A Collaboration Model to Recommend Network Security Alerts Based on the Mixed Hybrid Approach

Autores:

Arthur de Moura del Esposte (USP)

Rodrigo Campiolo (USP/UTFPR)

Fabio Kon (USP)

Daniel Macêdo Batista (USP)

Apresentador:

Rodrigo Campiolo

rcampiolo@utfpr.edu.br

Salvador, 01 de junho de 2016.

Roteiro

- Introdução
- Objetivos
- Trabalhos Relacionados
- Contribuição
- Métodos
- Resultados e Discussões
- Considerações Finais

Introdução

- Cibersegurança
  - Novas ameaças ou vulnerabilidades publicadas frequentemente.
  - Aumento no número de notificações e de fontes de notificações.
  - Nem todas notificações são relevantes para os administradores.
  - Tarefa onerosa para o administrador filtrar notificações de segurança ou mesmo manter-se atualizado.

Introdução

- Problema:

  Como minerar ou disponibilizar notificações de segurança relevantes para um administrador de redes considerando a variedade e quantidade de fontes, alertas e/ou rumores de ameaças obtidas de fontes de dados não estruturados?

Introdução

- Nossa proposta:

  Sistemas de Recomendação

- Definição e conceitos:
  - Indicar itens de interesse a usuários.
  - Abordagens comuns:
    - Filtragem colaborativa.
    - Filtragem baseada em conteúdo.
  - Abordagem híbrida mista (*mixed*).

Fonte: https://icrunchdatanews.com/recommender-systems-now-mainstream/ (2016)

Objetivos

- Projetar e avaliar de um **modelo de recomendação** para **alertas de cibersegurança** obtidos de **fontes de dados não estruturados**.

- Desenvolver um **recomendador** para **colaboração** entre **administradores de redes** e **especialistas de segurança**.

Trabalhos Relacionados

- Troca de informações entre organizações para prevenir e detectar ameaças antecipadamente (Apel et al. 2009, Flegel et al. 2010).
- Colaboração em redes sociais para extração de alertas de cibersegurança (Santos et al. 2013).
- Aplicações de sistemas de recomendação em diferentes áreas (filmes, artigos, ...).

Contribuição

- Modelo de recomendação para alertas de cibersegurança considerando os interesses de colaboração de administradores de redes.

Método de Pesquisa

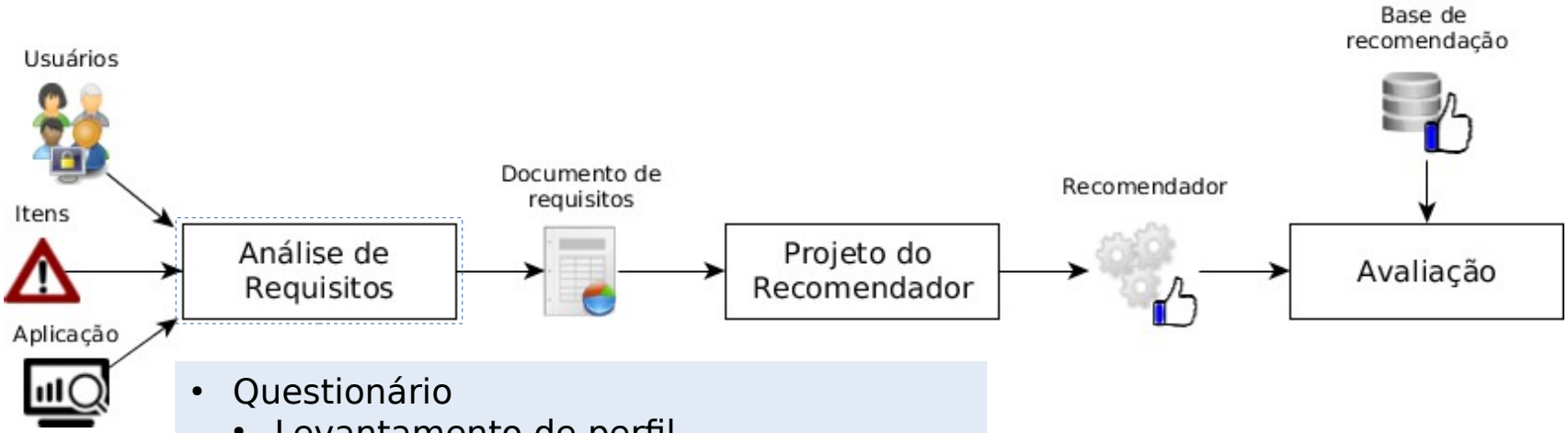
Figura: Fluxograma do método de pesquisa.

