Proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação

Janice Mayer (orientanda)
Leonardo Lemes Fagundes (orientador)

Universidade do Vale do Rio dos Sinos (UNISINOS)

j.mayer@brturbo.com.br

SBSEG 2008 - WTICG Sessão Técnica 2 - Segurança em Redes e Aplicações I
01 de Setembro de 2008

Sumário

Introdução

- A informação tornou-se um dos ativos mais valiosos para as organizações, a ponto de o vazamento ou a indisponibilidade colocar em risco a execução de processos vitais ao negócio.
- A *Gestão de Riscos* representa uma frente essencial para que a empresa possa estimar ameaças, vulnerabilidades e impactos em Segurança da Informação.
- A *Gestão de Riscos* é implementada para buscar conformidades com as leis, normas e regulamentações, bem como atender a requisitos obrigatórios da área de Segurança da Informação.

3

Motivação

- As empresas precisam implementar a gestão de risco de forma consistente e sistematizada.
- Não há um *modelo de maturidade* que meça ou avalie o nível de maturidade do processo de Gestão de Riscos em Segurança da Informação,
- diferentemente do que acontece com outras áreas que possuem modelos de maturidade como:
  - CMMI (*Capability Maturity Model Integration*)
  - COBIT (*Control Objectives for Information and related Technology*)

4

Objetivo

- Especificar e estruturar um modelo para avaliar o nível de maturidade das empresas em relação ao processo de Gestão de Riscos em Segurança da Informação.

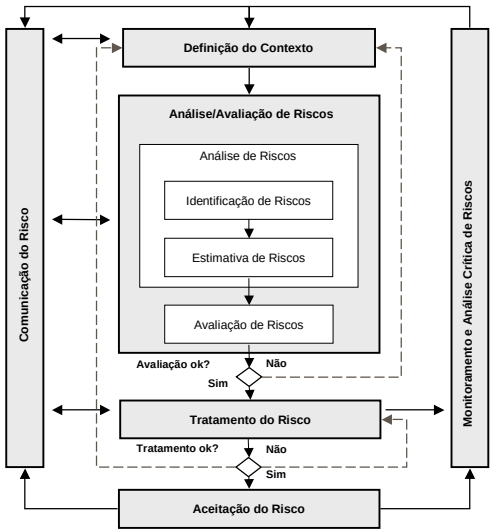
5

Gestão de Riscos

- É um elemento central na gestão da estratégia.
- Deve ser um processo contínuo e em constante desenvolvimento aplicado à estratégia da organização e à implementação desta estratégia.

6

Processo de Gestão de Riscos – ISO 27005



7

Modelos de Maturidade

- Atuam como referência para a obtenção de níveis adequados de qualidade nos bens e serviços produzidos.
- Possibilitam uma linguagem comum.
- Padronizam os bens e serviços.

✓ Considera-se que uma empresa atingiu sua maturidade quando os seus processos são explicitamente definidos, gerenciados, medidos, controlados e eficazes.

