# Protótipo de software para avaliação da segurança da informação de uma empresa conforme a norma NBR ISO/IEC 17799

Douglas Rosemann
Prof. Carlos Eduardo Negrão Bizzotto

# Roteiro de Apresentação

- Introdução
- Segurança da Informação
- Norma NBR ISO/IEC 17799
- Especificação
- Implementação
- Conclusão
- Extensões

# Introdução - Motivação

- Preocupação crescente das empresas com a padrões de segurança
- Por ser uma norma publicada recentemente, poucos são os trabalhos acadêmicos que tratam de sua aplicação às empresas em geral.
- Oferecer às empresas que utilizam as tecnologias da informação e da comunicação, um guia de fácil utilização para a quantificação da adequação da empresa com relação aos padrões propostos pela norma NBR ISO/IEC 17799.

# Introdução – Objetivo Principal

Desenvolver um protótipo de software para auxiliar na avaliação da adequação de uma empresa à norma NBR ISO/IEC 17799, que trata da segurança da informação.

# Introdução – Objetivos Específicos

Os objetivos específicos do trabalho foram:

- permitir a inclusão de um *check-list* com perguntas sobre os tópicos propostos pela norma
- estabelecimento da quantificação do grau de conformidade da empresa em relação a cada tópico da norma
- inclusão de novos tópicos, permitindo a definição do peso de cada tópico incluído
- inclusão de novas perguntas
- trazer para a empresa avaliada um relatório apontando críticas sobre a situação da empresa frente a cada item da norma

# Segurança da Informação

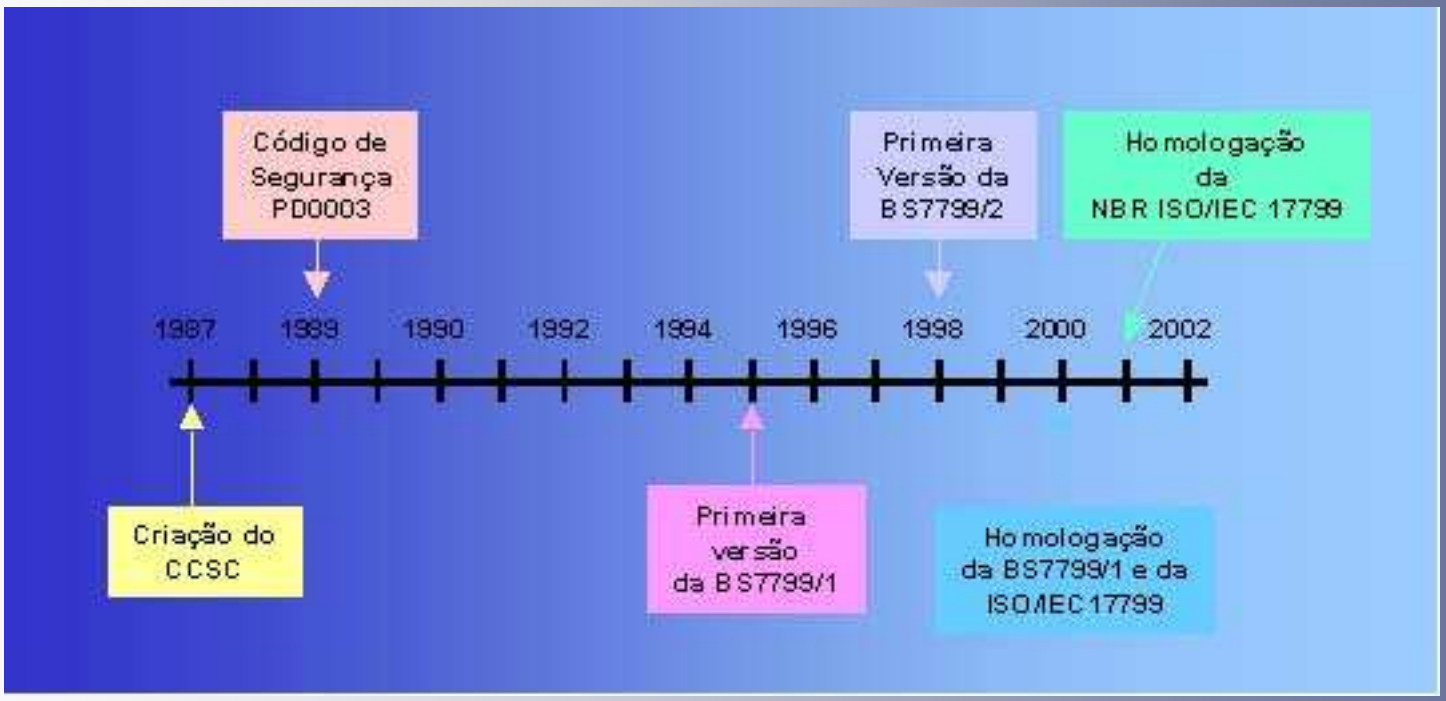
Segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio ABNT (2001).

Uma falha em um sistema informatizado, seja esta intencional ou não, pode causar a paralisação das atividades da organização com perdas muito significativas, quando não irreparáveis Ramos (2002).