Método de Pesquisa

- Usuários: administradores de redes
- Itens: alertas de cibersegurança
- Aplicação: notificações de segurança de fontes de dados não estruturados

Figura: Fluxograma do método de pesquisa.

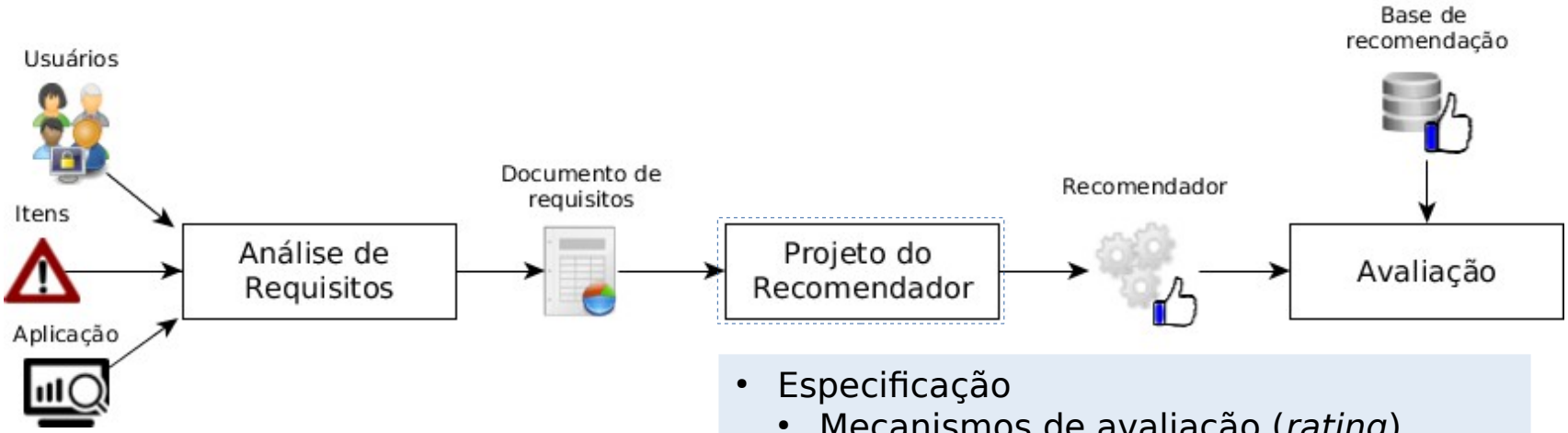
Método de Pesquisa



- Questionário
  - Levantamento de perfil
  - Conhecimento de segurança cibernética
  - Avaliação de interesse
  - Situações de uso

Figura: Fluxograma do método de pesquisa.

