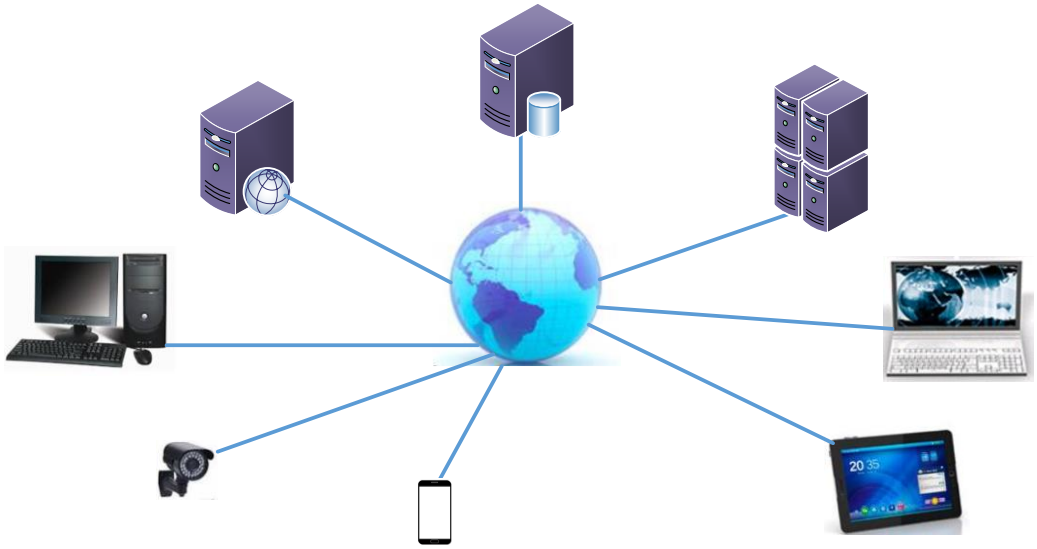
GESTÃO DE RISCOS DA SEGURANÇA DA INFORMAÇÃO



Prof. Dr. Márcio Andrey Teixeira
Instituto Federal de São Paulo – Campus Catanduva
Catanduva, SP
Membro Sênior do IEEE
marcio.andrey@ifsp.edu.br

CONTEÚDO

- REVISÃO – ABNT NBR ISO/IEC 27002:2013
- FUNDAMENTOS DE GESTÃO DE RISCOS
- ABNT NBR ISO/IEC 27005:2011
- PROCESSO DE GESTÃO DE RISCOS
- CONCLUSÃO
- REFERÊNCIAS BIBLIOGRÁFICAS
- SIGLAS:
  - *ABNT = ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS*
  - *NBR = NORMAS BRASILEIRAS*
  - *ISO = INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO)*
  - *IEC = INTERNATIONAL ELECTROTECHNICAL COMMISSION (COMISSÃO ELETROTÊCNICA INTERNACIONAL)*

REVISÃO – ABNT NBR ISO/IEC 27002:2013

- Uma família de normas
  - Voltadas para gestão e operação da Segurança da Informação;
  - Amadurecimento da área;
  - Imposição de novos desafios.

- Padrões, Leis e Boas Práticas
  - De fundamental importância por uma questão de conformidade e também um ponto de apoio para implementação das normas.

REVISÃO – ABNT NBR ISO/IEC 27002:2013

- TESTE DE CONFORMIDADE (ISO 27002)
  - Este instrumento vai auxiliá-lo a perceber o grau de aderência de sua empresa em relação às recomendações de segurança da informação da ISO 27002.
  - Pela superficialidade natural desse tipo de teste, o mesmo é comumente referenciado como ISO 27002 *Gap Analysis Light*, ou seja, um diagnóstico simples e rápido, baseado em perguntas objetivas com pontuação associada que vai revelar seu índice de aderência.

- Objetivos do teste
  - Permitir a percepção quanto ao grau de aderência da organização aos controles sugeridos pela norma ISO 27002.

REVISÃO – ABNT NBR ISO/IEC 27002:2013

- Índices de conformidade com a norma ISO 27002
  - São 59 questões do teste;
  - Existe um amplitude dos assuntos abordados pela norma;
  - Grande complexidade em planejar, implementar e gerir todos os controles de segurança;
  - Proteger: **Confidencialidade**, **Integridade** e **Disponibilidade**.

