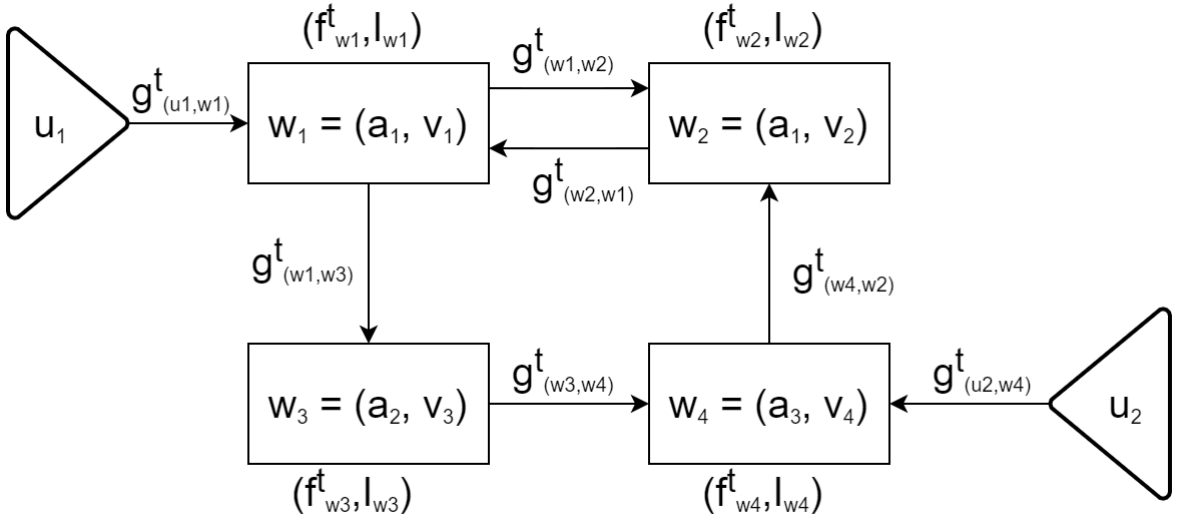
SOLUÇÃO

- Calcular estimativa do impacto de ataques informáticos nos processos-negócio das organizações
- Priorizar ameaças
- Plano de gestão de risco


Introdução
Revisão de Literatura
Solução Proposta
Avaliação
Conclusão

PROPAGAÇÃO DE AMEAÇAS

Risk Assessment Graphs (RAGs)

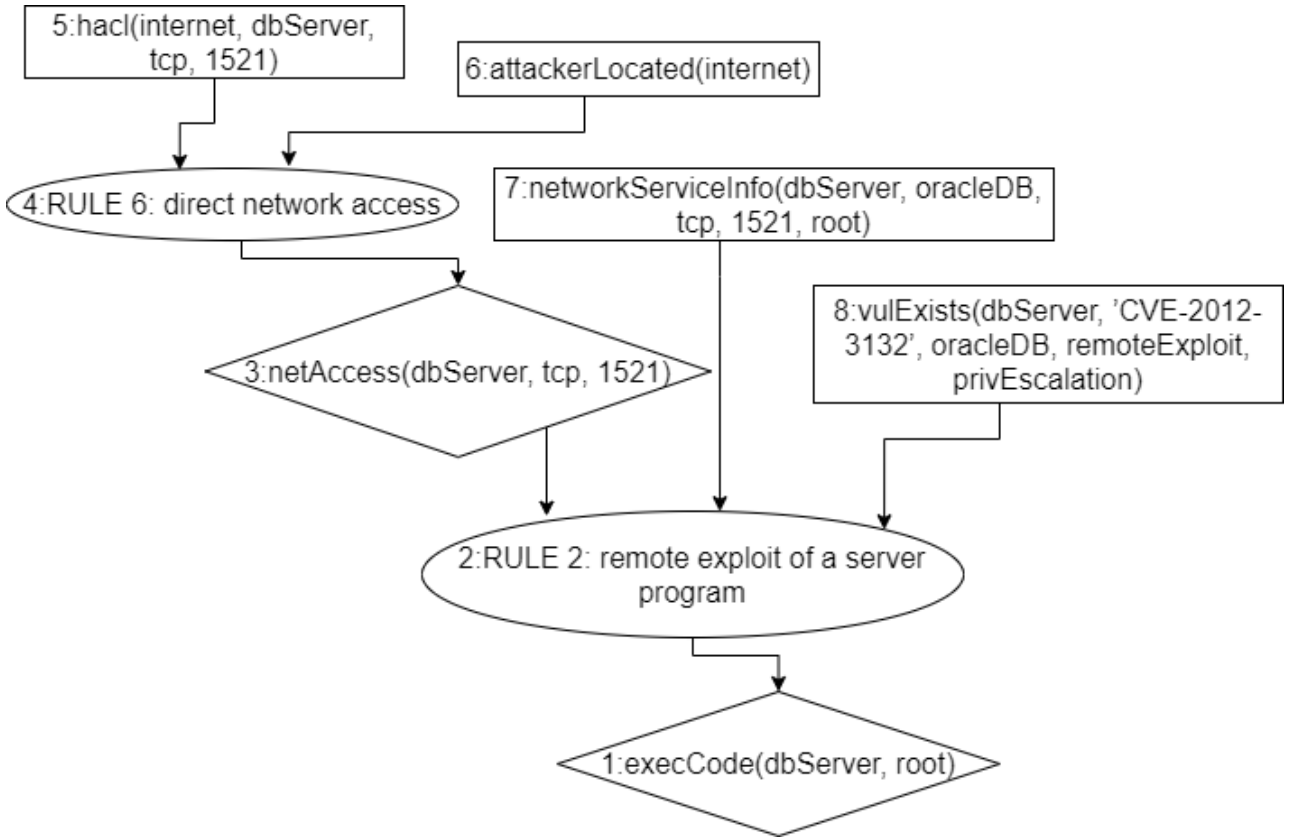


- Modelação de conectividade entre dispositivos
- Modelação de vulnerabilidades
- Estimativa de risco

N. Kheir, A. R. Mahjoub, M. Y. Naghmouchi, N. Perrot, and J.-P. Wary. Assessing the risk of complex ICT systems. Annals of Telecommunications, 73(1):95–109, 2018.

PROPAGAÇÃO DE AMEAÇAS

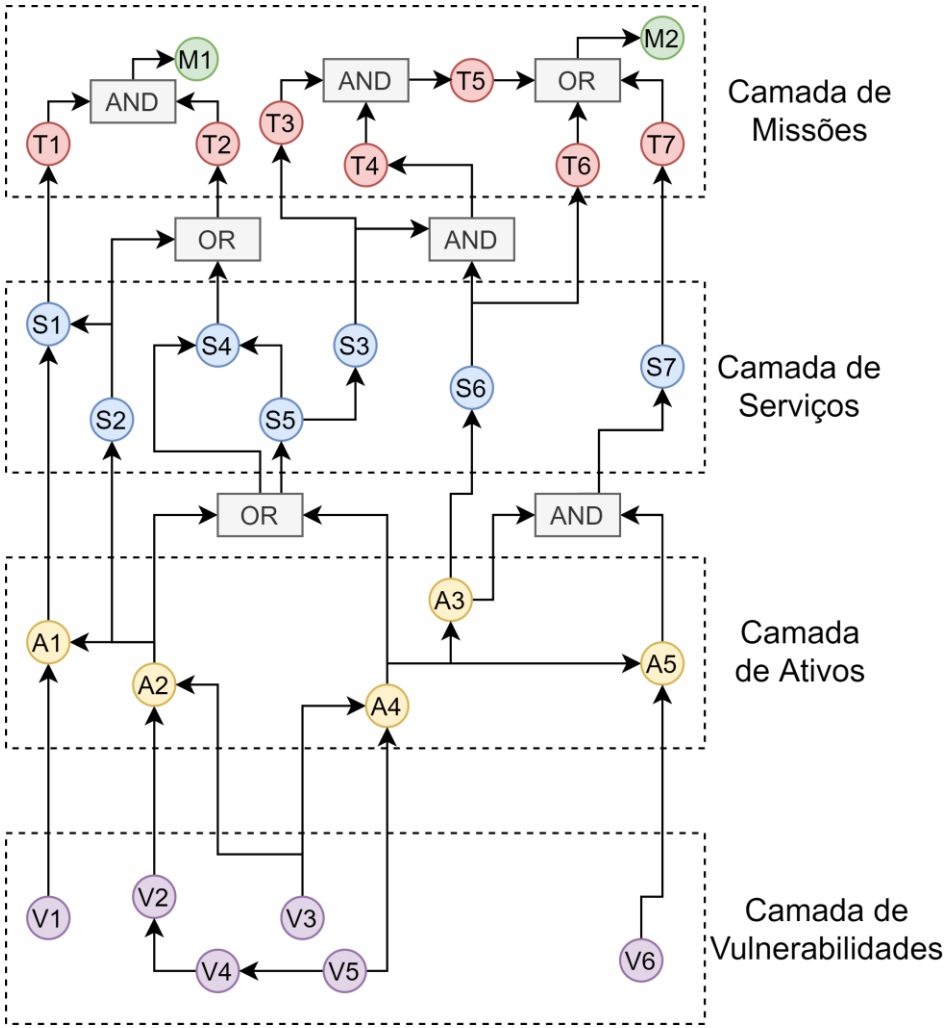
Grafos de ataque



- Programação Lógica: primitivas e regras
- Grafo de ataque com serviços afetados

R. E. Sawilla and X. Ou. Identifying critical attack assets in dependency attack graphs. In European Symposium on Research in Computer Security, pages 18–34. Springer, 2008.