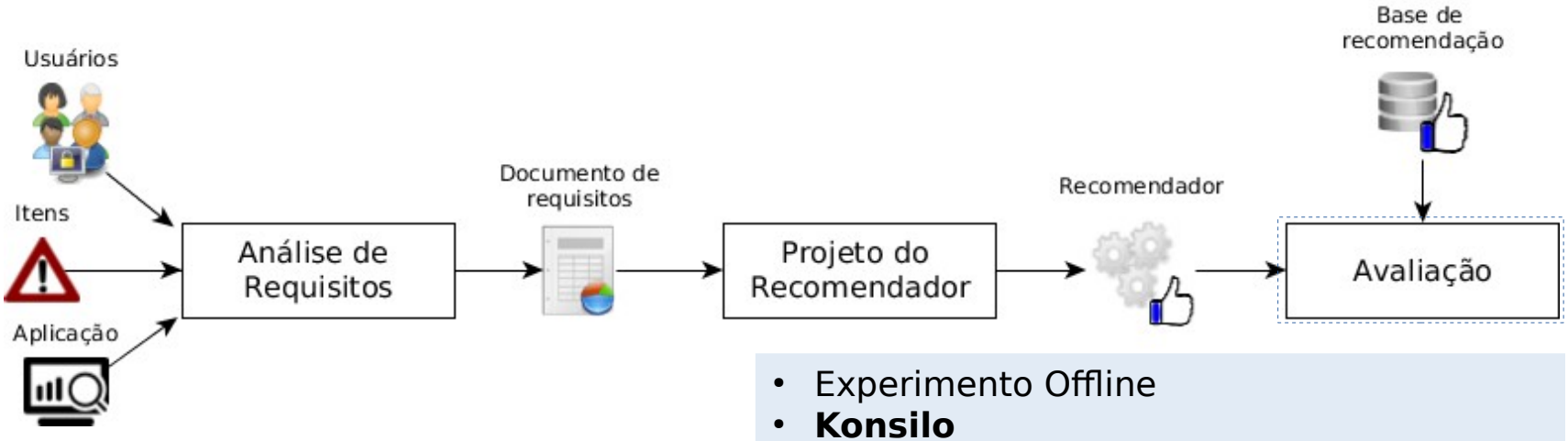
Método de Pesquisa



- Especificação
  - Mecanismos de avaliação (*rating*)
  - Modelo de transações do recomendador
  - Fluxo do modelo
- Seleção e implementação dos algoritmos

Figura: Fluxograma do método de pesquisa.

Método de Pesquisa



- Experimento Offline
- **Konsilo**
- Algoritmos
  - Precisão e abrangência
  - Limitação: base não específica

Figura: Fluxograma do método de pesquisa.

Resultados

- Questionário (20 respostas)
  - Perfil e conhecimento de cibersegurança: média 8 anos, maioria lê notícias de cibersegurança, minoria interage com outros administradores diretamente.
  - Interesse e situações de uso:

    todos tem interesse em um sistema de colaboração, sistemas operacionais e tipos de ataque como preferências dos usuários.
  - Alerta:

    (1) título (2) fonte (3) criticidade.