  - *Classificação dê acordo com os resultados adquiridos pelo teste:*

Resultado entre: 78-118 → Parabéns!

Resultado entre: 39-77 → Atenção!

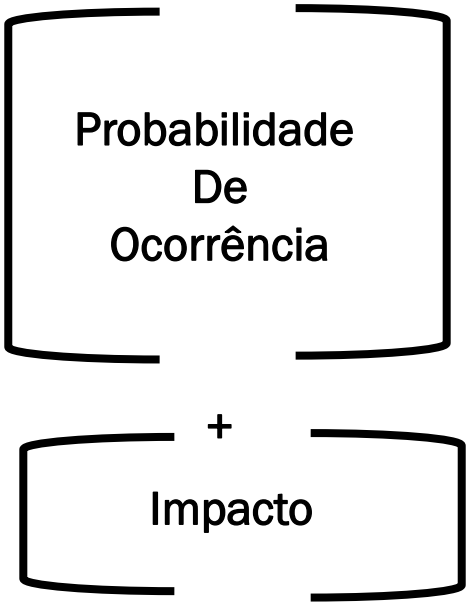
Resultado entre: 0-38 → Cuidado!

OBJETIVOS

- Apresentar o processo de Gestão de Riscos de Segurança da Informação;
- Debater sobre a implementação (prática) do processo de gestão de riscos, com ênfase para as atividades de Análise, Avaliação e Tratamento de Riscos;