PROPAGAÇÃO DE AMEAÇAS



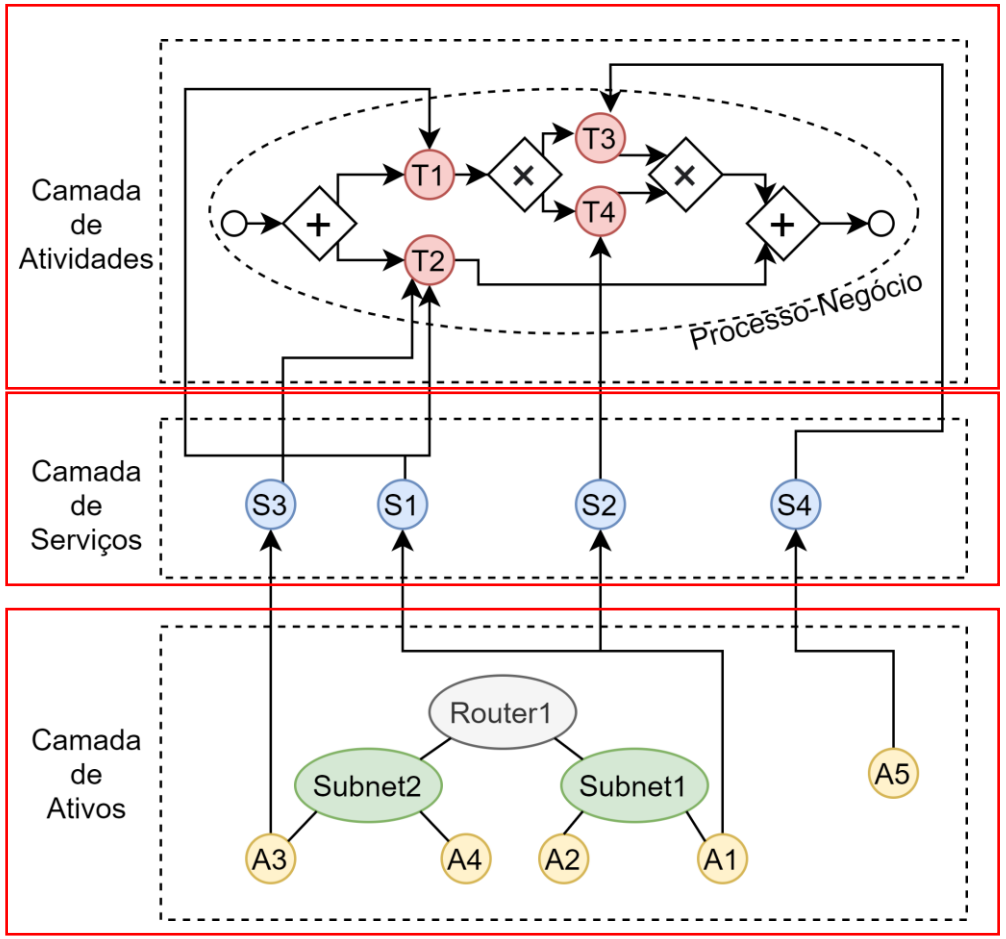
Vulnerabilidades-Ativos-Serviços-Missões (VASM)

- Modelo de abstração em quatro camadas
- Dependências são estabelecidas através de nós AND e OR

Y. Sun, T.-Y. Wu, X. Liu, and M. S. Obaidat. Multilayered impact evaluation model for attacking missions. IEEE Systems Journal, 10(4):1304–1315, 2014.

PROPAGAÇÃO DE AMEAÇAS

Revisão de Literatura



Business Impact Assessment (BIA)

Processo-negócio – Sequência de Atividades

Atividades – Ações realizadas no contexto de um processo-negócio

Serviços – ex.: Sistemas Operativos, Aplicações

Dispositivos – ex.: Computadores, Servidores, Routers

C. Kopke, K. Srivastava, L. Konig, N. Miller, M. Fehling-Kaschek, K. Burke, M. Mangini, I. Praça, A. Canito, O. Carvalho, et al. Impact Propagation in Airport Systems. Cyber-Physical Security for Critical Infrastructures Protection, 12618:191, 2020.

Business Impact Assessment

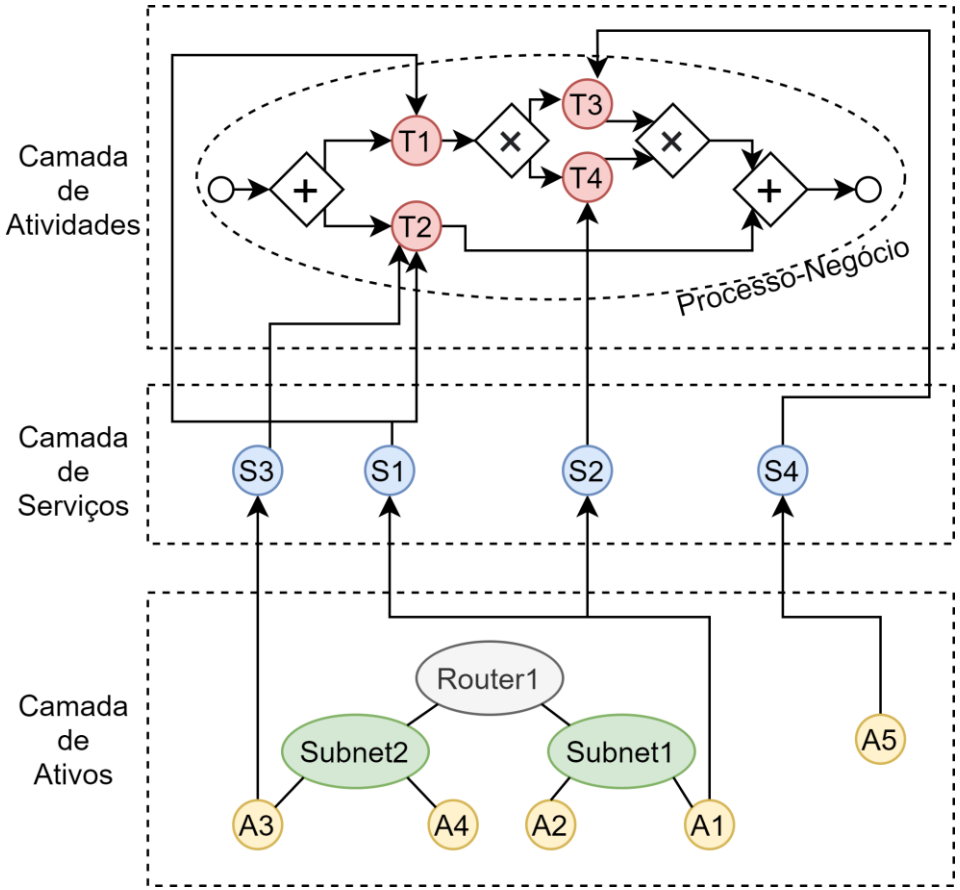


Diagrama de Processos-Negócio (BPMN)

Gateway Paralelo (AND)

Gateway Exclusivo (OR)