Resultados

- Questionário

Figura: Mecanismos de avaliação

Resultados

- Questionário

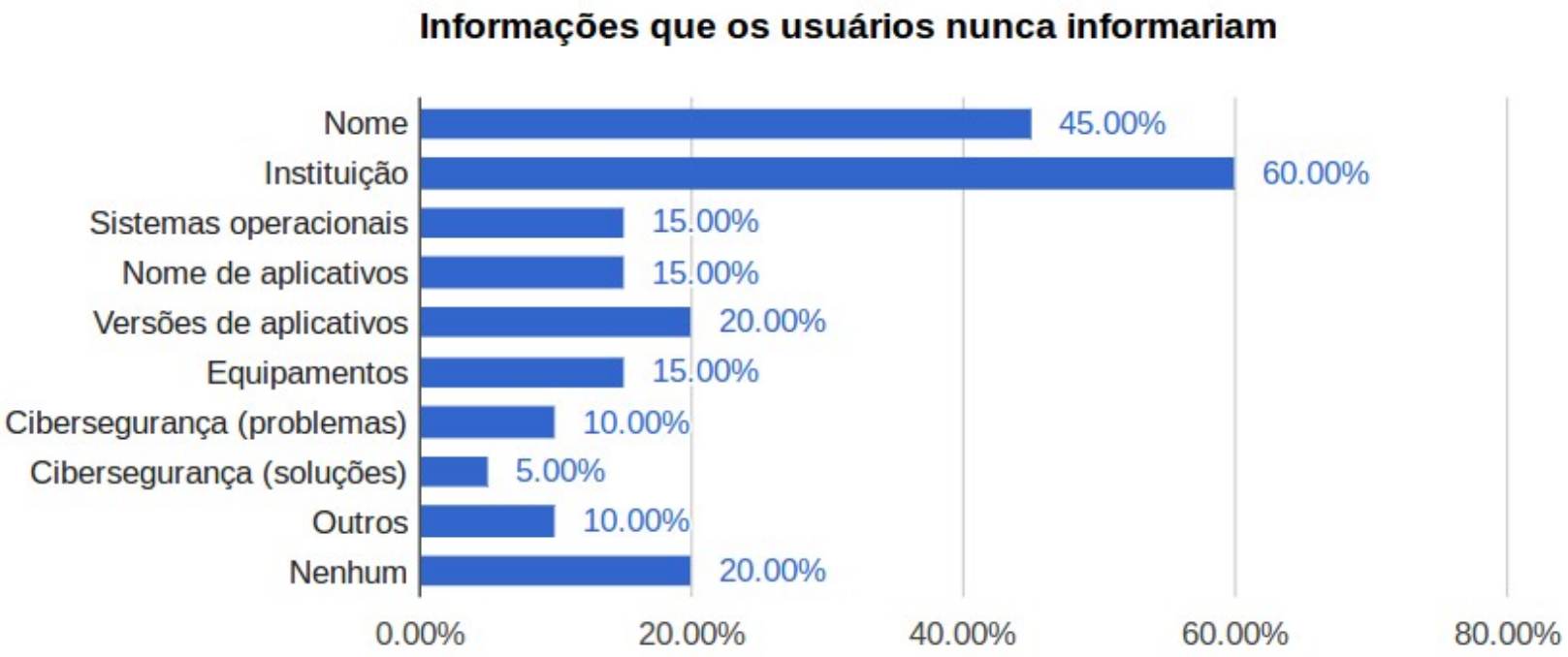


Figura: Informações que os usuários nunca forneceriam.

Resultados

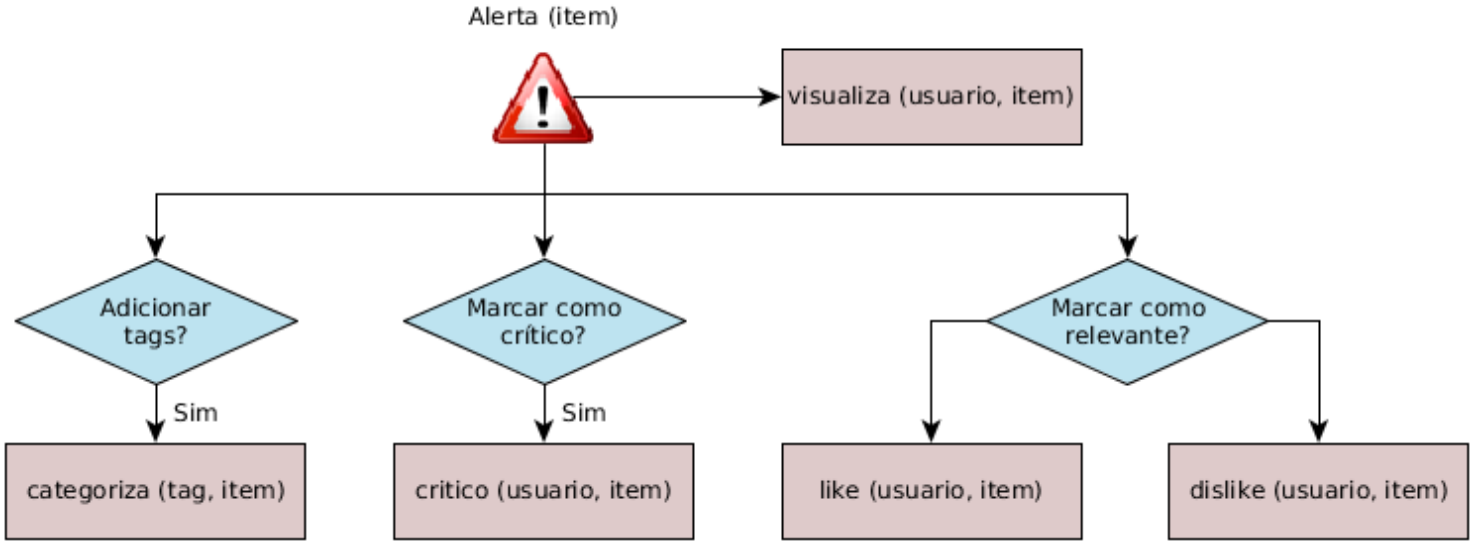
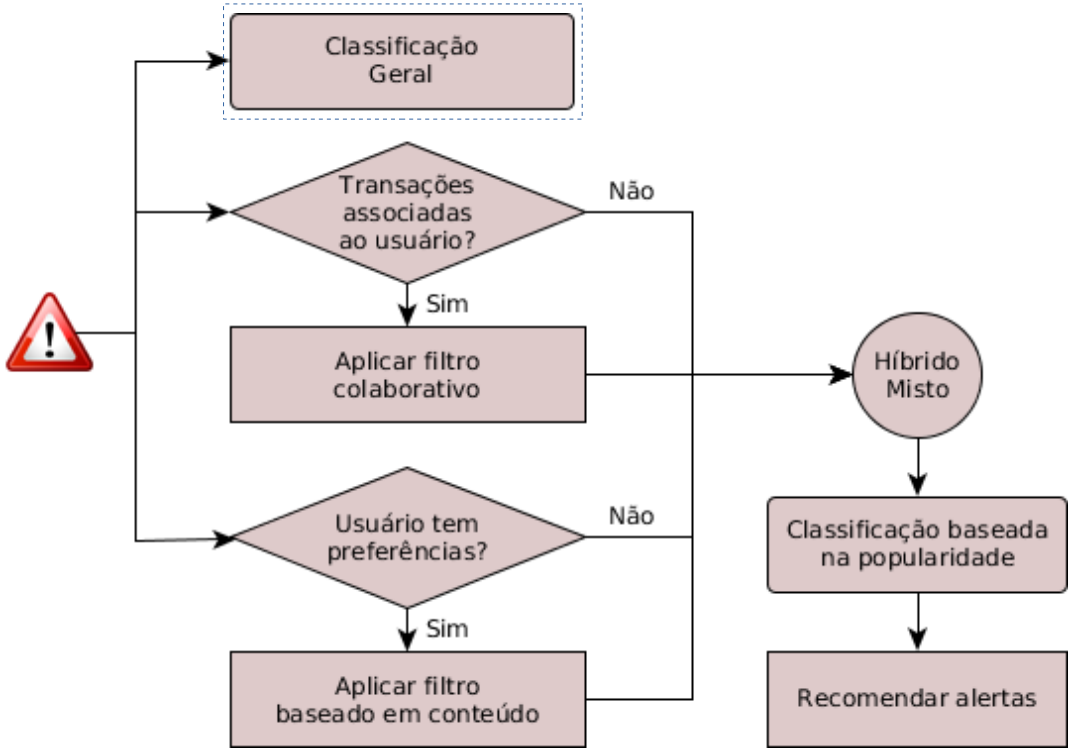