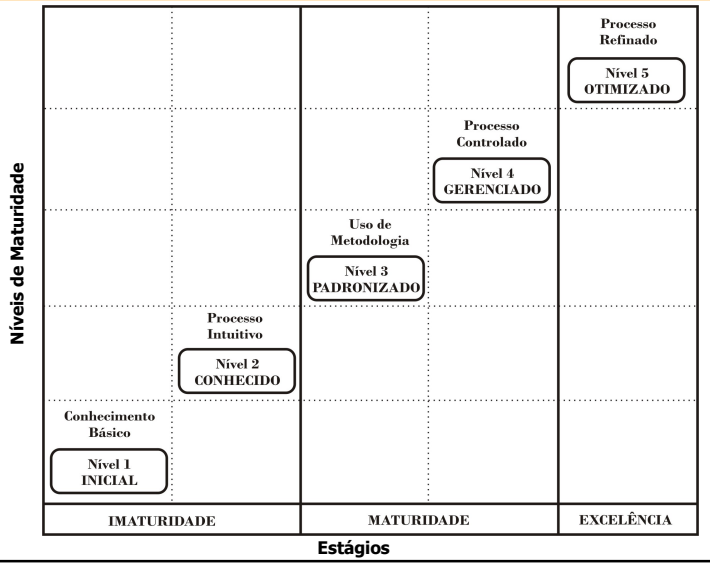
8

Proposta do Modelo de MMGRSI

- É apresentada a proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação.
- O modelo é constituído por um conjunto de boas práticas que oferece uma estrutura formal para o desenvolvimento da gestão de riscos de segurança da informação.
- O modelo é norteado por três estágios:
  - **Imaturidade:** os processos são improvisados.
  - **Maturidade**: a organização já tem seus processos definidos, padronizados e controlados.
  - **Excelência:** a organização consegue otimizar seus processos.

9

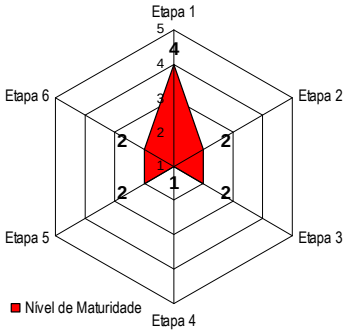
Modelo de Maturidade de Gestão de Riscos em SI



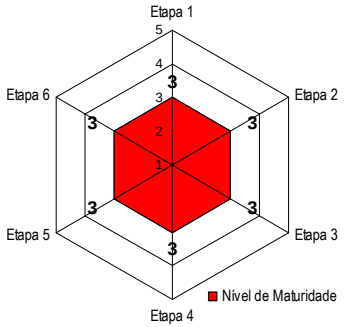
10

Modelo de Maturidade de Gestão de Riscos em SI

- Cada etapa da Gestão de Riscos será avaliada e classificada em um nível de maturidade, segundo o modelo proposto.



(a)



(b)

Considerações Finais

- Os resultados da avaliação da maturidade do processo de gestão de riscos em Segurança da Informação fornecerão informações valiosas que podem ajudar a organização a planejar, executar e monitorar suas iniciativas de melhoria e gerenciamento de seus processos de negócios, bem como orientar os processos de tomada de decisão.

- Ainda é necessário:
  - revisar e ampliar a descrição formal do Modelo;
  - concluir a elaboração de um instrumento de auditoria e avaliação dos níveis de maturidade;
  - esse instrumento será repassado a algumas instituições já definidas e os dados serão analisados.

Trabalhos Futuros

- Após a conclusão, acredita-se que sejam trabalhos futuros pertinentes:

  (a) ampliar o número de estudos de caso com o objetivo de identificar necessidades de ajustes no modelo de maturidade,

  (b) aprimorar os instrumentos de avaliação e

  (c) desenvolver uma ferramenta de apoio ao processo de avaliação e monitoramento dos níveis de maturidade.

13

Referências

- ABNT – Associação Brasileira de Normas Técnicas (2005) "**Norma NBR ISO/IEC 27001** - *Information Security Management Systems-Requirements*", Rio de Janeiro.
- ABNT – Associação Brasileira de Normas Técnicas (2005a) "**Norma NBR ISO/IEC Guia 73**: Gestão de Riscos – Vocabulário –Recomendação para uso em normas", Rio de Janeiro.
- ABNT – Associação Brasileira de Normas Técnicas (2008) "**Norma NBR ISO/IEC 27005**: Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação", Rio de Janeiro.
- Chrissis, M. B., Konrad, M. e Shrum, S. (2005) "**CMMI®** - *Guidelines for Process Integration and Product Improvement*", Estados Unidos.
- ISO – *International Organization for Standardization* (2008) "**Norma ISO/DIS 31000**: *Risk management – Principles and guidelines on implementation*", Suiça.

14

UNISINOS

Muito Obrigada!

15