Sistemas de Informação

PUC Minas

Segurança de Sistemas de Informação

Aula 5: Gestão de Riscos

Prof. Fábio Leandro Rodrigues Cordeiro, Me.
fabio@pucminas.br

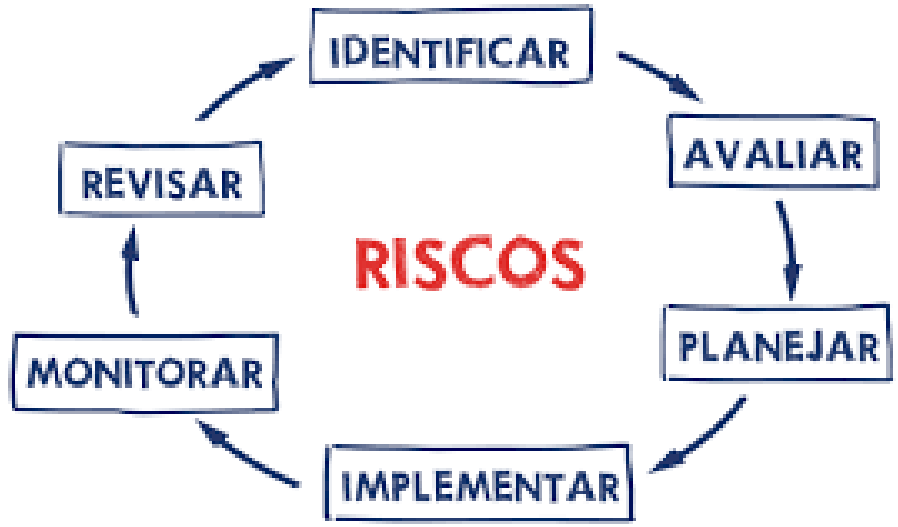
Objetivo da Aula

- Apresentar o processo de Gestão de Riscos de Segurança da Informação;

- Discutir aspectos de implementação do processo de gestão de riscos, com destaque para as atividades de Análise, Avaliação e Tratamento de Riscos.

Sumário

- Fundamentos de Gestão de Riscos
- Processo de Gestão de Riscos
- Considerações Finais
- Referências



Risco

Definição

Risco é a combinação da **probabilidade** de um determinado **evento** ocorrer e de suas **consequências (impacto)**.

Evento: é a reação entre ameaças, as vulnerabilidades e os danos causados – **consequências**;

Ao descrever os riscos estamos detalhando cenários, cujas consequências afetam a **CID** de determinados ativos.