Figura: Mecanismos de avaliação e transações.

Resultados



- Classificação Geral

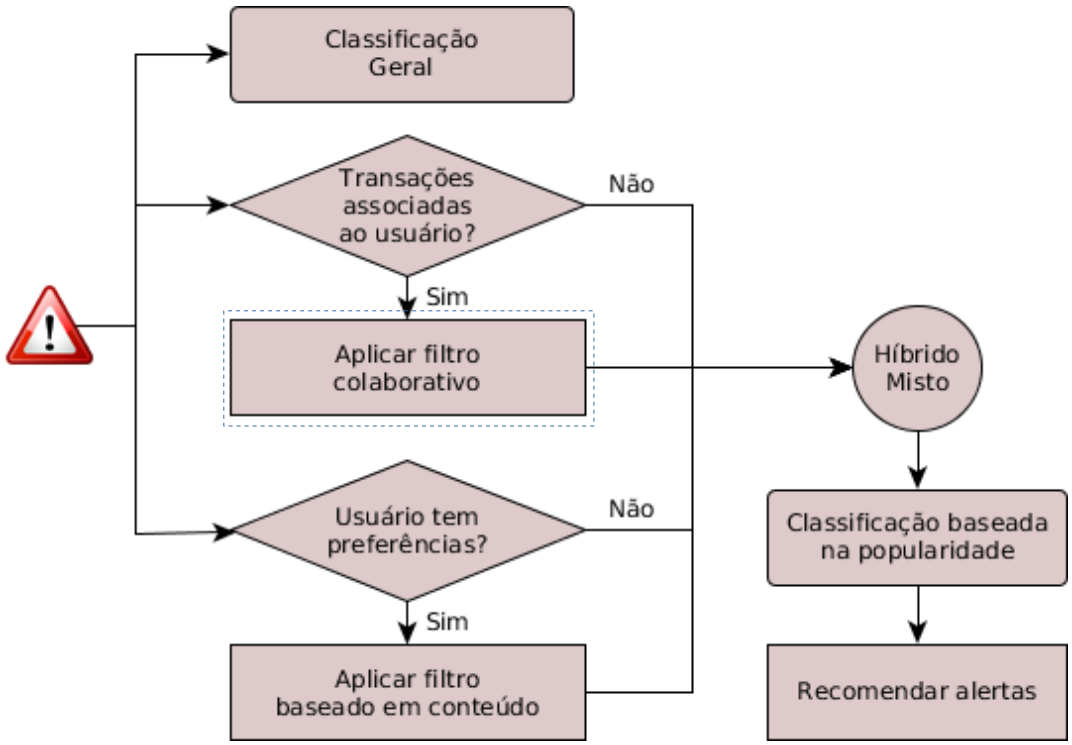
$$ranking\_score(i) = \frac{(\bar{v} \cdot \bar{r}) + (v_i \cdot r_i)}{\bar{v} + |r_i|}$$