Grafos de ataque → Deteção da propagação de uma ameaça

QUANTIFICAÇÃO DE IMPACTO

PRINCIPAL LIMITAÇÃO DO BIA

- Não oferece forma de quantificar o impacto da propagação de ciber-ameaças

SOLUÇÃO

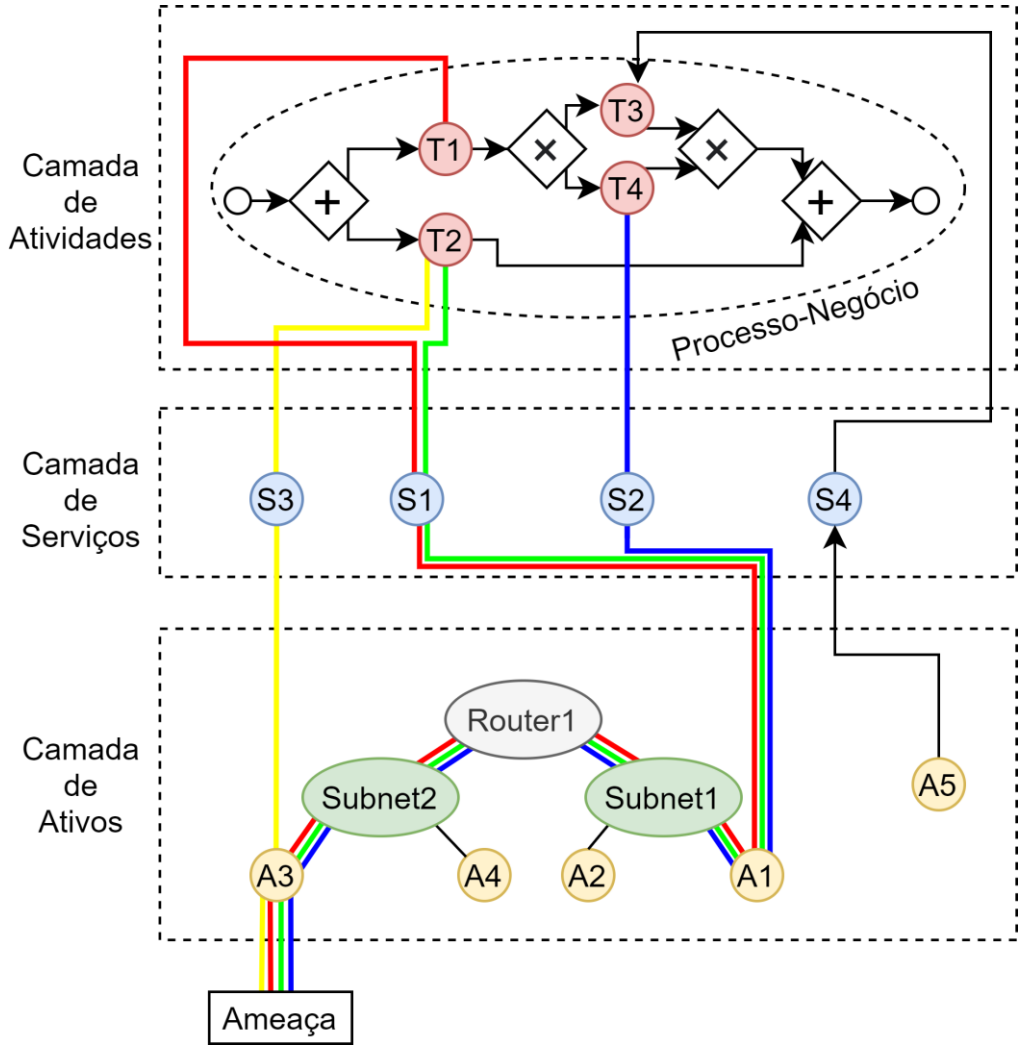
- Algoritmo desenvolvido por Gabriel Jakobson propõe algoritmo para cálculo de impacto de ciber-ameaças no modelo VASM

G. Jakobson. Mission cyber security situation assessment using impact dependency graphs. In 14th international conference on information fusion, pages 1–8. IEEE, 2011.

Estrutura da Apresentação

BUSINESS IMPACT CALCULATOR (BUSICALC)

Solução Proposta



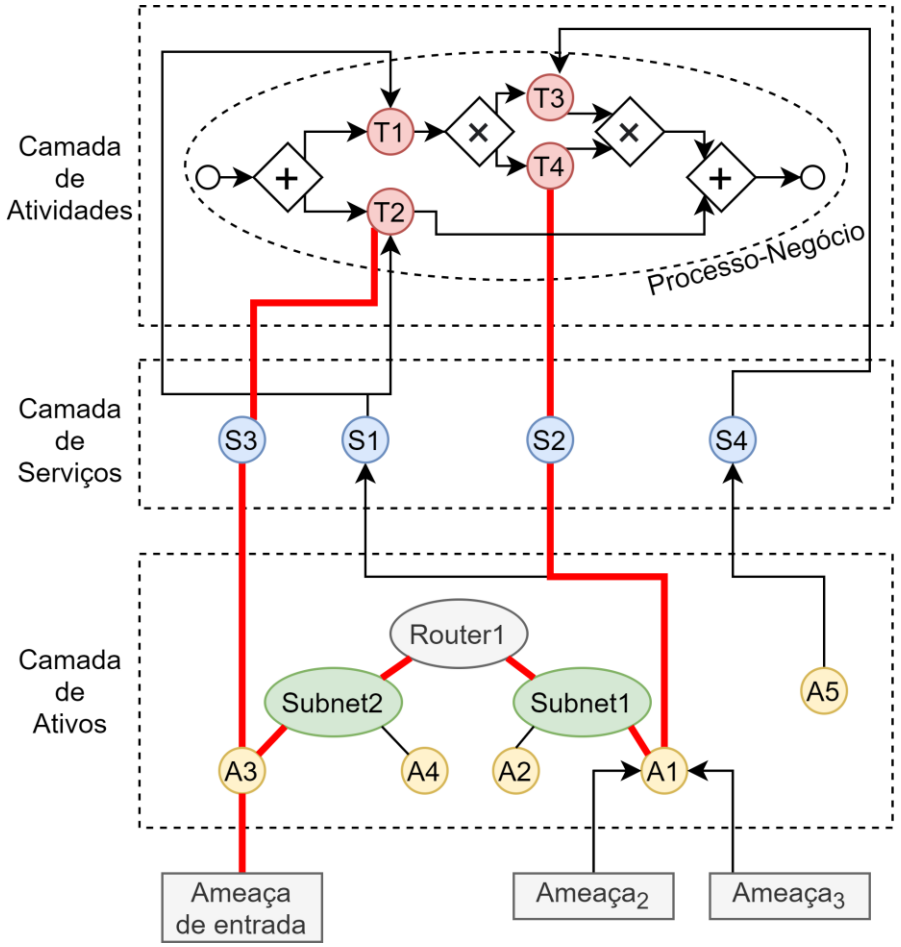
Caminhos identificados pelo BIA (caminhos triviais)

Impossível modelar ataques complexos

Solução: Possibilidade de agregar caminhos triviais

BUSINESS IMPACT CALCULATOR (BUSICALC)

Solução Proposta

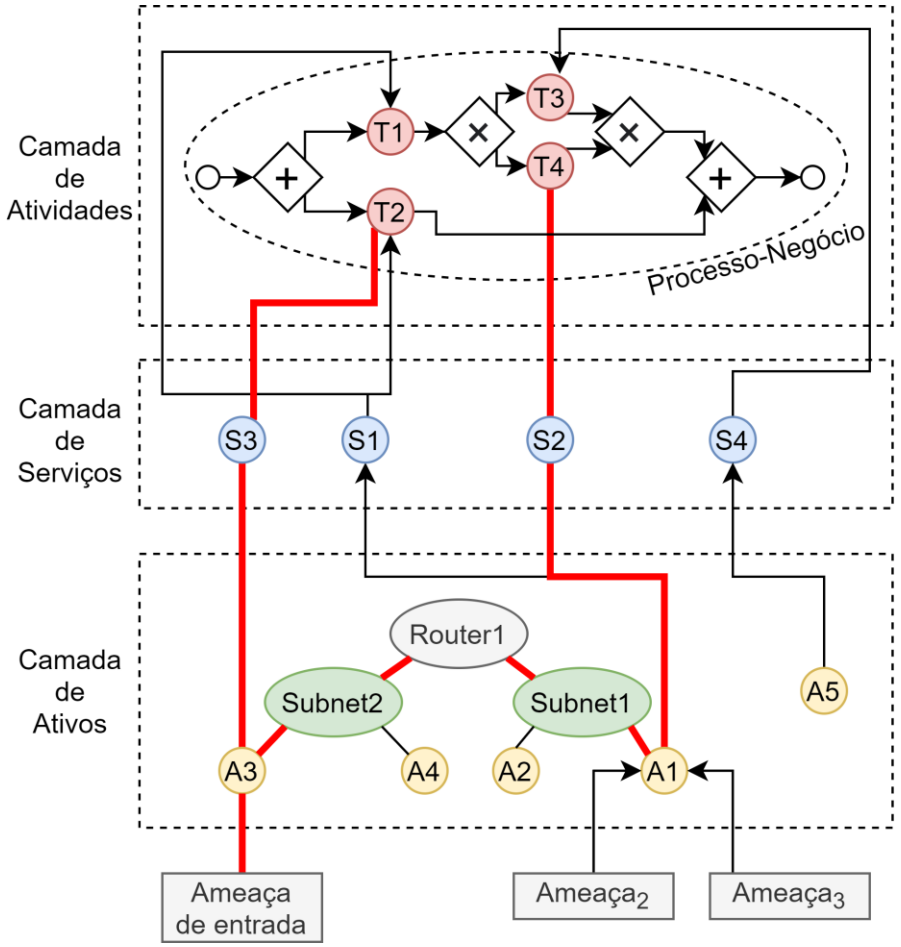


Fator de Impacto (IF) – Capacidade de a ameaça comprometer o ativo atacado

$$IF_{Ameaça} = \frac{CVSS_{Vulnerabilidade}}{10}$$

BUSINESS IMPACT CALCULATOR (BUSICALC)