# Tipos de Segurança

- físico: portas, trancas, travas de acesso a disquetes, circuito interno de TV, sistemas de controle de incêndio
- lógico (Técnico): senhas, permissões para arquivos, listas de controle de acesso, privilégios de contas, sistemas de proteção de energia
- administrativo: conscientização sobre segurança, revogação de contas de usuários, políticas

# Linha do Tempo




Fonte: Machado, 2002

# Norma NBR ISO/IEC 17799

Tecnologia da informação – Código de prática para a gestão da segurança da informação

- Esta norma possui recomendações para a gestão da segurança da informação, para ser usado pelos responsáveis na introdução, implementação ou manutenção da segurança em suas organizações.
- A norma prove uma base padrão de desenvolvimento de normas de segurança da organização, como também para as práticas de gestão de segurança provendo confiança no relacionamento entre as organizações.

# Capítulos da Norma

- Objetivo
- Termos e definições
- Política de Segurança
  - Prover a direção apoio
- Segurança Organizacional
  - Responsabilidade com terceiros e fornecedores
- Classificação e Controle dos Ativos de Informação
  - Proteção e responsabilidade dos ativos
- Segurança em Pessoas
  - Erros humanos, fraudes, uso indevido

# Capítulos da Norma

- Segurança Ambiental e Física
  - Acesso não autorizado, dano, perda, inserir perímetros
- Gerenciamento das Operações e Comunicações
  - Procedimentos operacionais, prevenção de vírus, backup, correio eletrônico
- Controle de Acesso
  - Controlar o acesso a informação, com senhas, monitoração
- Desenvolvimento de Sistemas e Manutenção
  - Segurança nos sistemas e suporte
- Gestão de Continuidade do Negócio
  - Evitar a interrupção das atividades
- Conformidade
  - Evitar violação de leis, regulamentos, estatutos ou outras regulamentações

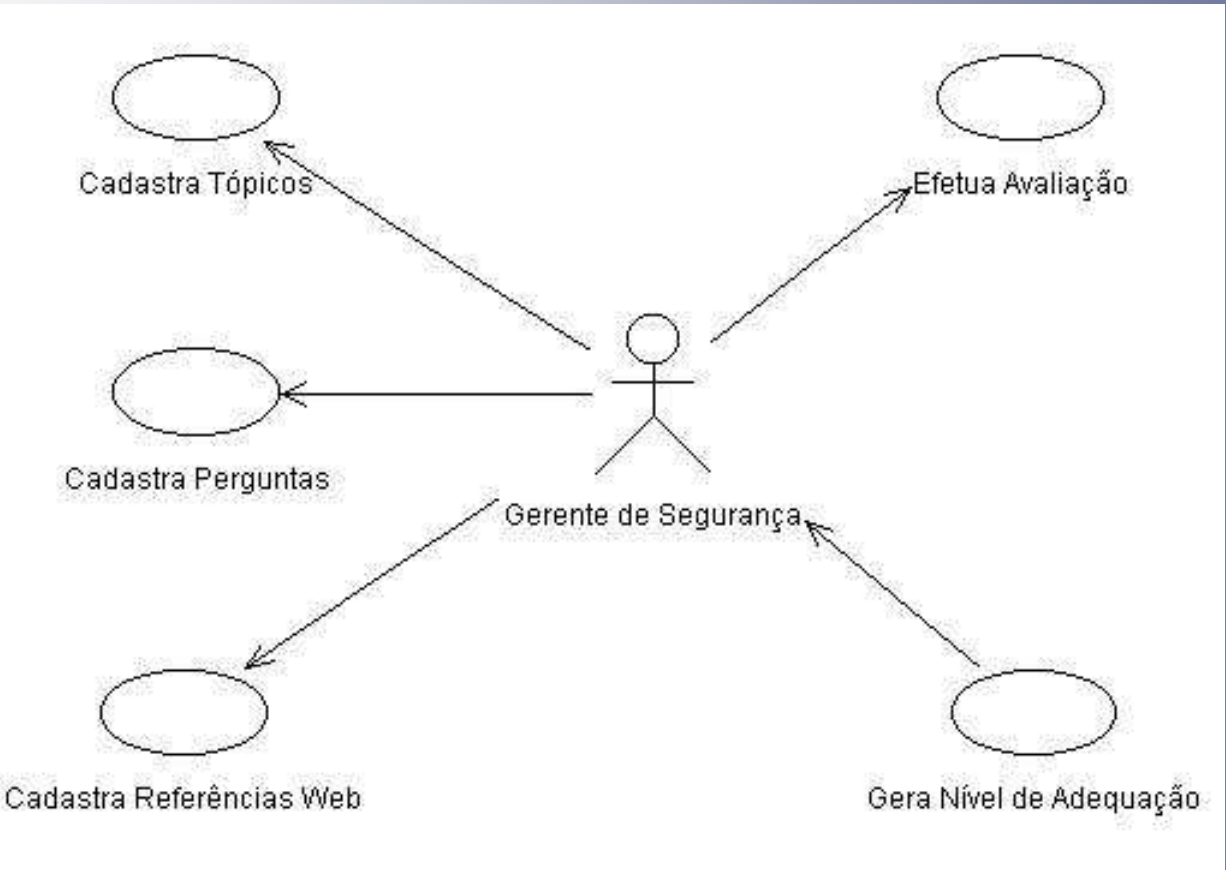
# Considerações da Norma

- Não é necessário implantar todos os tópicos propostos pela norma na organização