$$r_i = \alpha c_i + \beta l_i - \phi d_i$$

i = item
v = votos
r = avaliação
c = criticidade
l = votos positivos (likes)
d = votos negativos (dislikes)

Figura: Fluxo do modelo do recomendador.

Resultados



- Filtragem Colaborativa

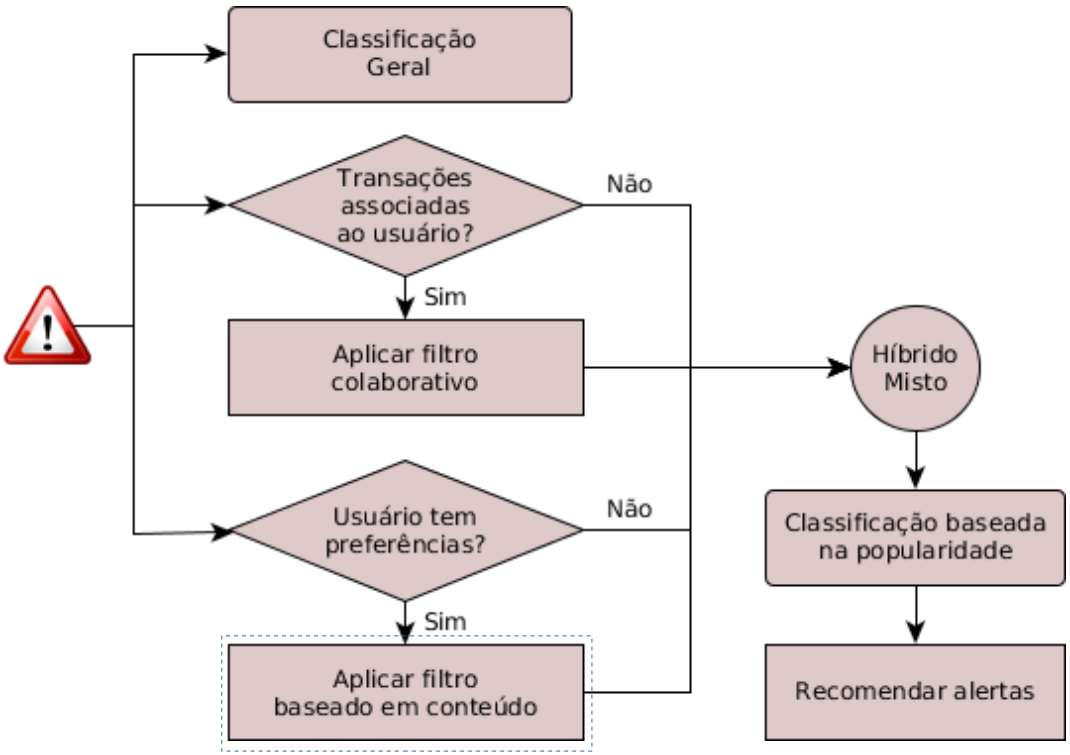
$$J(u,v) = \frac{|U_l \cap V_l|}{|U_l \cup V_l|} = \frac{|U_l \cap V_l|}{|U_l| + |V_l| - |U_l \cap V_l|}$$

$$score(u,r) = \frac{\sum_{v \in Neighbor_{(u)}} R_{v,r} \times J(u,v)}{|\sum_{v \in Neighbor_{(u)}} J(u,v)|}$$

U = itens do usuário u
V = itens do usuário v
r = item
R = avaliação

Figura: Fluxo do modelo do recomendador.