Solução Proposta



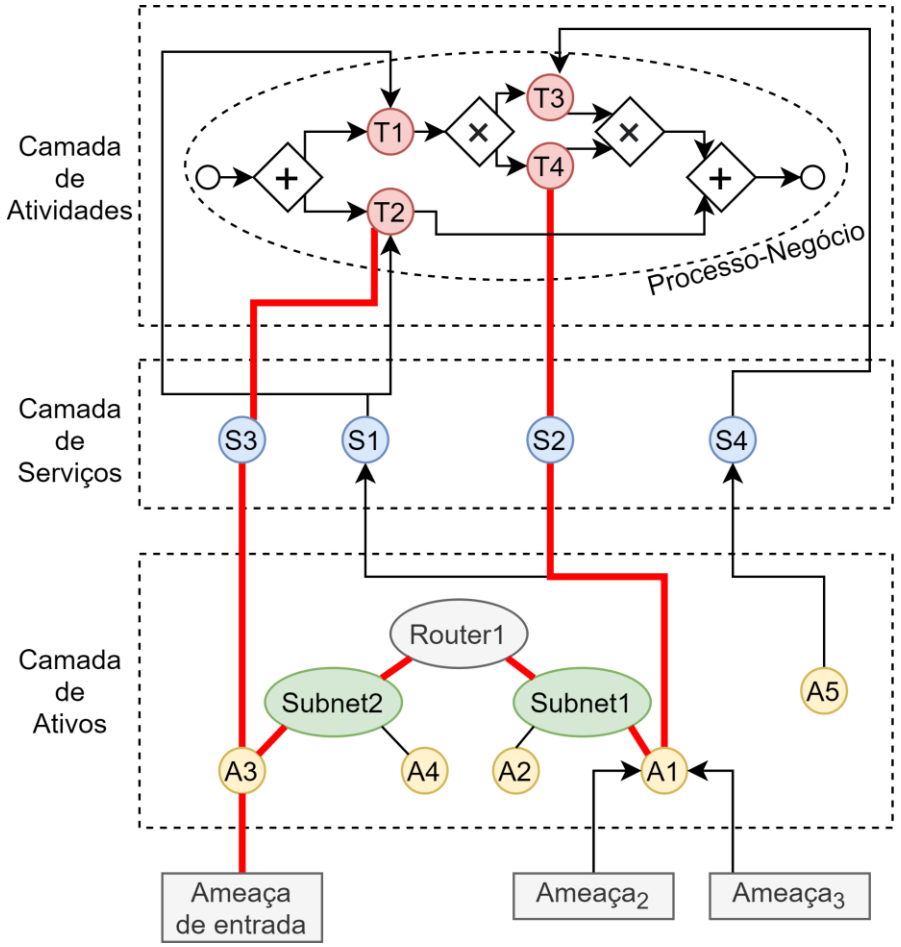
Capacidade Operacional (OC) – Nível de operacionalidade dos Ativos/Serviços/Atividades

$$OC_{A3} := 1 - IF_{Ameaça\ de\ entrada\ (A3)}$$

$$OC_{A1} := min(\ OC_{A3},\ 1 - IF_{Ameaça_2},\ 1 - IF_{Ameaça_3})$$

BUSINESS IMPACT CALCULATOR (BUSICALC)

Solução Proposta



$$OC_{S3} := OC_{A3}$$

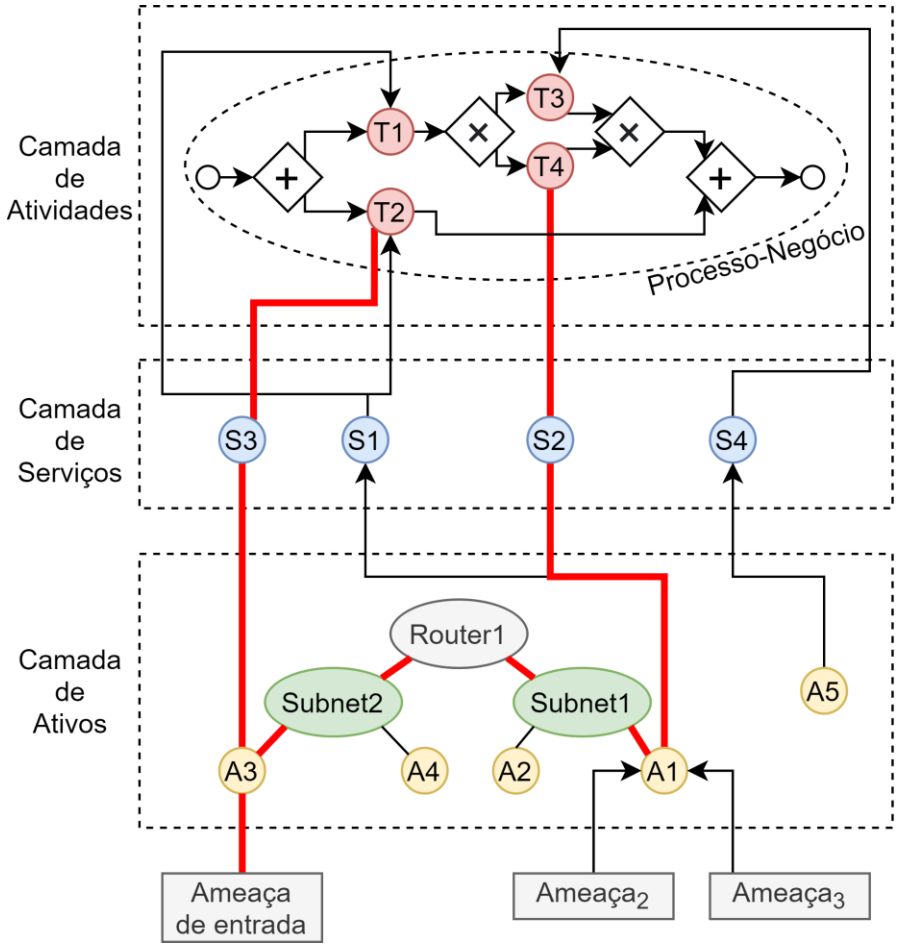
$$OC_{S2} := OC_{A1}$$

$$OC_{T2} := média(OC_{S3}, OC_{S1})$$

$$OC_{T4} := OC_{S2}$$

BUSINESS IMPACT CALCULATOR (BUSICALC)

Solução Proposta



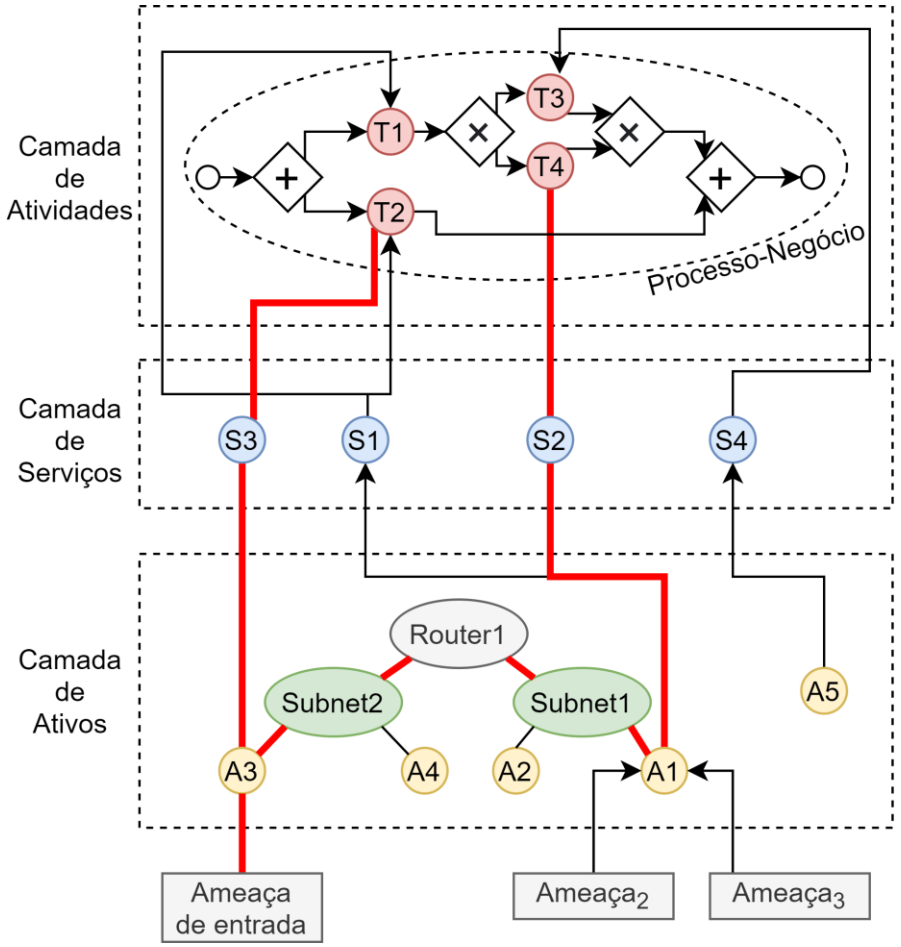
Fio de execução – Conjunto de atividades que torna um processo-negócio concluído

Fios de execução: $\{T1, T2, T3\}$ e $\{T1, T2, T4\}$

$$OC_{\{T1,T2,T3\}} = OC_{T1} \times OC_{T2} \times OC_{T3}$$
$$OC_{\{T1,T2,T4\}} = OC_{T1} \times OC_{T2} \times OC_{T4}$$

BUSINESS IMPACT CALCULATOR (BUSICALC)