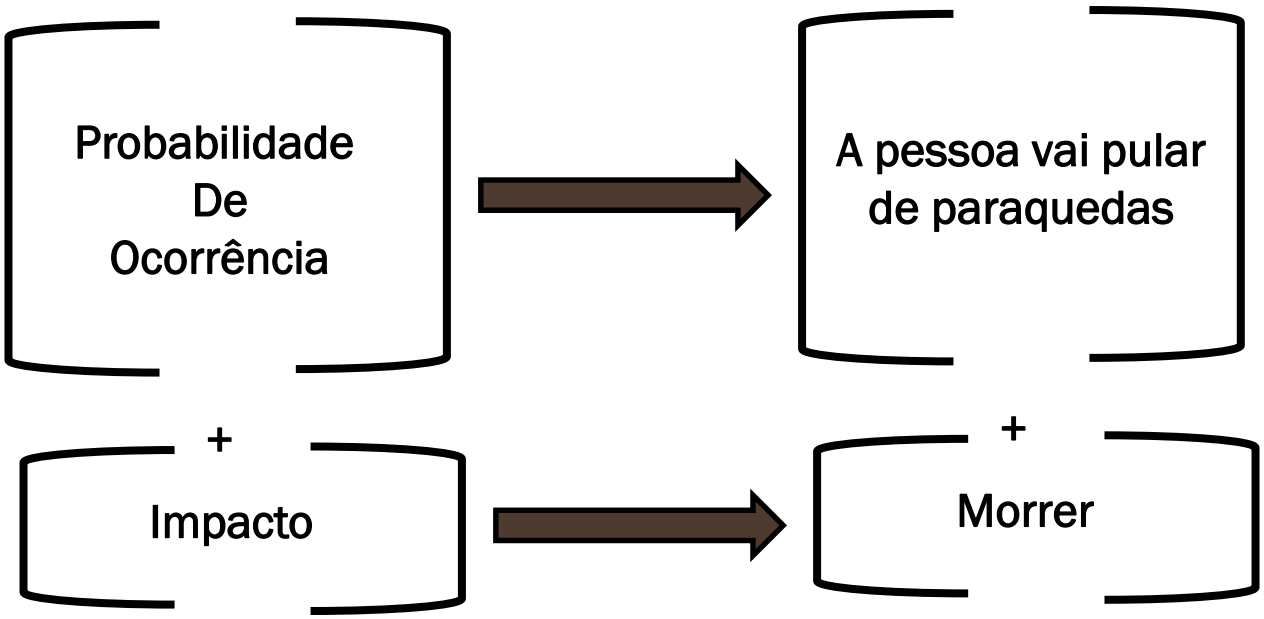
RISCO

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



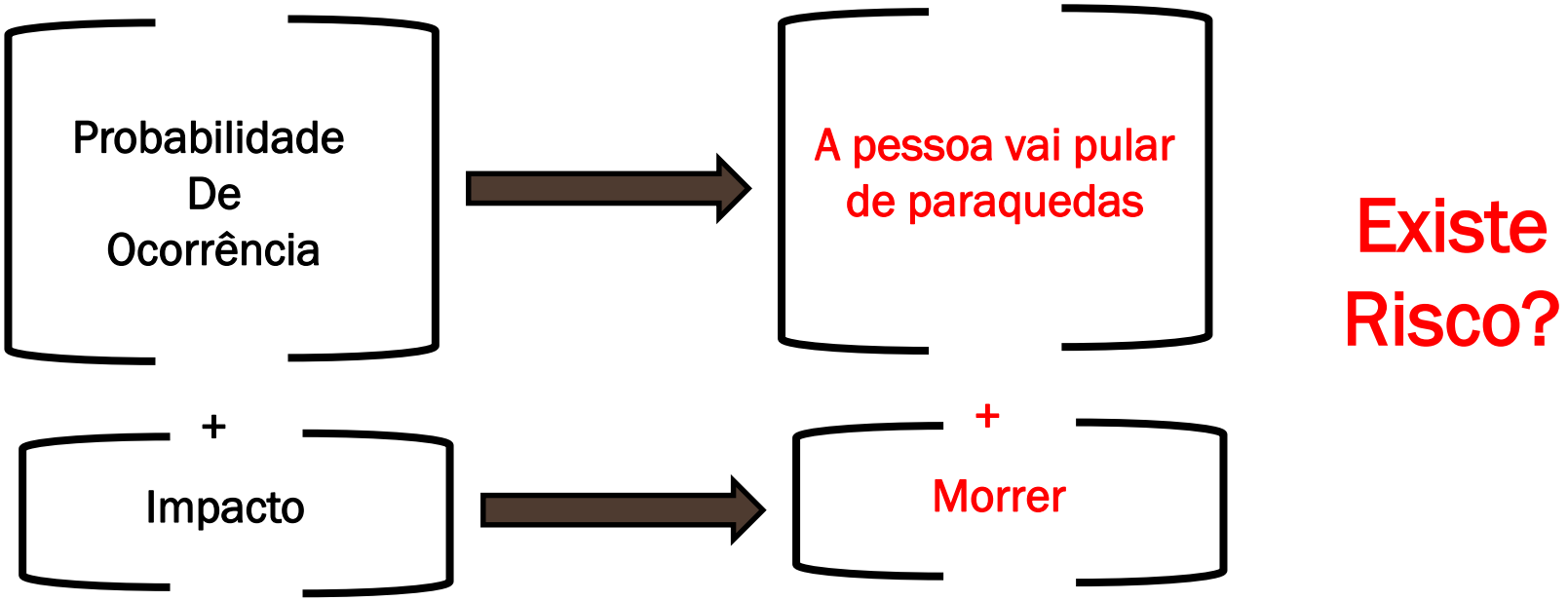
RISCO

Exemplo:



RISCO

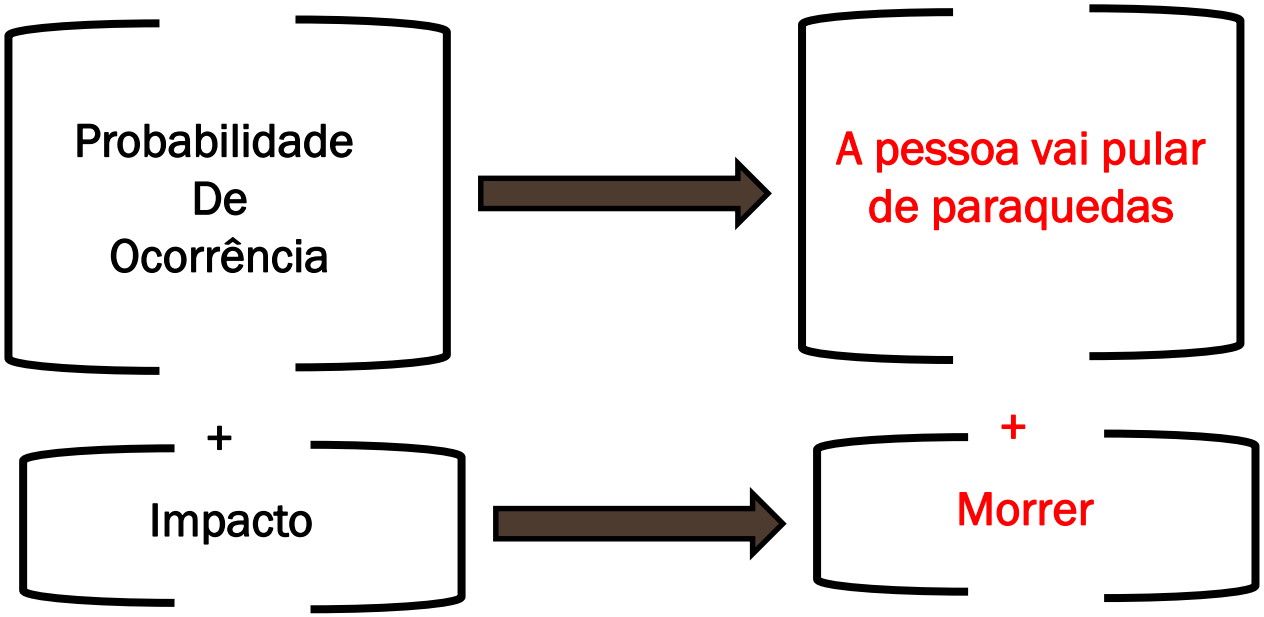
Exemplo:



Existe Risco?

RISCO

Exemplo:



Sim, pois alguma vez o paraquedas não abriu.

RISCO

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

RISCO

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

RISCO

- Gestão de risco

Probabilidade De Ocorrência + Impacto

Como evitar, minimizar ou até eliminar os impactos desse risco.

RISCO

- Ao descrever os riscos estamos detalhando cenários, cujas consequências afetam a “vida” de determinados ativos.

RISCO

- Exemplo de um Evento de Riscos

Ativo: estação de trabalho

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

INTRODUÇÃO: A ABNT NBR ISO/IEC 27005:2011

- **Objetivo:** fornecer diretrizes para o processo de gestão de riscos de SI de uma organização.
- Direciona-se particularmente aos requisitos de um **sistema de gestão de segurança da informação** (SGSI).
- **É a organização que define sua conduta ao processo de gestão de riscos,** atribuindo em conta, o modelo do seu SGSI, contexto da gestão de riscos e o seu ramo de atividade econômica.

INTRODUÇÃO: A ABNT NBR ISO/IEC 27005:2011

- Convém que seja sempre integrante das atividades de gestão de si e que seja aplicada tanto à implementação quanto à operação cotidiana de um SGSI.

- **Seja um processo contínuo.**

- Este processo define os contextos interno e externo, avalie os riscos e trate os riscos usando um plano de tratamento a fim de implementar as recomendações e decisões.

- Analise os possíveis acontecimentos e suas consequências, antes de decidir o que será feito e quando será feito. Assim reduzindo os riscos a um nível aceitável.

CONTRIBUIÇÕES: ABNT NBR ISO/IEC 27005:2011

- A identificação de riscos.
- O processo de avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência.
- A comunicação e entendimento da probabilidade e das consequências destes riscos.
- O estabelecimento da ordem prioritária para tratamento do risco.
- A priorização das ações para reduzir a ocorrência dos riscos.