Resultados



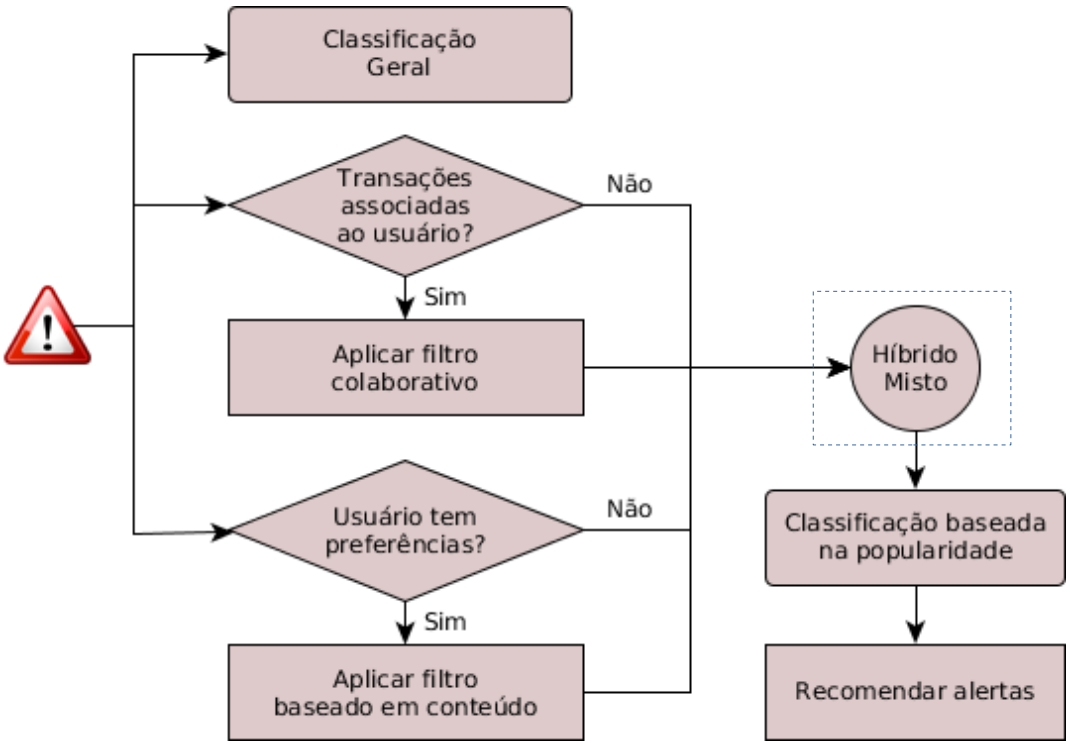
- Filtragem Baseada em Conteúdo

$$w_{tag}(u,i) = \frac{\sum_{t_i \in tag(i)} weight(u,t_i)}{\sum_{t_j \in tag(u)} weight(u,t_j)}$$

u = usuário
i = item
t = tag

Figura: Fluxo do modelo do recomendador.

Resultados



- Filtragem Híbrida Mista

$$mixed\_score(u,i) = 2^{\gamma} \cdot ranking\_score(i)$$

u = usuário
i = item

Figura: Fluxo do modelo do recomendador.