Solução Proposta



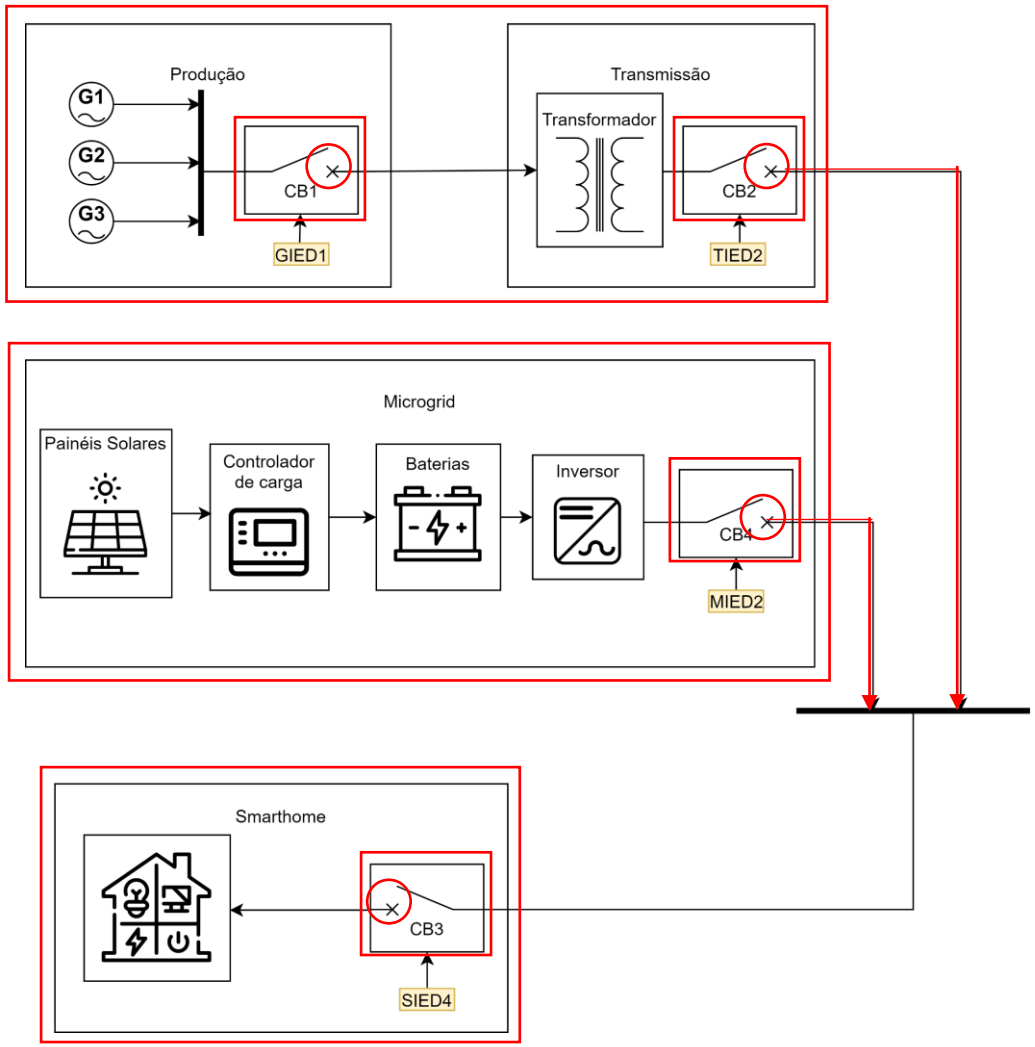
$$OC_{PN} = média(OC_{\{T1,T2,T4\}}, OC_{\{T1,T2,T4\}})$$

$$Impacto = 1 - OC_{PN}$$

Estrutura da Apresentação

DATASET

Avaliação

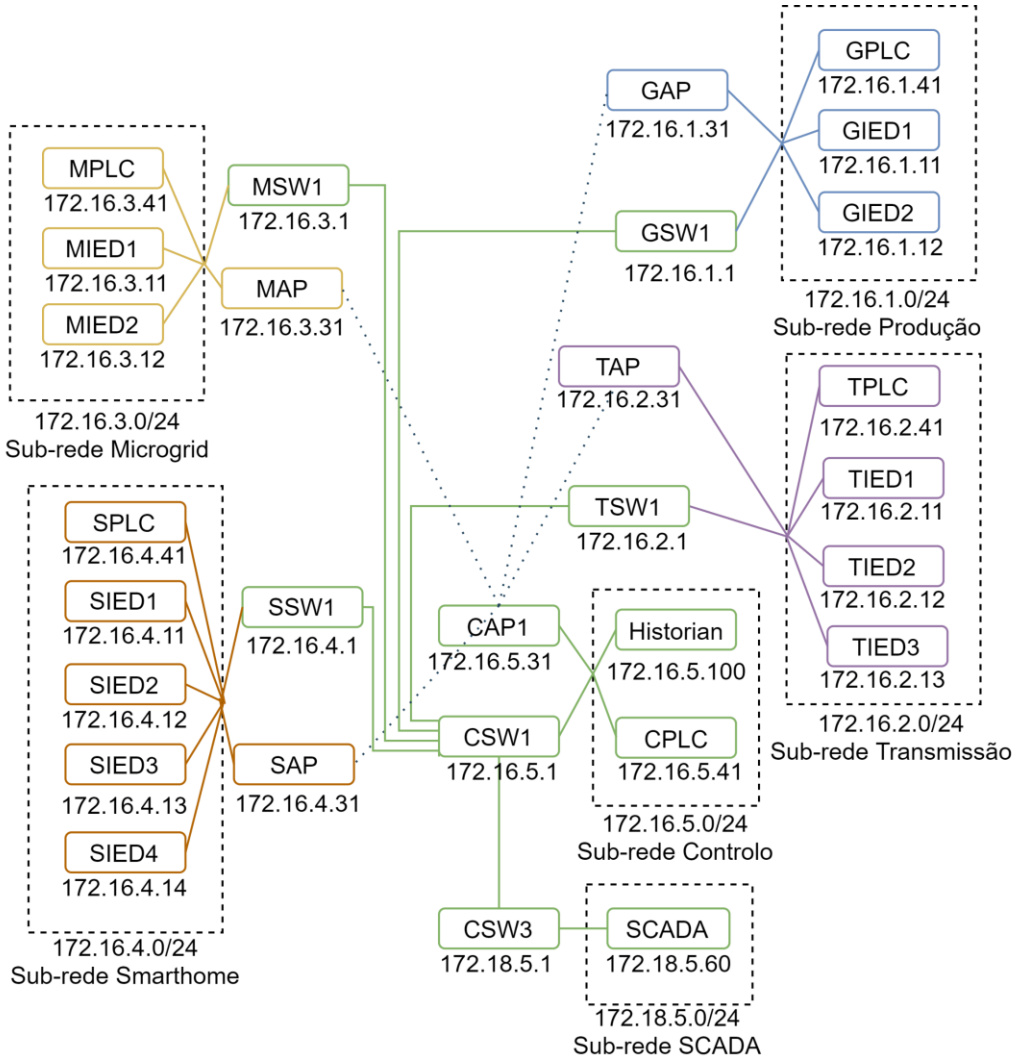


Rede Elétrica Inteligente em escala reduzida (EPIC)

- Fluxo de energia controlado por disjuntores
- Redundância no fornecimento de energia
- Fornecimento de energia garantido por CB1, CB2, CB3 OU CB4, CB3

DATASET

Avaliação



- AP - Access Point
- IED - Dispositivo Elétrico Inteligente
- SW - Network switch
- PLC - Controlador Lógico Programável
- SCADA - Sistema de supervisão e aquisição de dados

DATASET

Avaliação

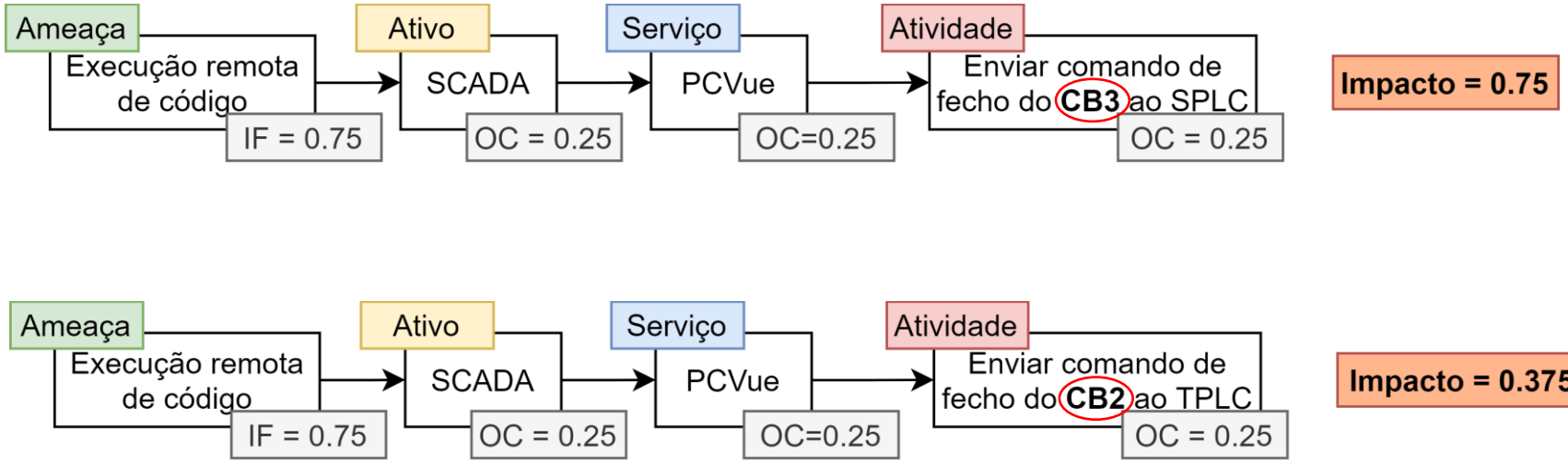
Tipo de Ativo	ID da Vulnerabilidade	Descrição	Pontuação CVSS
SCADA	CVE-2020-26867	Execução arbitrária de código	9.8
	CVE-2020-26868	Denial Of Service	7.5
	CVE-2020-26869	Divulgação de informação confidencial	7.5
	CVE-2019-0752	Execução remota de código	7.5
PLC	CVE-2018-5459	Execução de comandos não autorizados	9.8
IED	CVE-2019-10938	Execução arbitrária de código	9.8
	CVE-2019-19279	Denial Of Service	7.5