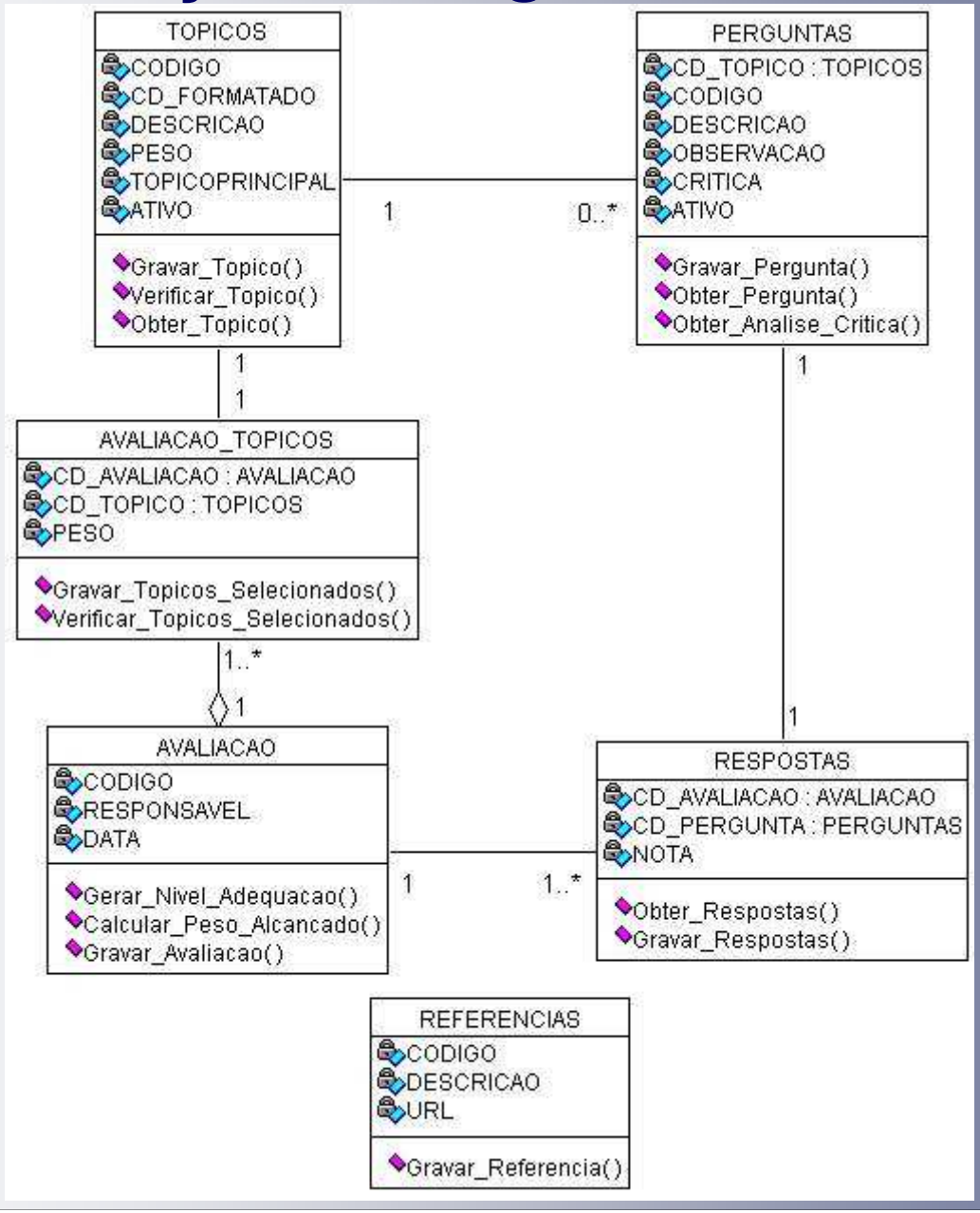
# Especificação:
## Técnicas e Ferramentas utilizadas