Risco

Exemplo

Exemplo de um Evento de Riscos

Ativo: Estação de trabalho

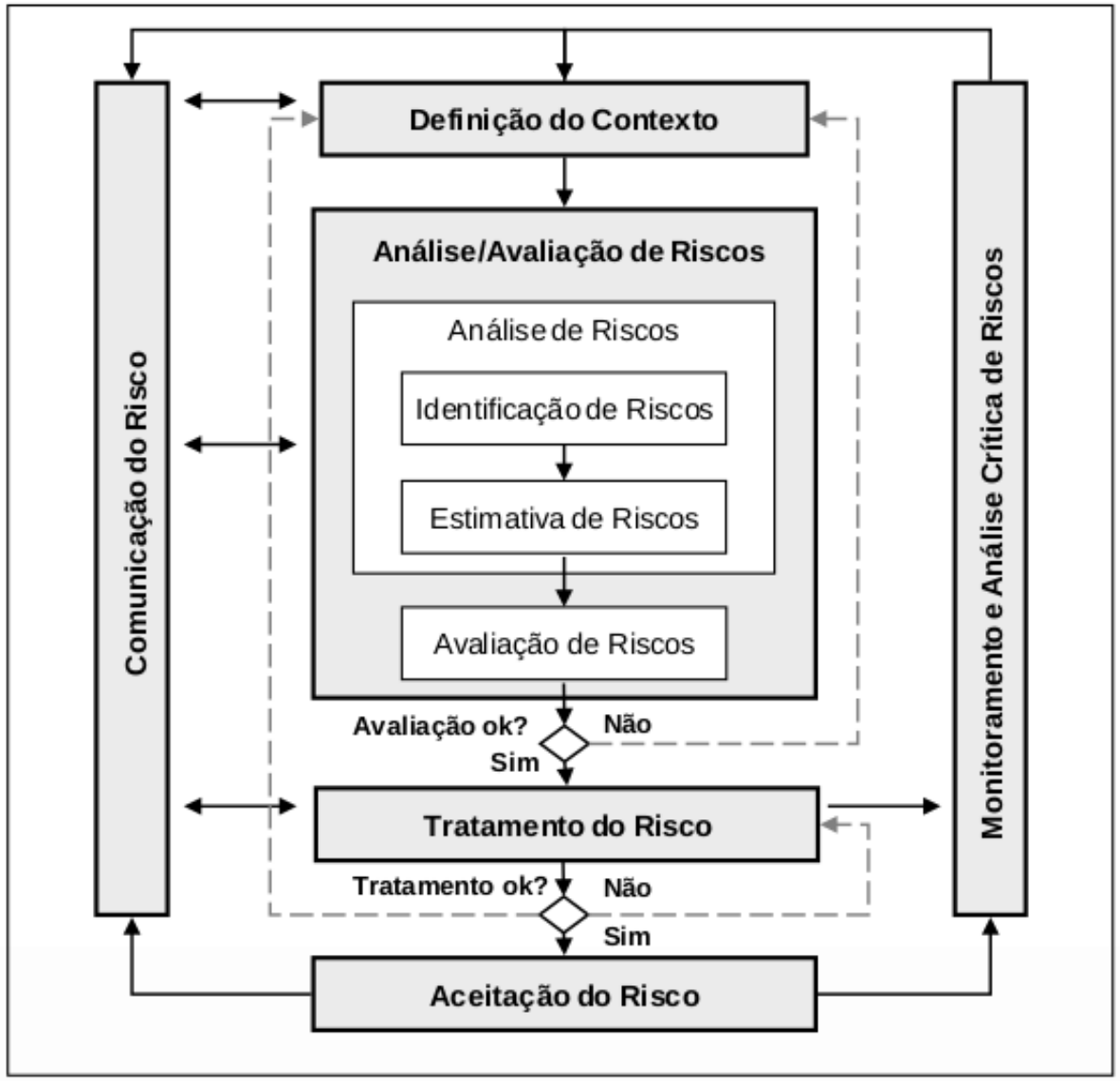
Evento: **Usuário** consegue acesso lógico não autorizado, devido a erros na definição de permissões.

Processo de Gestão de Riscos

ISO 27005

O processo de Gestão de Riscos em Segurança da Informação conforme a **ISO 27005**

Atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.



Processo de Gestão de Riscos

Definição de Contexto

O contexto para GR de SI envolve: (a) a definição de **critérios básicos**, (b) a definição do **escopo** e dos limites da GR e (c) o estabelecimento de uma **organização apropriada** para operar a Gestão de Riscos de SI.

Processo de Gestão de Riscos

Análise e Avaliação de Riscos

Convém que os riscos sejam **identificados**, **quantificados** ou **descritos qualitativamente**, **priorizados** em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização.

A análise/avaliação de riscos consiste nas seguintes atividades:

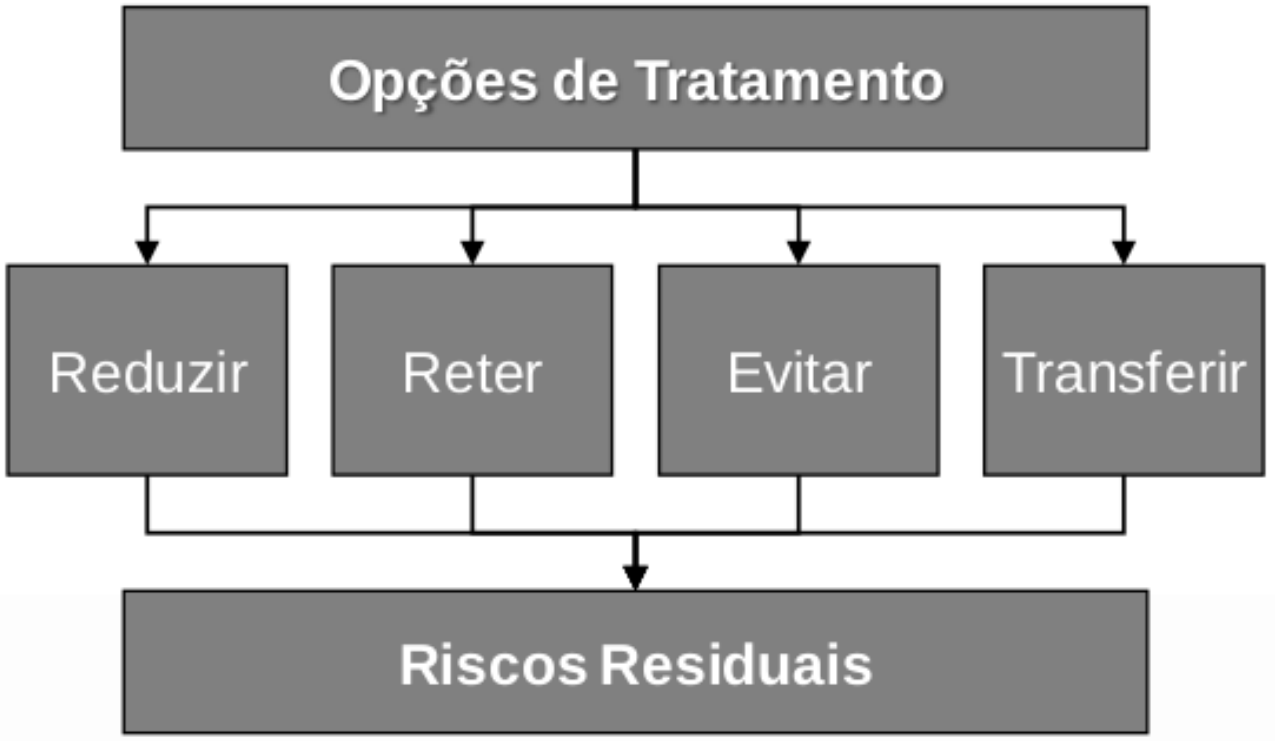
- Análise de Riscos
  - Identificação e Estimativa de Riscos