Ameaça de ponto de entrada considerada por defeito

EXPERIÊNCIA #1

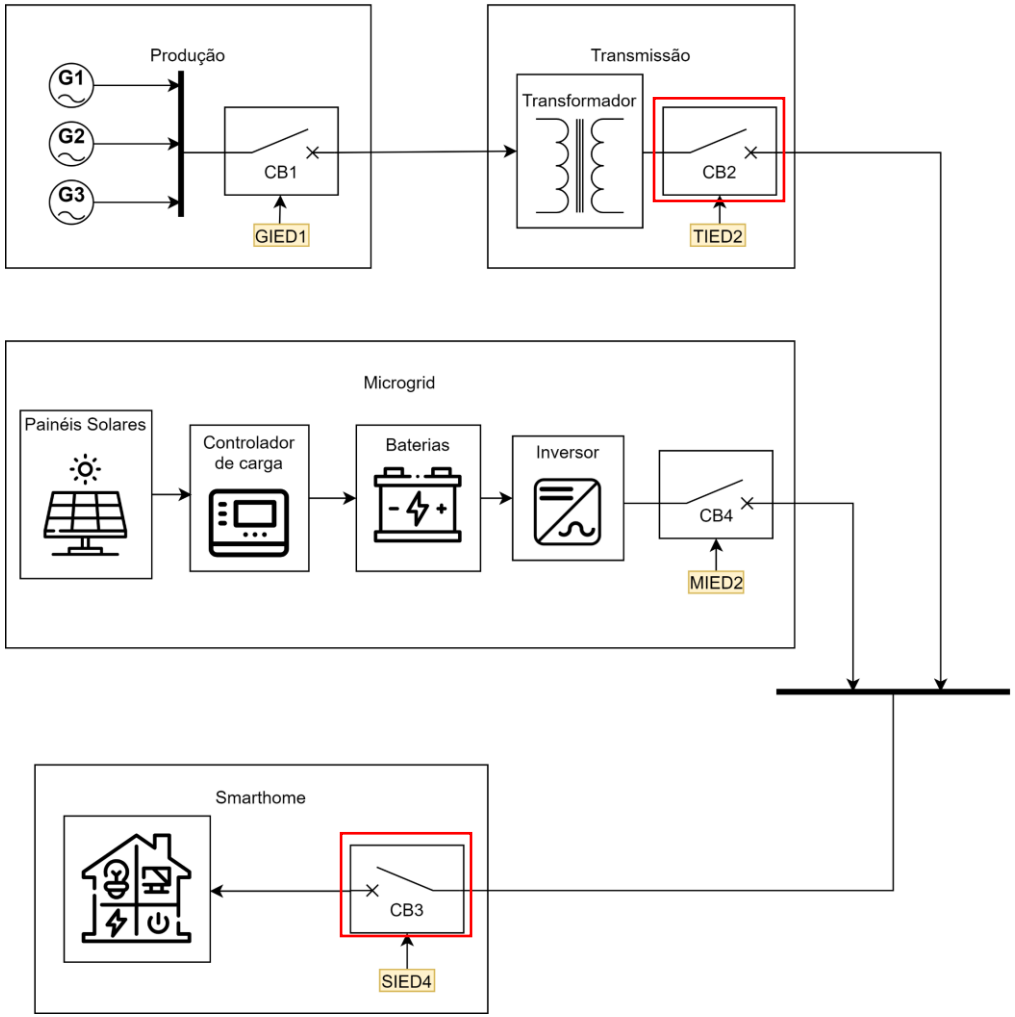
Avaliação

De que forma o posicionamento das atividades dentro do processo-negócio tem influência no impacto?



EXPERIÊNCIA #1

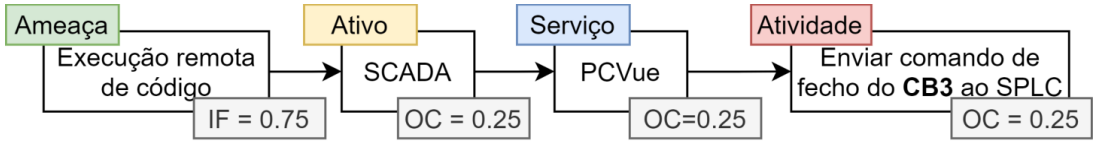
Avaliação



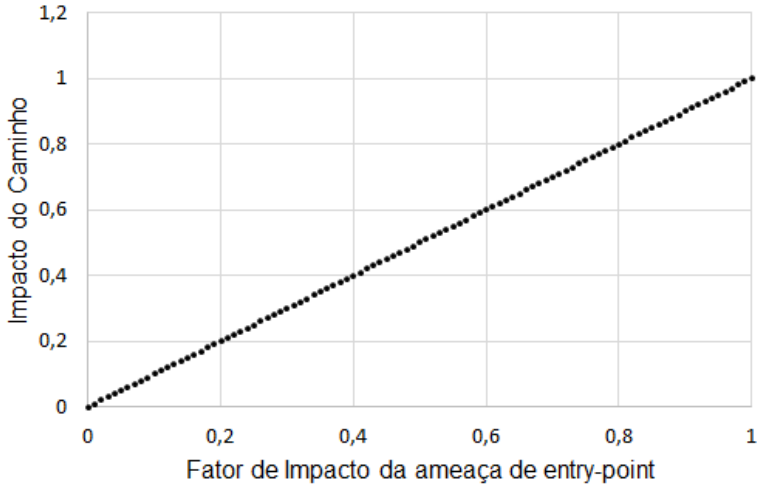
CB3 representa um papel mais crucial que o CB2, razão pela qual o primeiro caminho tem maior impacto

