POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Rogério Nunes de Freitas

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Política : texto de alto nível, que dá direcionamento geral e significado aos objetivos e intenções da administração quanto à segurança da informação.

Padrões : Conjunto de medidas necessárias para estabelecer o controle.

Procedimentos : descrição passo-a-passo sobre como atingir os resultados

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Para que servem:

- estão relacionados ao uso da informação em uma organização.
- fornecem direcionamento para implementações técnicas
- formam um conjunto de ações que compõem a Gestão da Segurança

Importância da Informação

- Qual a utilidade da Informação ?
  - Lembrar dos fins: suporte, estratégia, ...
- Qual o valor da Informação ?
  - Avaliação pessoal do dono da informação
- Qual a validade da Informação ?
  - Deve possuir um período de validade
- Quem é o responsável pela manutenção da classificação da informação ?
  - O criador é responsável pela classificação inicial.

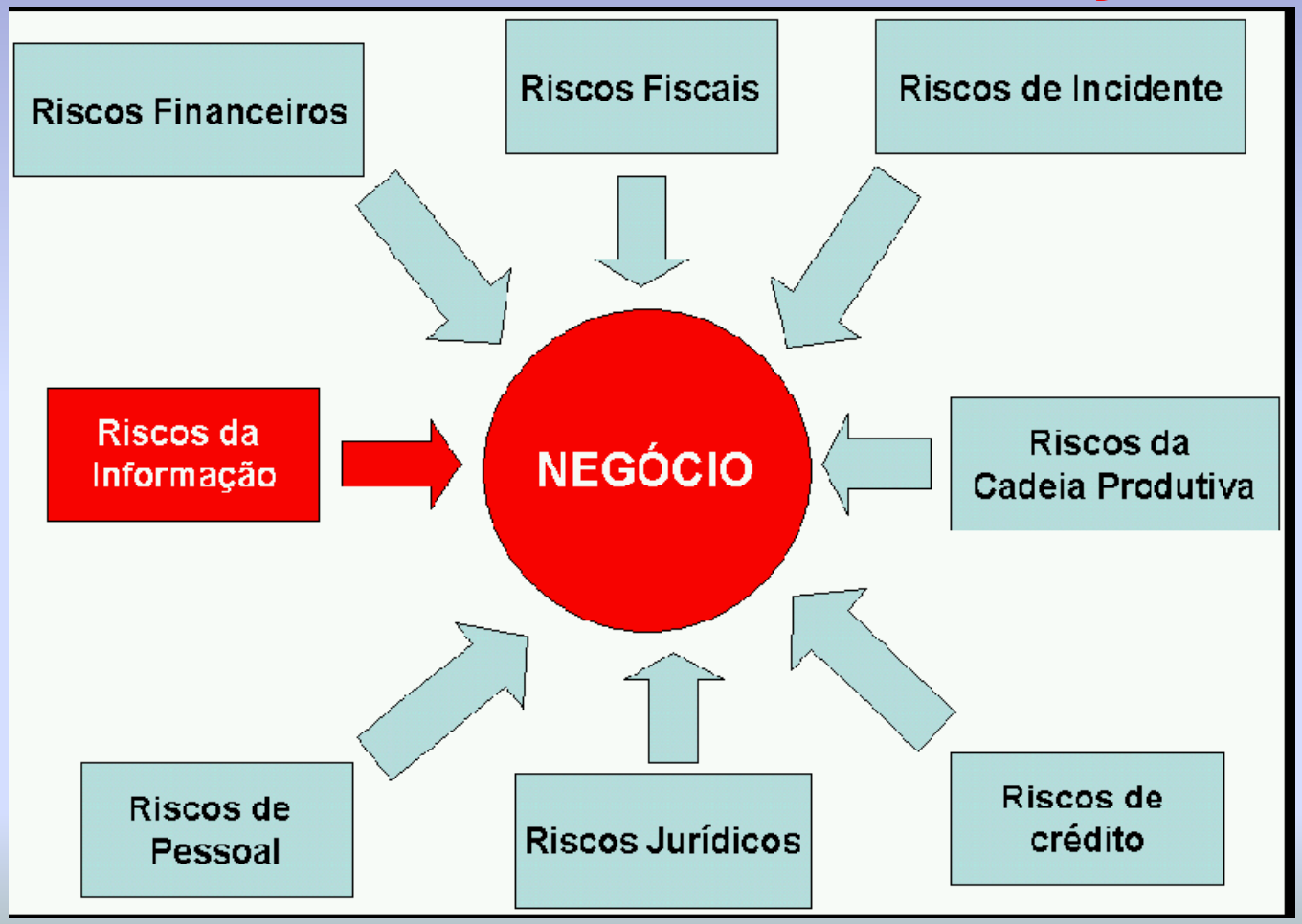
Importância da Informação

- Vale a pena proteger tudo?
  - Segurança requer investimentos
  - Pode-se utilizar o ROI - *Return on Investment*
    - Não existe um modelo unificado
  - Conhecimento do Negócio
    - Este é o ponto chave de qualquer gerenciamento de riscos