SEÇÃO 6: PROCESSO DE GESTÃO DE RISCOS

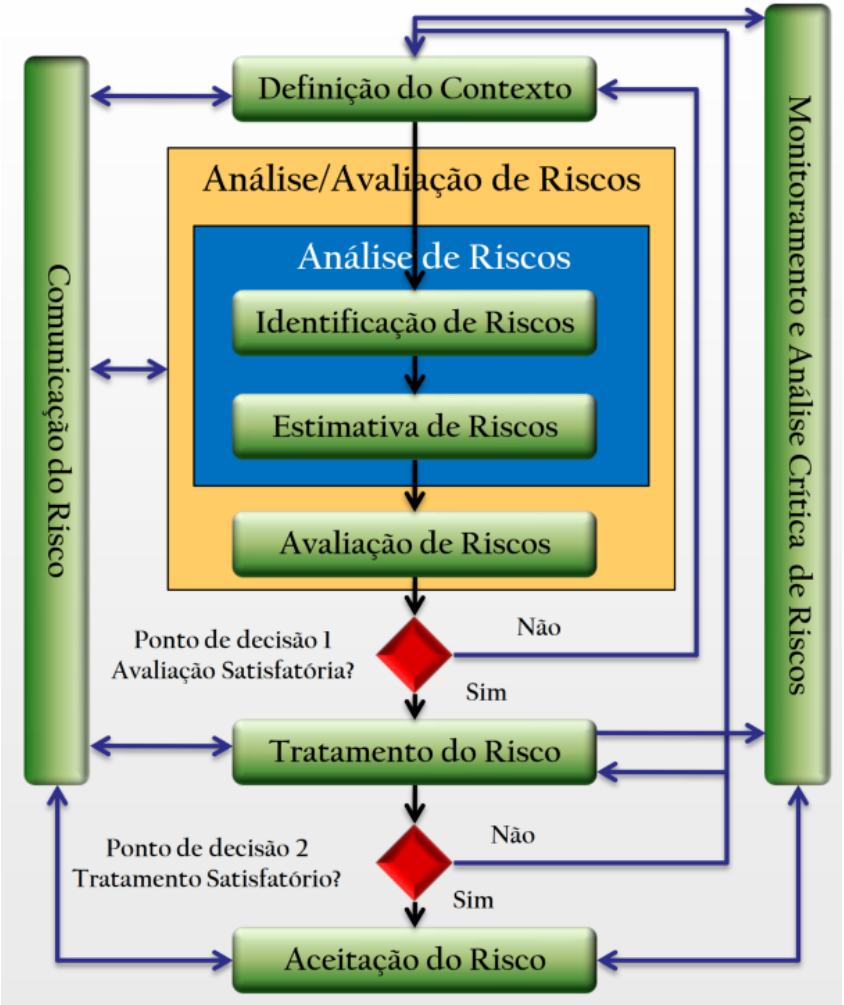
Alinhamento do processo de SGSI com o processo de gestão de riscos de SI

PROCESSO DO SGSI	PROCESSO DE GR DE SI
Planejar	Definição do Contexto Processo de avaliação de riscos Definição do 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 Gestão de Riscos de Segurança da Informação