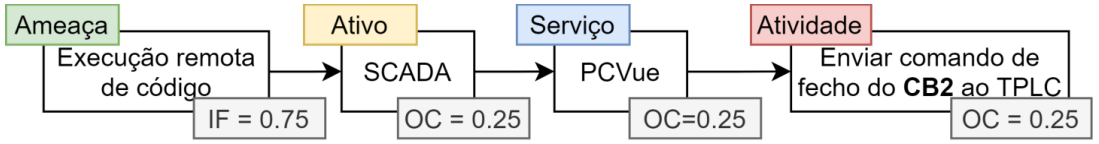
EXPERIÊNCIA #1

Avaliação

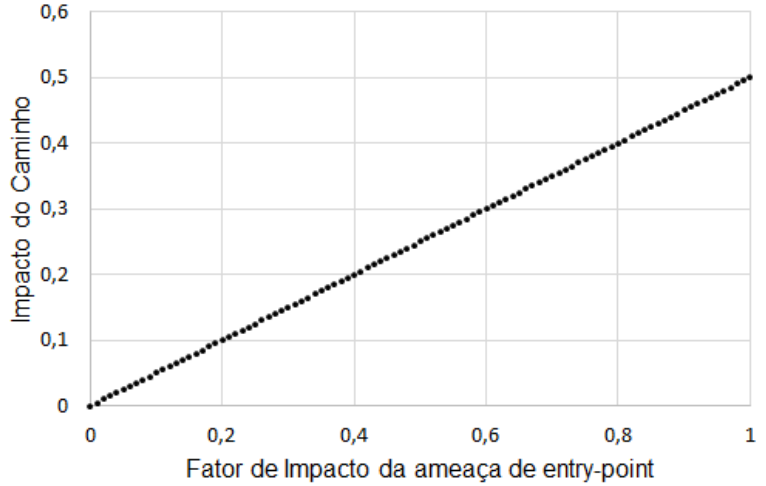


Impacto = 0.75





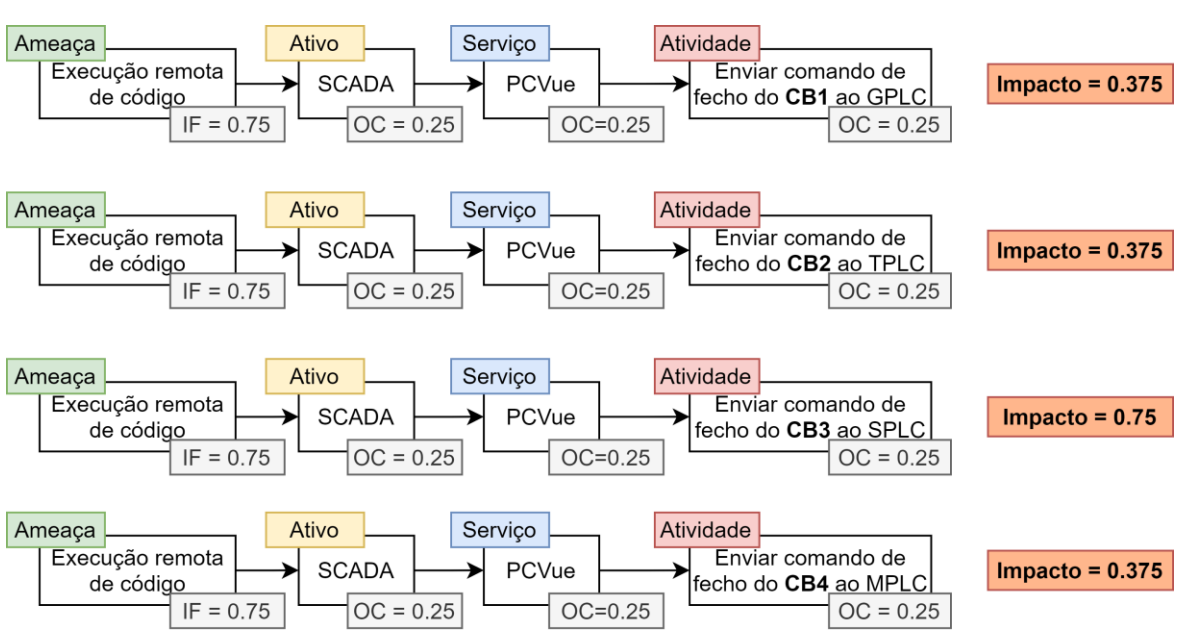
Impacto = 0.375

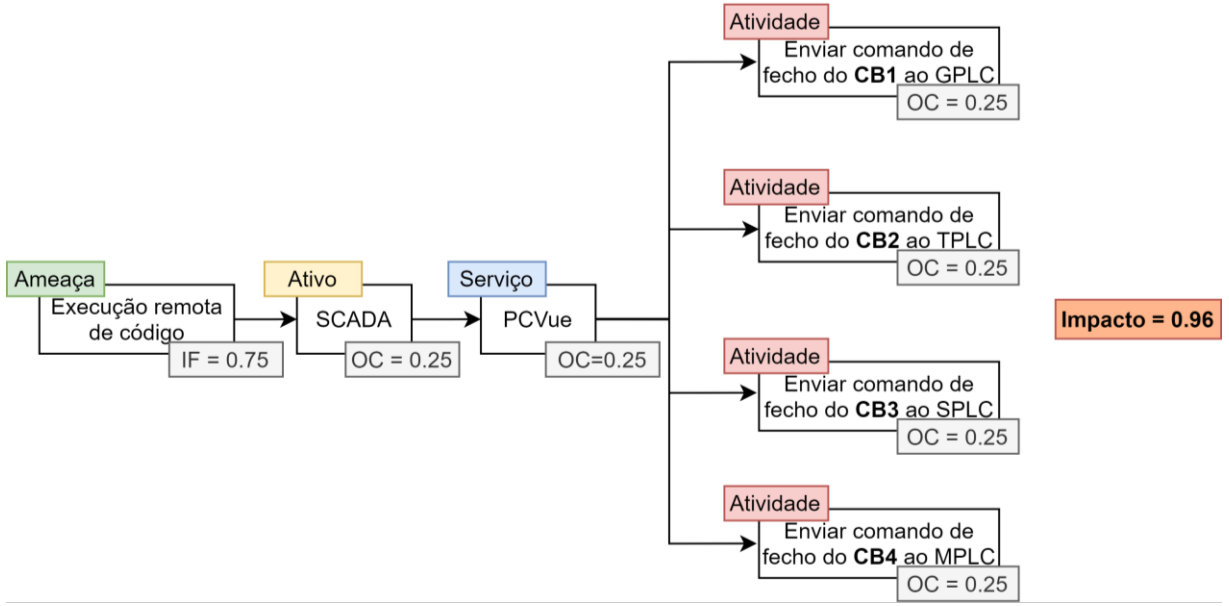


EXPERIÊNCIA #2

Avaliação

De que forma a combinação de caminhos triviais afeta o impacto?





EXPERIÊNCIA #2

Avaliação

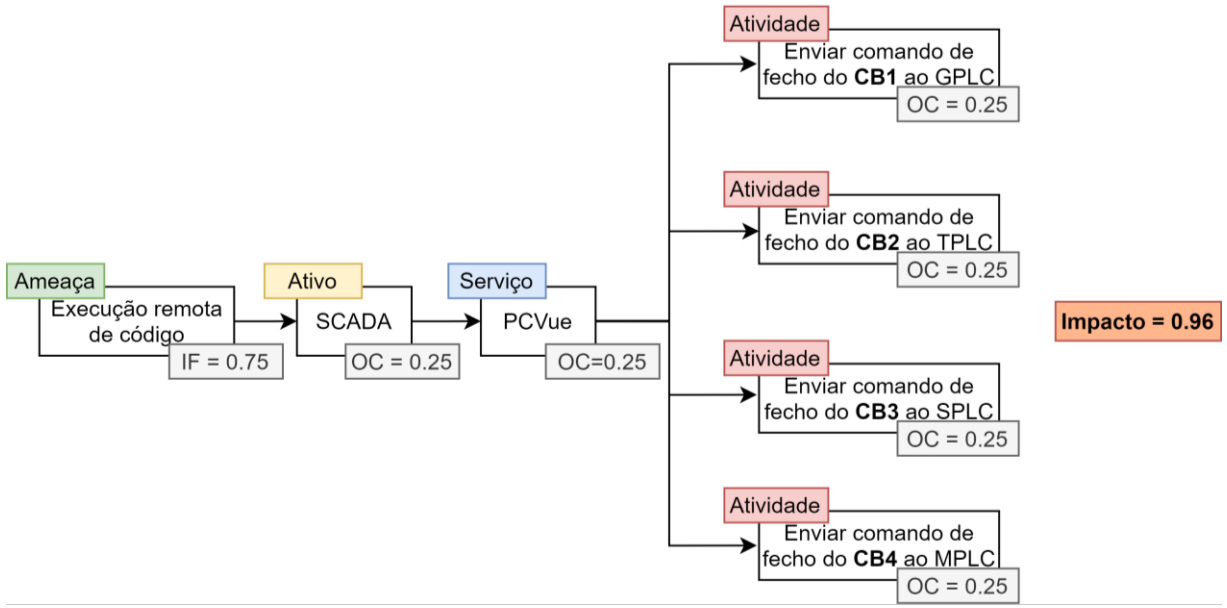
De que forma a combinação de caminhos triviais afeta o impacto?

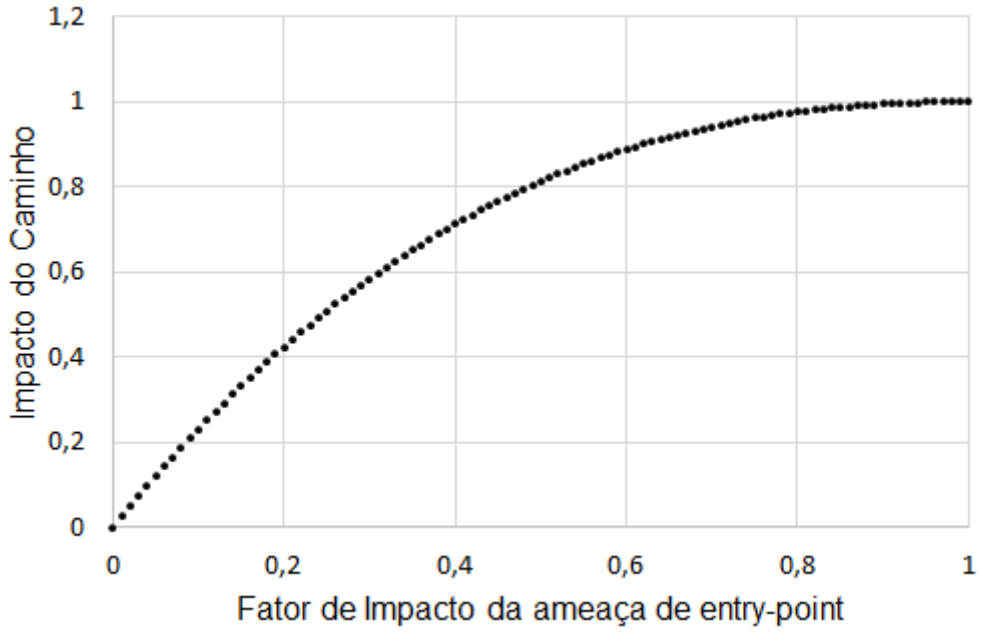
Propriedade: Quando são agregados dois ou mais caminhos, o impacto resultante é sempre superior ou igual aos impactos dos caminhos individuais

EXPERIÊNCIA #2

Avaliação

De que forma a combinação de caminhos triviais afeta o impacto?