Avaliação

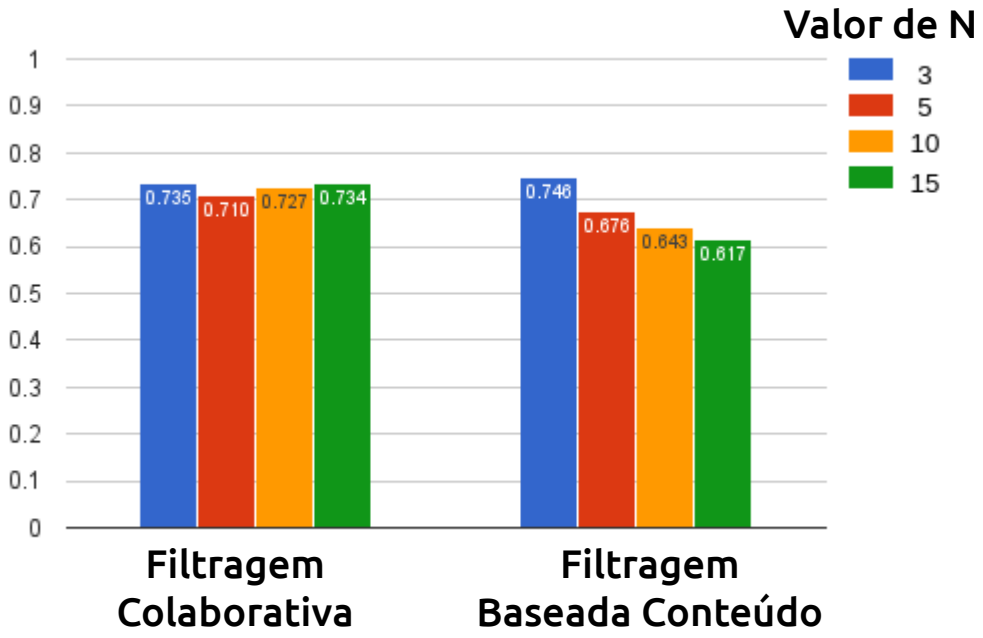


Figura: Precisão.

Avaliação

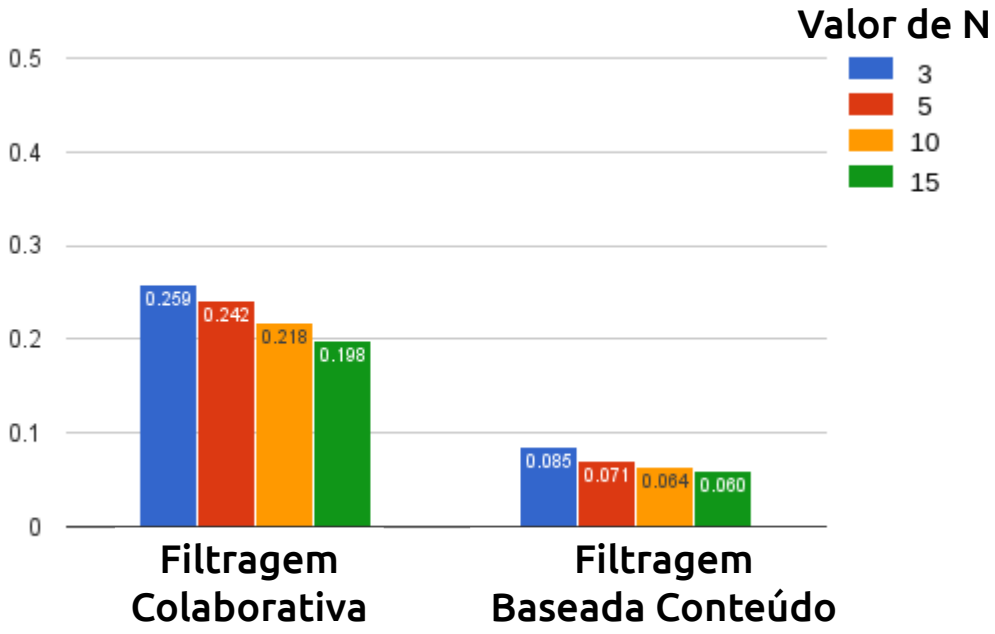


Figura: Abrangência.

Considerações Finais

- Modelo colaborativo para recomendação de alertas de cibersegurança.
- Exploração de técnicas de recomendação no escopo de Segurança da Informação.
- Limitações na avaliação do recomendador devido ausência de base.

- Trabalhos futuros: avaliação em base sintética e experimento on-line no projeto GT-EWS (Grupo de trabalho da RNP).

A Collaboration Model to Recommend Network Security Alerts Based on the Mixed Hybrid Approach

Obrigado pela presença e atenção.

Rodrigo Campiolo
rcampiolo@utfpr.edu.br

Arthur de Moura del Esposte
esposte@ime.usp.br

Daniel Macêdo Batista
batista@ime.usp.br

Fabio Kon
kon@ime.usp.br

PARANÁ
GOVERNO DO ESTADO
Secretaria da Ciência, Tecnologia e Ensino Superior

FUNDAÇÃO ARAUCÁRIA
Apoio ao Desenvolvimento Científico e Tecnológico do Paraná

RNP
REDE NACIONAL DE ENSINO E PESQUISA

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CAMPUS CAMPO MOURÃO

IME-USP