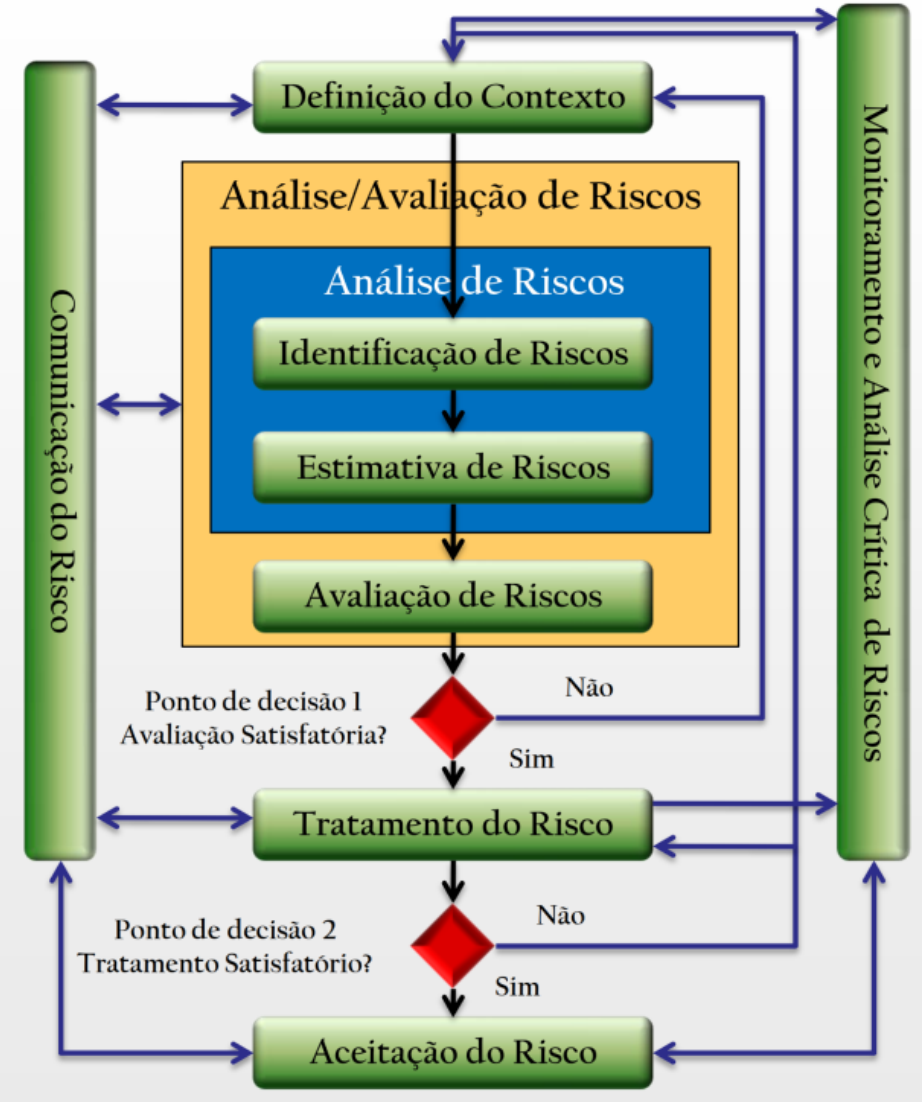
SEÇÃO 6: PROCESSO DE GESTÃO DE RISCOS

- 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.

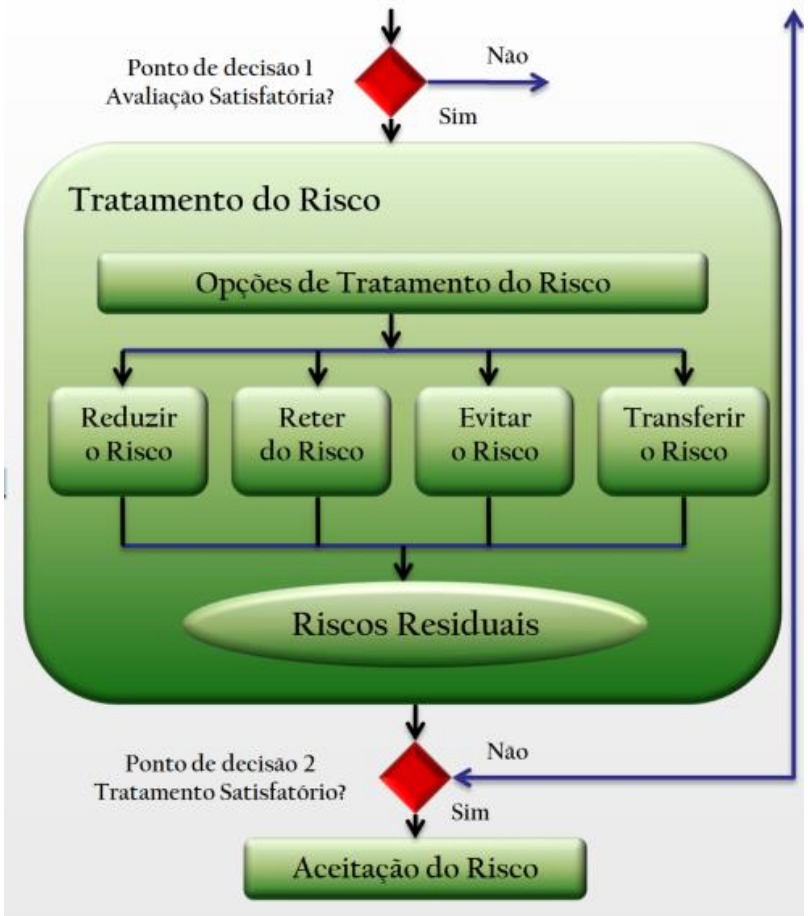


SEÇÃO 6: PROCESSO DE GESTÃO DE RISCOS



Tratamento do risco dentro do processo de gestão de riscos de SI.

Para tratar o risco deve-se basear no resultado do processo de avaliação de riscos, custo esperado para implementar essas opções e nos benefícios previstos.



PROCESSO DE GESTÃO DE RISCOS

O contexto para Gestão de Riscos (GR) de Segurança da Informação (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.

TRATAMENTO DO RISCO DE SEGURANÇA DA INFORMAÇÃO

Aceitação dos Riscos

Convém que a ***decisão de aceitar os riscos*** seja tomada e formalmente registrada, juntamente com a responsabilidade pela decisão.

A política de gestão de riscos (item critérios para a aceitação do risco) oferece suporte a essa tomada de decisão.