- Avaliação de Riscos

Processo de Gestão de Riscos

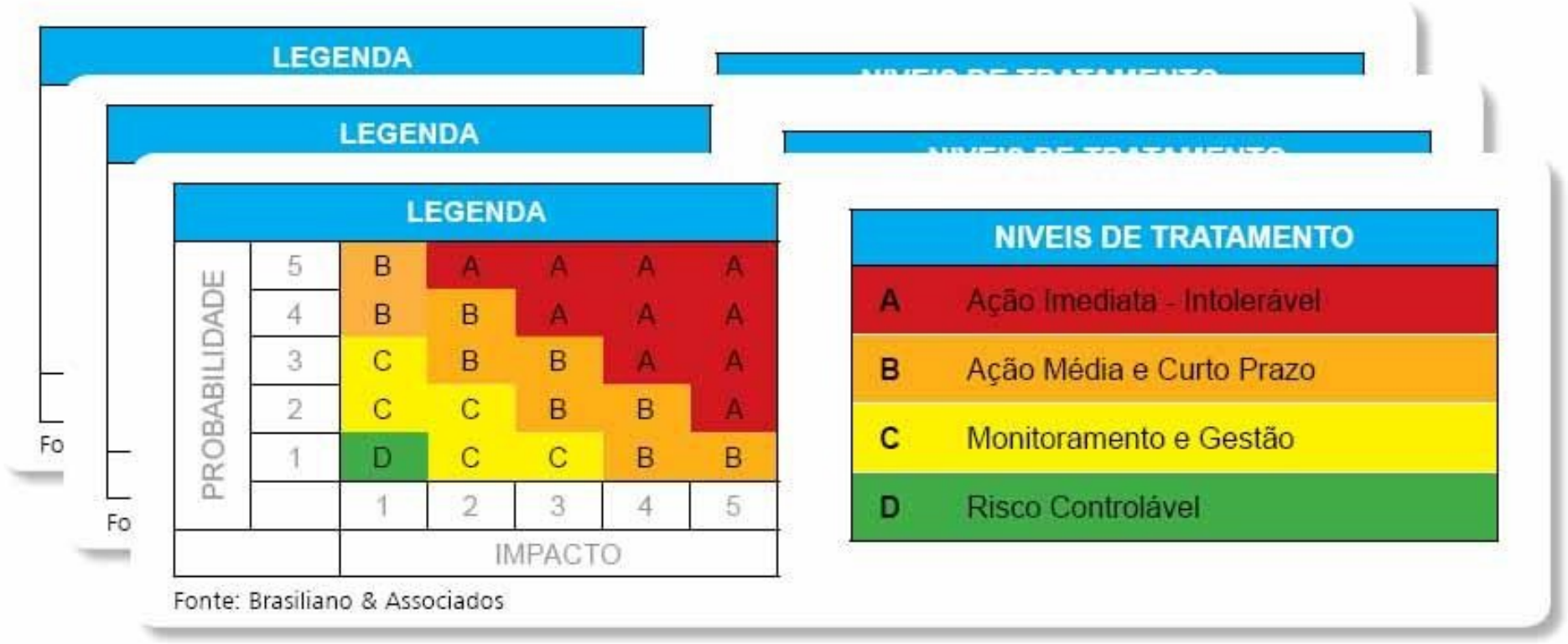
Tratamento de Riscos

Convém que opções para o tratamento dos riscos sejam selecionadas e que o **Plano de Tratamento do Risco (PTR)** seja definido.