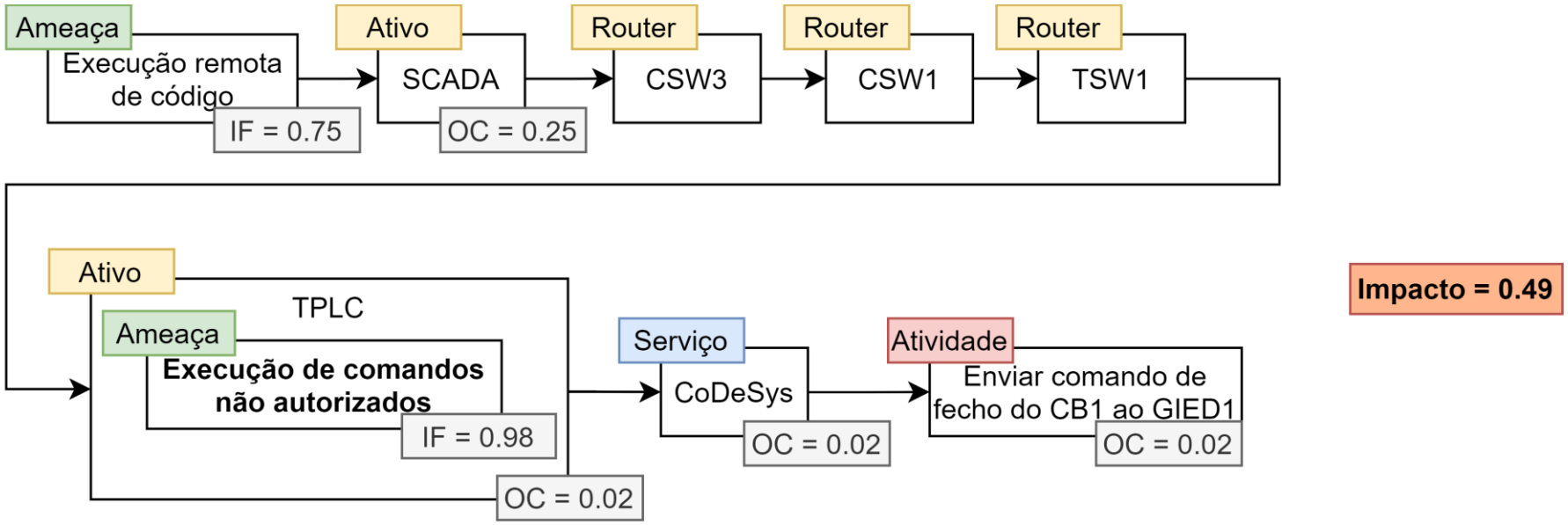




EXPERIÊNCIA #3

Avaliação

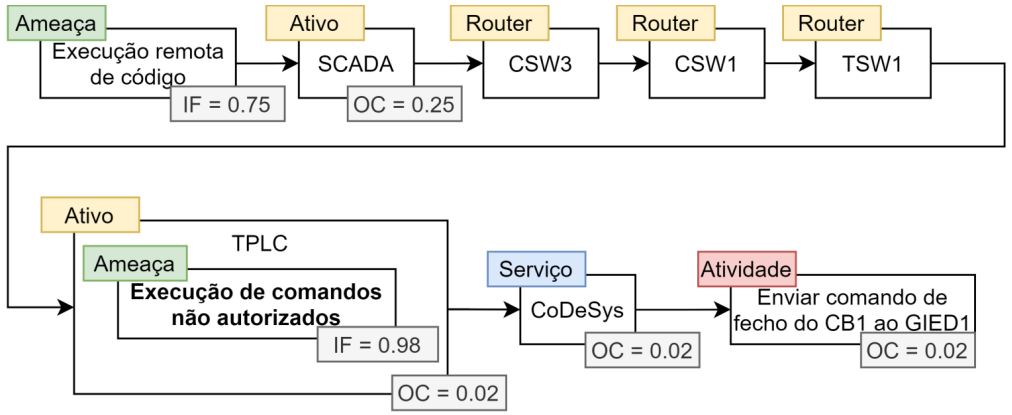
De que forma o facto de o atacante se mover lateralmente através da rede pode influenciar o impacto?



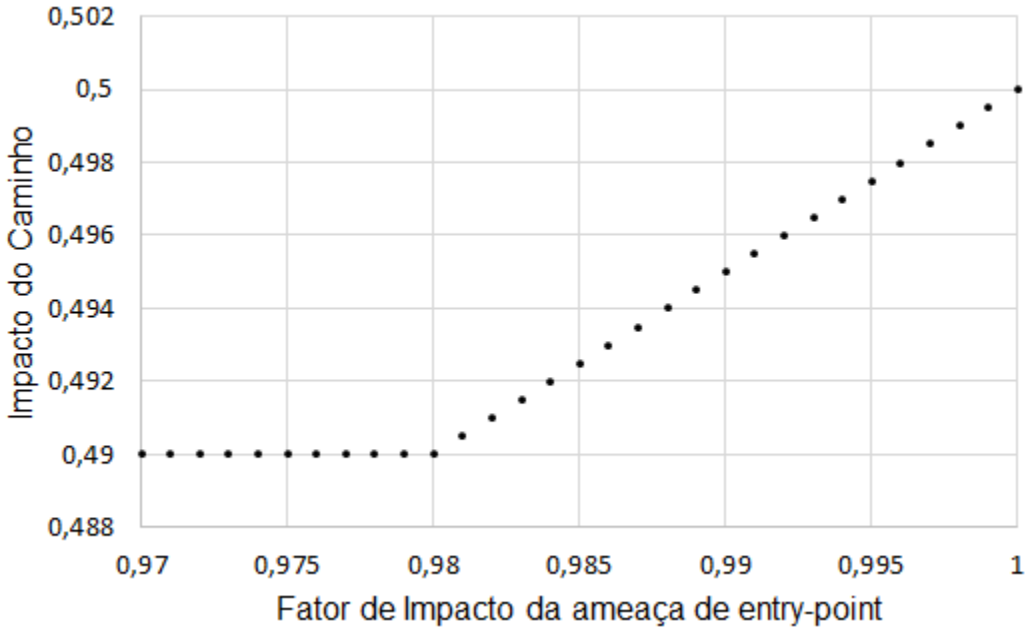
EXPERIÊNCIA #3

Avaliação

De que forma o facto de o atacante se mover lateralmente através da rede pode influenciar o impacto?

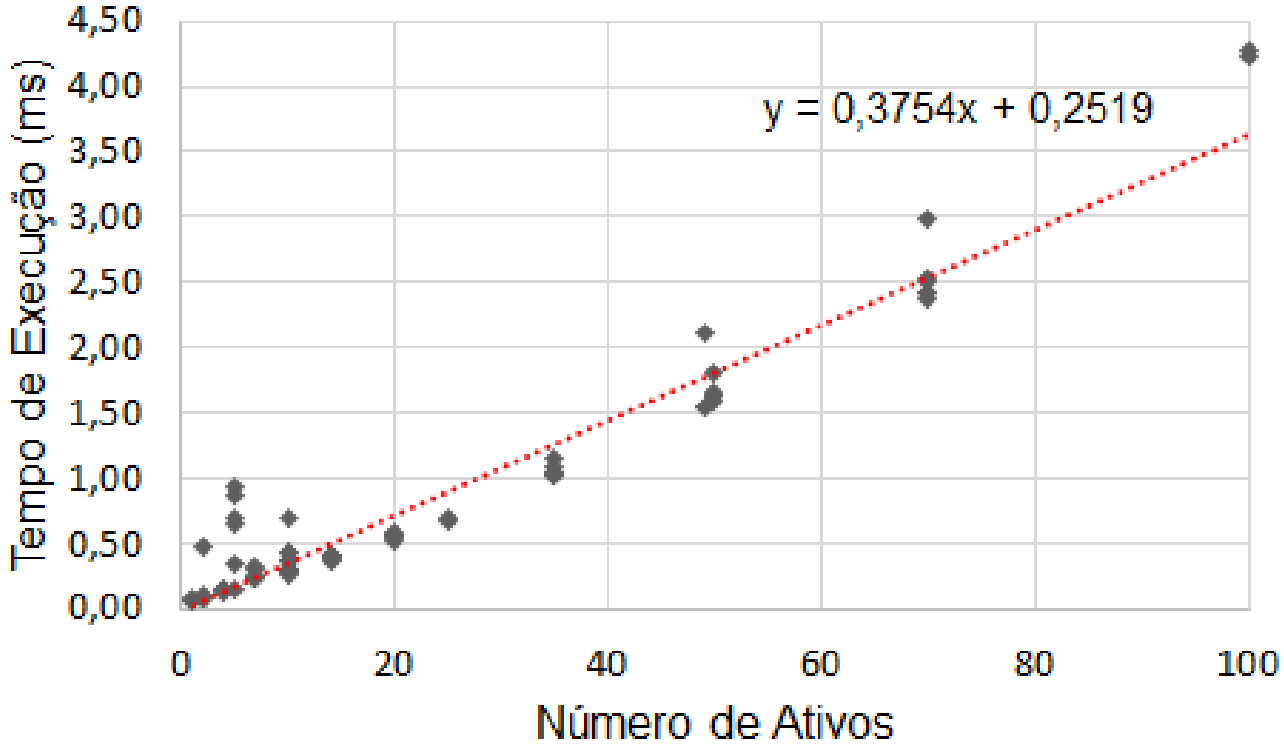


Impacto = 0.49



Análise de Performance

Avaliação



Complexidade: $O(n)$ → Solução é escalável

Estrutura da Apresentação

- **OBJETIVOS ALCANÇADOS**
  - Quantificação de impacto de ciber-ataques nos processos-negócio das organizações → Identificação de ameaças prioritárias → Plano de gestão de risco
  - Aplicação em Infrastruturas Críticas → Impacto de ciber-ameaças nos Processos Físicos

- **TRABALHO FUTURO**
  - Impacto de ameaças tendo em conta os Efeitos em Cascata que podem originar das dependências entre diferentes infraestruturas

Obrigado pela atenção!