- Orientação a Objetos
- UML
- Rational Rose

# Especificação: *Use-Case*

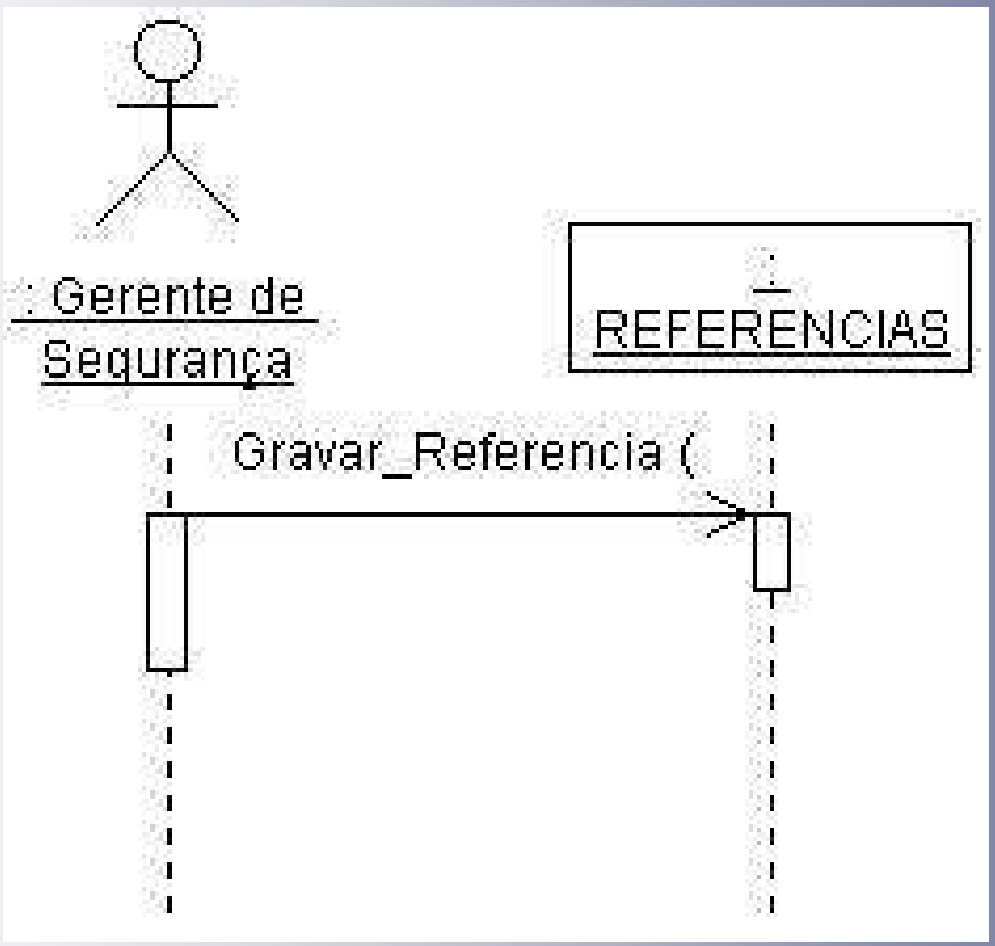


# Especificação: Diagrama de Classes



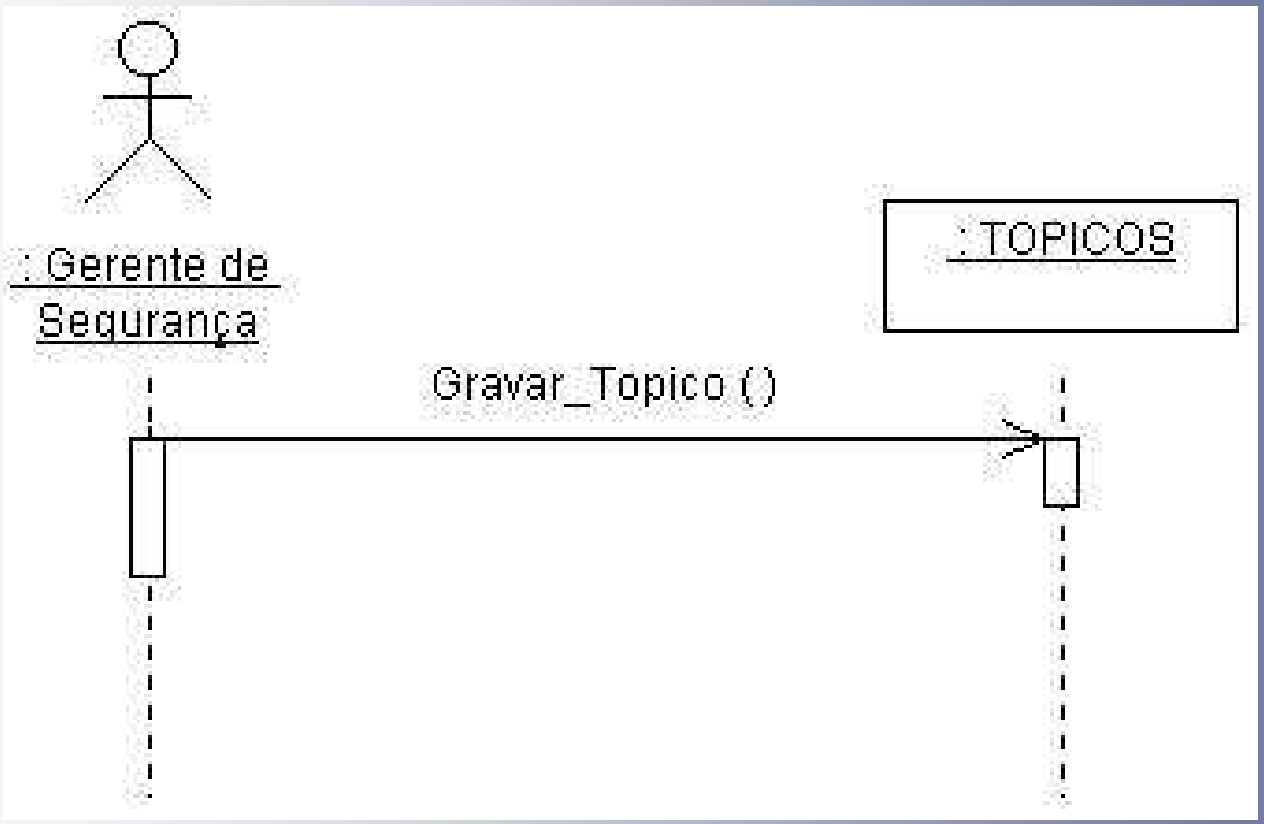
# Especificação:

## Diagrama de Seqüência – Cadastrar Referências



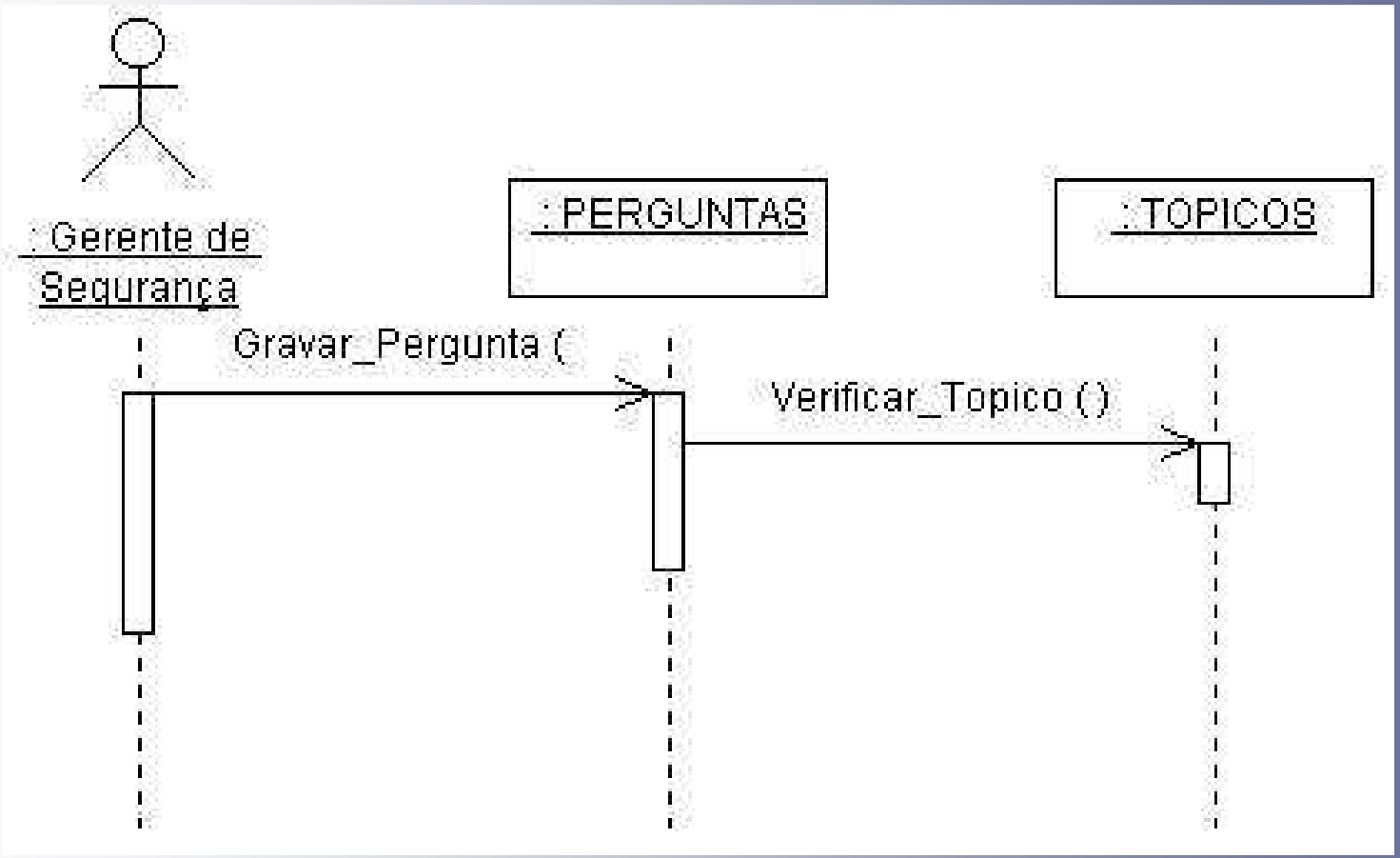
# Especificação:

## Diagrama de Seqüência – Cadastrar Tópicos



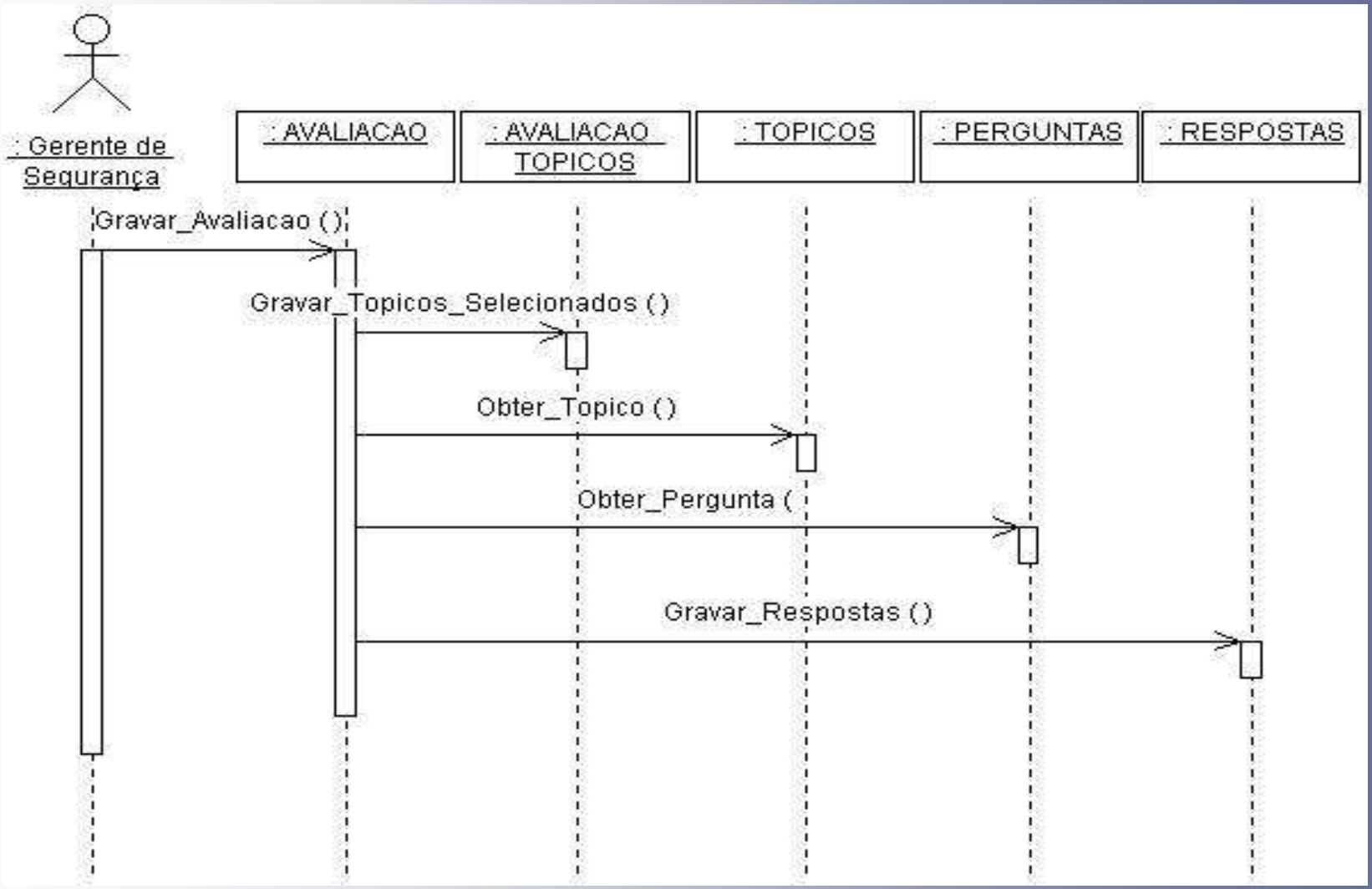
# Especificação:

## Diagrama de Seqüência – Cadastrar Perguntas



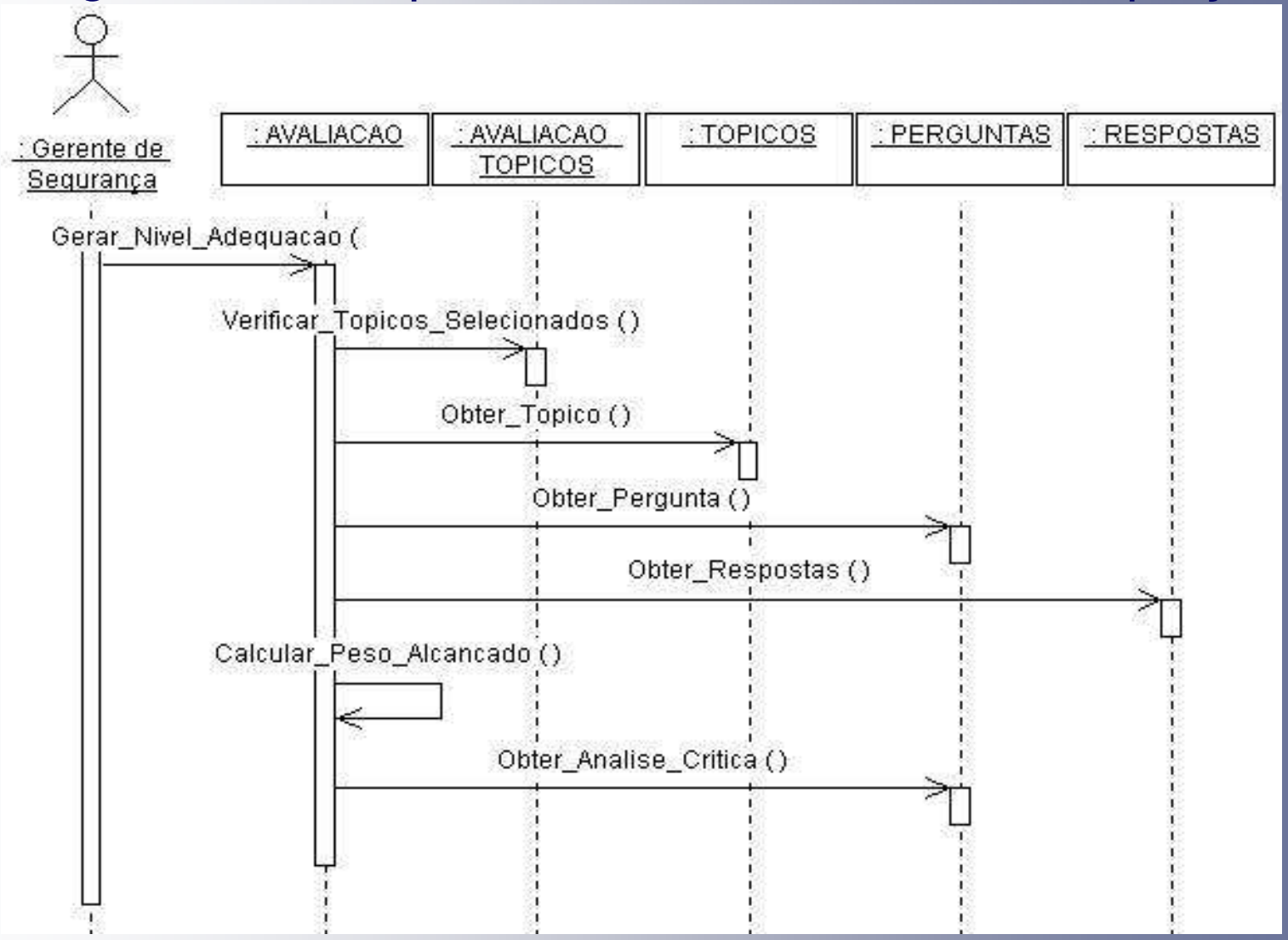
# Especificação:

## Diagrama de Seqüência – Efetua Avaliação

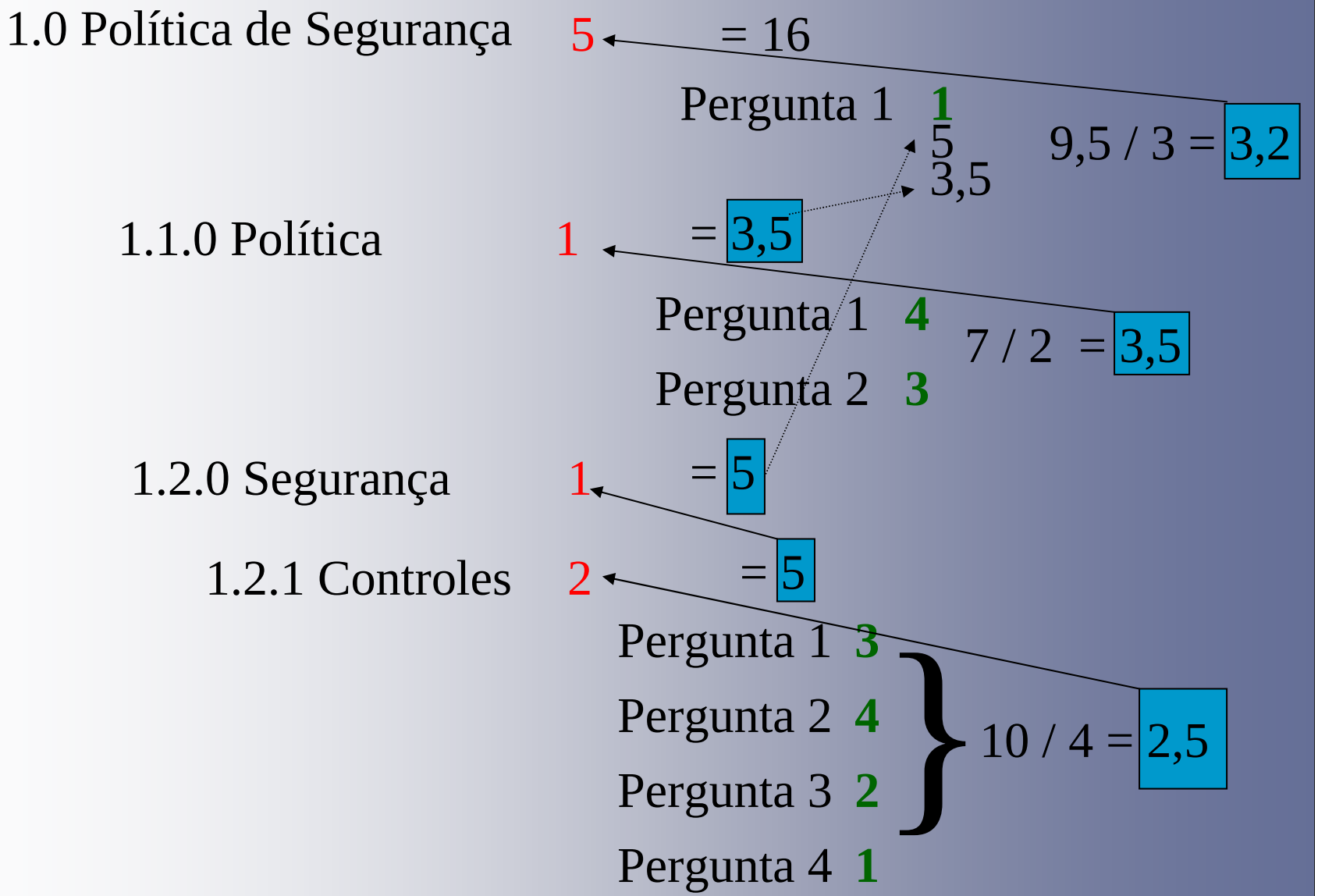


# Especificação:

## Diagrama de Seqüência – Gerar Nível de Adequação



# Exemplo da Geração

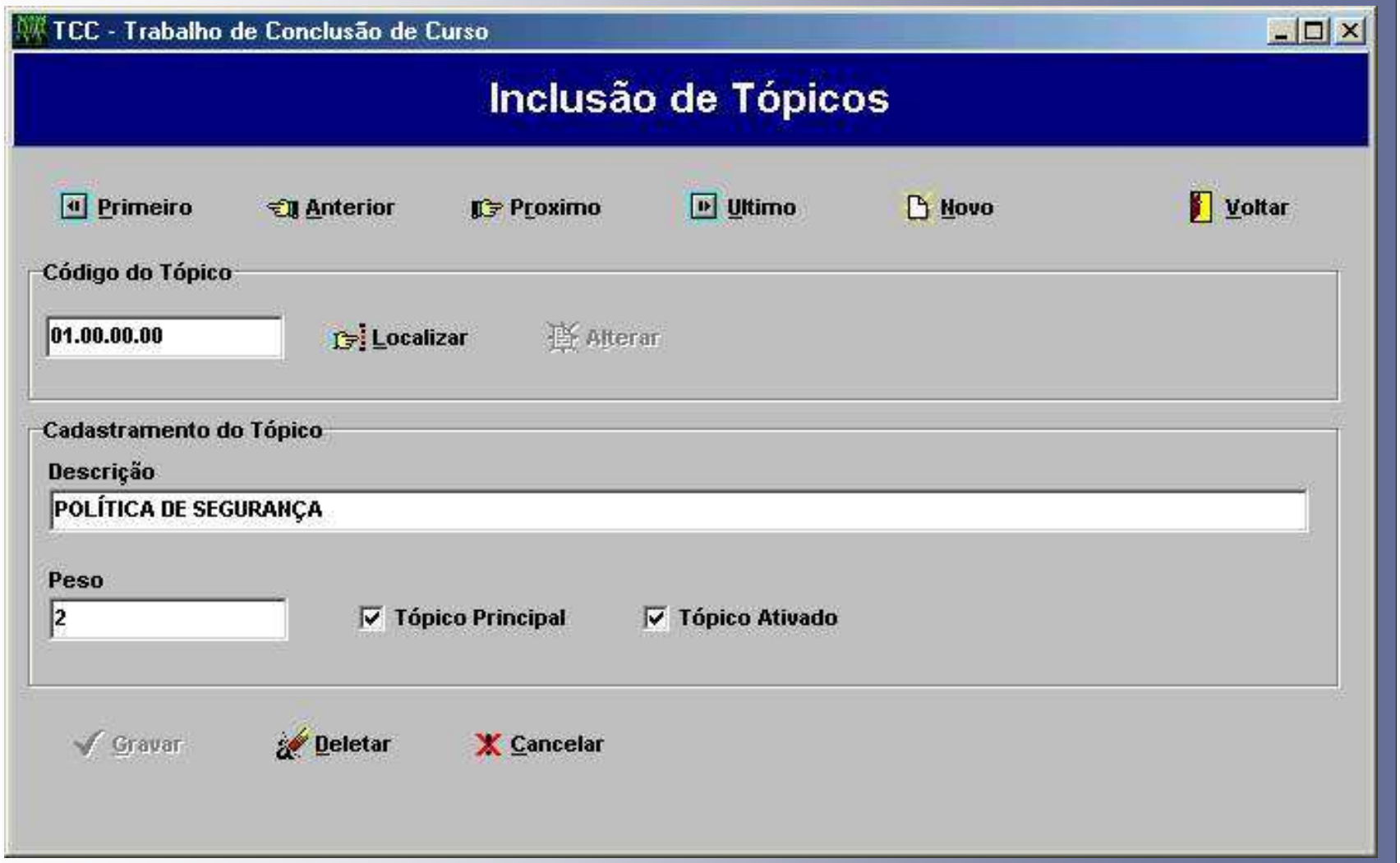



Média do Tópico foi 3,2, mas a quantificação foi 16

# Implementação:
## Técnicas e Ferramentas utilizadas

- Borland Delphi 5
- Banco de Dados Interbase

# Implementação



# Implementação

# Conclusão

- Objetivo principal foi atingido
- permite que sejam incluídos novos tópicos e perguntas(adequação rápida)
- quantifica em relação a cada tópico da norma
- Aponta críticas sobre a situação da empresa frente a cada tópico da norma
- A partir desse relatório a empresa pode estabelecer um plano para melhorar o grau de adequação com relação à norma NBR ISO/IEC 17799

# Extensões

- Integrar o software desenvolvido com softwares de outros TCC’s relacionados à qualidade de software
- Permitir que a avaliação possa ser feita via internet, de forma que pessoas em locais diferentes da empresa possam realizar a avaliação ao mesmo tempo
- Geração de relatórios gráficos, onde se possa visualizar, rapidamente, o desempenho da empresa nos diferentes tópicos