Processo de Gestão de Riscos

Tratamento de Riscos

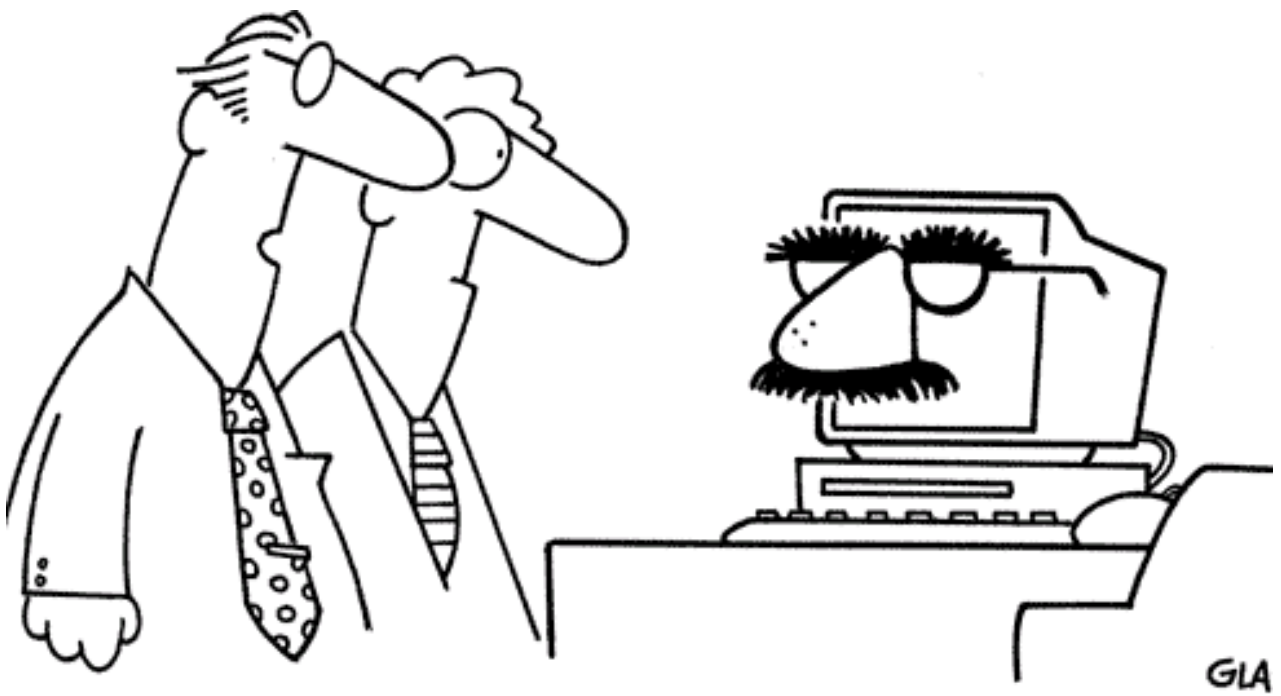


Fonte: Brasiliano & Associados

Processo de Gestão de Riscos

Tratamento de Riscos

Deve ser ter planejamento de orçamento para GR.



“I’m sure there are better ways to disguise sensitive information, but we don’t have a big budget.”

Processo de Gestão de Riscos

Tratamento de Riscos

O **risco residual** representa o **nível de risco remanescente** após o tratamento de riscos. Uma vez que o **PTR** tenha sido definido, os riscos residuais precisam ser estimados.

Processo de Gestão de Riscos

Aceitação do Risco

Convém que as informações sobre riscos sejam trocadas e/ou compartilhadas entre o tomador de decisão e as outras partes interessadas, com o objetivo de **atingir um consenso sobre como os riscos devem ser administrados**.

Processo de Gestão de Riscos

Monitoramento dos Riscos

Convém que os riscos e seus fatores (valores dos ativos, impactos, ameaças, vulnerabilidades e probabilidade de ocorrência) sejam monitorados e analisados criticamente, a fim de se **identificar**, o mais rapidamente possível, **eventuais mudanças no contexto da organização** e de se manter uma visão geral dos riscos.