Comunicação dos Riscos

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***.

TRATAMENTO DO RISCO DE SEGURANÇA DA INFORMAÇÃO

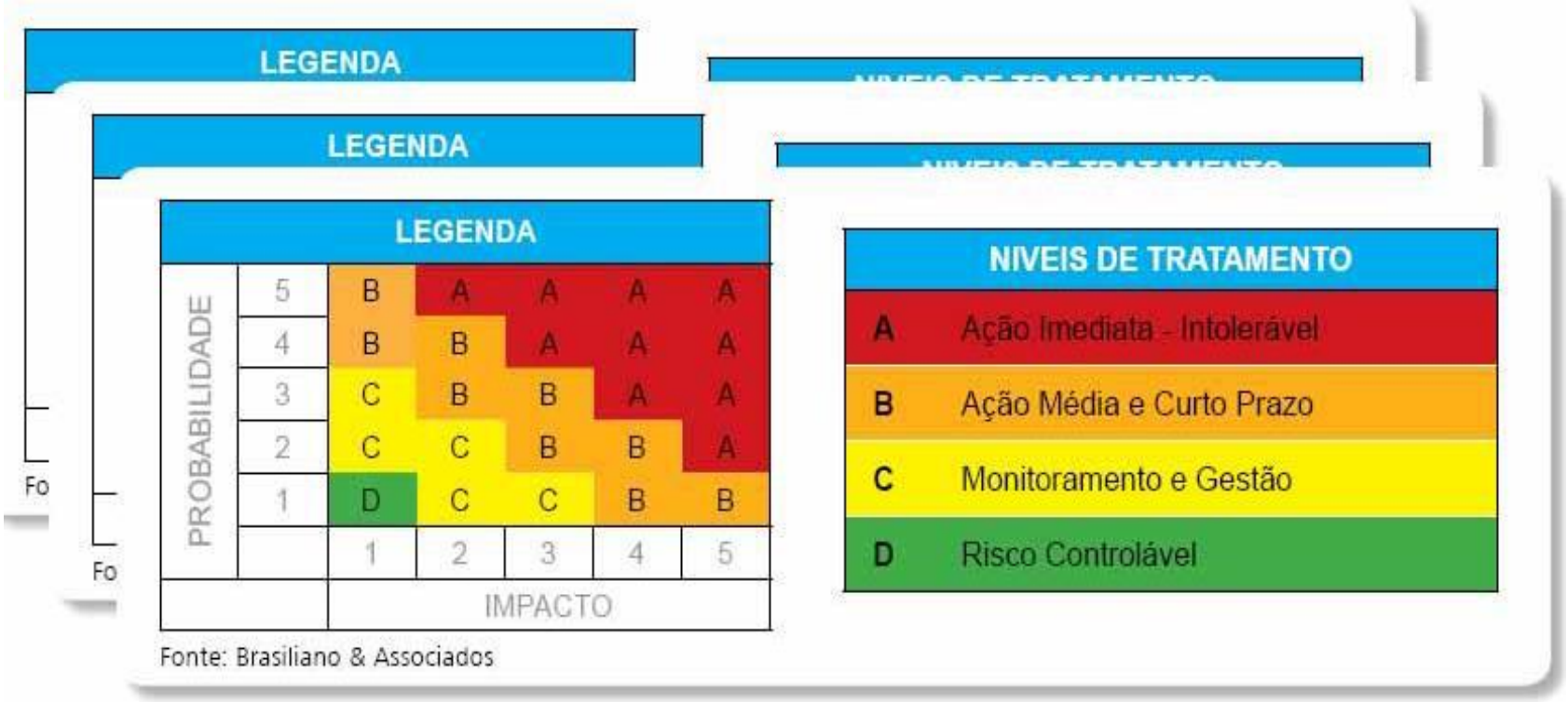
Monitoramento dos Riscos

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.

Risco Residual

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

TRATAMENTO DO RISCO DE SEGURANÇA DA INFORMAÇÃO



A ABNT NBR ISO/IEC 27005:2011

TERMOS E DEFINIÇÕES:

- **consequência:** resultado de um evento que afeta os objetivos
- **controle:** medida que está modificando o **risco**
- **evento:** ocorrência ou mudança em um conjunto específico de circunstâncias
- **contexto externo:** ambiente externo no qual a organização busca atingir seus objetivos (cultural, social, político, econômico, etc)
- **contexto interno:** ambiente interno no qual a organização busca atingir seus objetivos (governança, estrutura organizacional, funções e responsabilidades pessoas, si, cultura da organização, etc)
- **nível de risco:** magnitude de um **risco**, expressa em termos da combinação das **consequências** e de suas **probabilidades**.