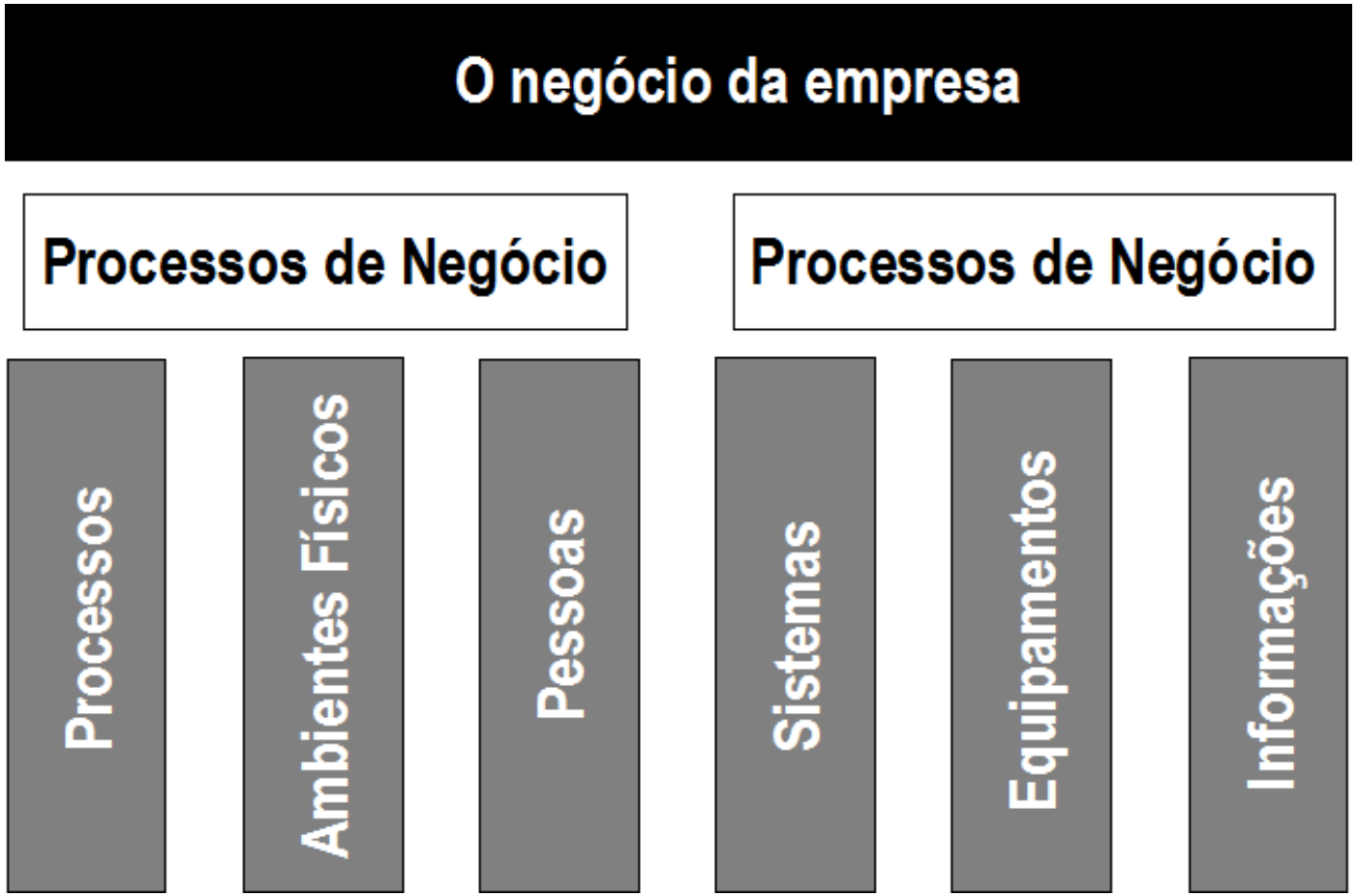
Processo de Gestão de Riscos

Melhoria contínua (PDCA)

Processo do SGSI	Processo de GR de SI
Planejar	Definição do Contexto Análise/Avaliação de Riscos Plano de Tratamento do Risco Aceitação do Risco
Executar	Implementação do Plano de Tratamento do Risco
Verificar	Monitoramento Contínuo e Análise Crítica de Riscos
Agir	Manter e Melhorar o Processo de GR de Segurança da Informação

Processo de Gestão de Riscos

Considerações



Processo de Gestão de Riscos

Fatores Críticos de Sucesso

- A análise e riscos deve fazer parte de um **processo permanente** de gestão de riscos de segurança da Informação, capaz de identificar novas vulnerabilidades e ameaças.

- É necessário criar uma estrutura adequada para gestão de riscos, mas tão importante quanto definir funções e responsabilidades é desenvolver uma **cultura de gestão de riscos.**

- Com isso a organização mantém o nível de risco em **patamares aceitáveis**.

Estudo de Caso

Gestão de Riscos (ISO-27005) e Startups

Levando em consideração o cenário cada vez mais crescente de Startups em diversos áreas, faça uma análise na ótica da Gestão de Riscos em função desse novo modelo de empreendimento e os impactos da Gestão de Riscos no seus modelos.

a) Faça uma análise exploratório dos impactos positivos e negativos que a gestão de riscos acarreta nesse modelo de iniciativas.

b) Pesquise cenários substanciais onde a aplicação de Gerência de Riscos como guia e normalização influenciou positivamente ou negativamente na construção do produto ou serviço.

c) Faça uma análise crítica desse modelo de investimento levando em considerações questões normativas de gerência de riscos e outros padrões de normatização.

d) Tipos de Startups: I) Fintech II) Small Business III) Scalable Startup IV) Large Company V) Lifestyle VI) Buyable VII) Social Startup

e) Trabalho deverá ser feito em grupo de 6 a 7 pessoas. Não será aceito trabalho individual.

f) Deverá seguir regras de padronização conforme norma de artigo PUC Minas, impreterivelmente em Latex.

Referências

Notas de Aula: Prof. Prof. Leonardo Lemes Fagundes.

ISO 27001 Security. Information Security Compliance. 2011.

ABNT NBR ISO/IEC 27002:2006. Código de Prática para a Gestão da Segurança da Informação, 2006.