A ABNT NBR ISO/IEC 27005:2011

- **probabilidade:** chance de algo acontecer
- **risco residual – risco:** remanescente após o **tratamento do risco**
- **risco:** efeito da incerteza nos objetivos
- **análise de riscos:** processo de compreender a natureza do risco e determinar o nível de risco
- **processo de avaliação de riscos:** processo global de identificação de riscos, análise de riscos e avaliação de riscos
- **comunicação e consulta:** processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar e obter informações, e se envolver no diálogo com as **partes interessadas**, com relação a gerenciar **riscos**.

CONSIDERAÇÕES FINAIS

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.**

- No escopo da nossa disciplina, irá fornecer informações para o levantamento de dados anterior a etapa de desenvolvimento da Política de Segurança da Informação.

EXERCÍCIOS: ISO/IEC 27005:2011

Exercícios com base na norma ABNT NBR ISO/IEC 27005:2011

1 – Defina o que é Gestão de Riscos?

2 – No capítulo "3 – Termos e definições", cite todos os termos juntamente com as suas definições e, quando houverem notas, cite ao menos uma.

3 – Como a norma está organizada?

4 – Considerando a seção "6 – Visão geral do processo de GR de SI" cite, resumidamente, as etapas do processo de gestão de riscos dê acordo com as figuras 1 e 2.

5 – Na seção "8 – Processo de avaliação de riscos de SI", é descrito as atividades para executá-lo. Quais são estas atividades?

6 – As seções 8.2.3 e 8.2.5 orienta e ajuda a identificar os tipos de ameaças e vulnerabilidades. Sendo assim, existe algum anexo, juntamente à norma, que demonstra quais são as possíveis ameaças e vulnerabilidades? Caso exista, cite-os e escolha 5 tipos de ameaças e vulnerabilidades existentes.

7 – Considerando a seção "9 – Tratamento do risco de SI" mostre quais são as opções existentes, para o tratamento do risco?

8 – Defina os processos de: Aceitação, Comunicação e consulta do risco de SI. Estudem as seções 10 e 11.

9 – Porque é importante monitorar os riscos?

10 – Para conhecermos melhor o funcionamento de uma organização (estrutura, limitações, valorização e identificação dos ativos), na implantação do processo de Gestão de Risco de SI, quais anexos podem nos auxiliar?

EXERCÍCIOS: TEXTO COMPLEMENTAR

Ler o texto complementar: Norma de Gestão de Riscos e responda:

1 – O que é Risco?

2 – Como você caracteriza e entende sobre a Gestão de Riscos (GR)?

3 – Cite exemplos de fatores: Internos e Externos.

4 – Considerando o processo da Análise de Riscos mostre quais são os procedimentos para a realização desta análise:

5 – De acordo com o item *4.3 Estimativa dos riscos*, referente ao processo de Análise de Riscos, quais são os termos utilizados para classificar o grau de *probabilidade* e *consequências*?

6 – O que é Tratamento de Riscos?

7 – O que você entende por *Financiamento de Riscos?*

8 – No processo de 8.Estrutura e administração da gestão de riscos, no sub-ítem 8.4 Papel da Função gestão de riscos, cite 4 processos importantes.

9 – Mostre algumas funções da auditoria interna.

10 – Explique, de acordo com sua compreensão, o termo: "É preciso não esquecer que as organizações são dinâmicas e funcionam em ambientes dinâmicos".

REFERÊNCIAS BIBLIOGRÁFICAS

- ABNT NBR ISO/IEC 27005:2011. **Gestão de Riscos da Segurança da Informação.**
- ABNT NBR ISO/IEC 27002:2013. **Código de Prática para a Gestão da Segurança da Informação.**
- Sêmola, Marcos. **Gestão da Segurança da Informação: Uma Visão Executiva. Rio de Janeiro, Ed. Campus, 2014.**
- Centro de Estudos, Respostas e Tratamento de Incidentes. CERT.Br - http://www.cert.br/