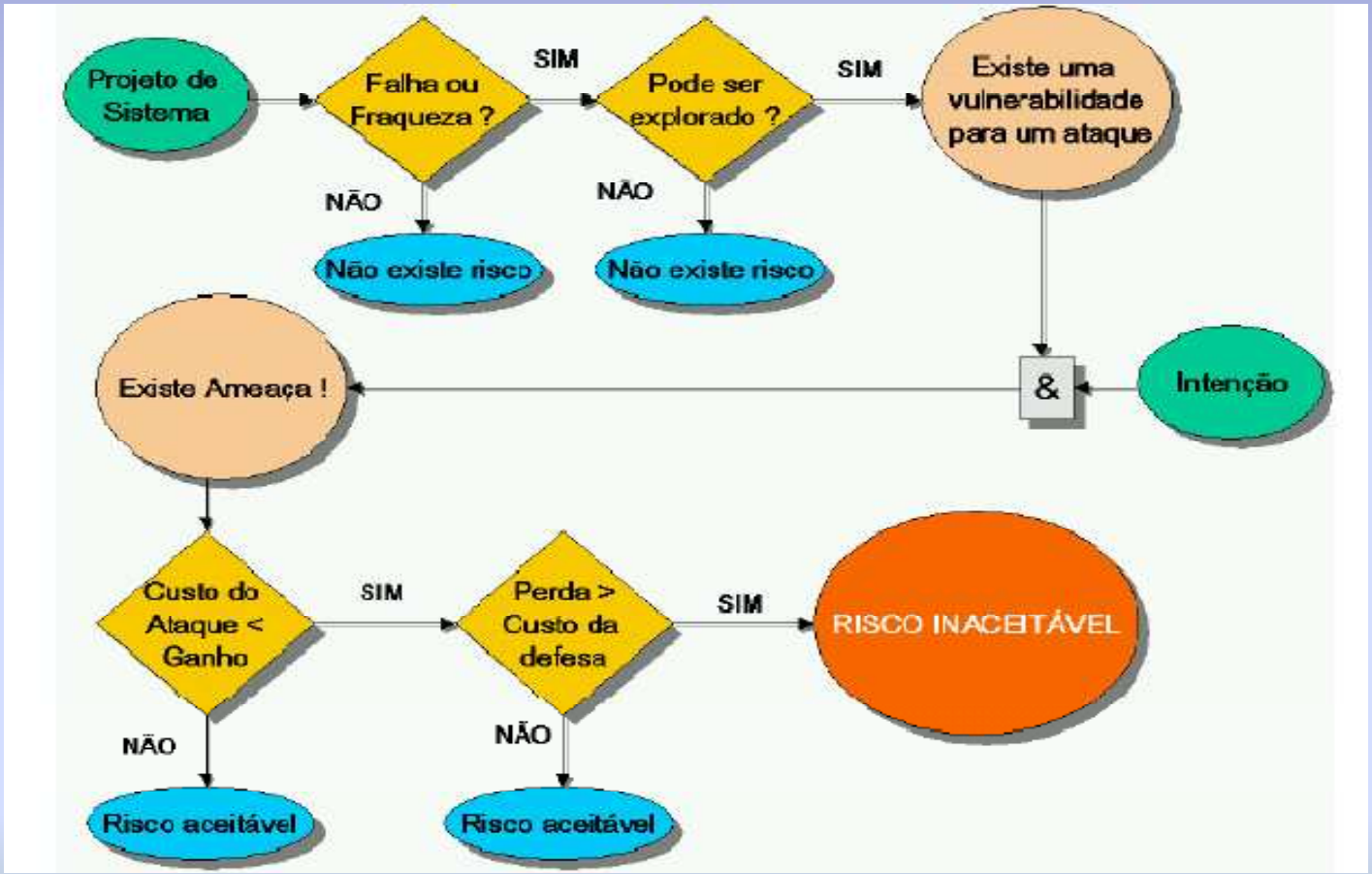
Classificação da Informação

- Classificar todas as informações críticas segundo o seu grau de teor crítico:
  - Informações Confidenciais: Devem ser disseminadas somente para empregados nomeados;
  - Informações Corporativas: Devem ser disseminadas somente dentro da Empresa;
  - Informações Públicas: Podem ser disseminadas dentro e fora da Empresa

Classificação e controle dos ativos de informação



Roteiro para identificar riscos



POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Informação = um ativo institucional, tudo o que representa valor para o negócio da instituição

A política de informação é elaborada a partir;

a) **Classificação dos ativos**

b) conscientização e treinamento

c) desenvolvimento da política

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

A classificação leva em consideração

- a) o valor, o risco e o uso da informação
- b) diferença no uso dos mecanismo de proteção e processos de recuperação
- c) custo e ajuda na tomada de decisão institucional

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Benefícios da Classificação

- a) manutenção da confidencialidade, integridade e disponibilidade da informação
- b) melhor direcionamento dos investimentos em recursos físicos e lógicos

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Questões importantes para a classificação:

- a) quem é responsável formal pelo projeto?
- b) O que se deseja proteger, e do que/quem?
- c) existem políticas ou leis corporativas a serem respeitadas?
- d)na organização, existe proprietários para a informação?
- e) os recursos estão disponíveis?

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

É importante a elaboração de uma política de informação que contenha:

- a) definição da informação como ativo de negócio
- b) declaração que a direção institucional é proprietária da informação
- c) identificação dos custodiantes
- d) definição de metas

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Análise de impacto

1) fator crítico de sucesso é o comprometimento da alta direção

2) a análise de impacto deve ser feita por uma equipe muldisciplinar

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

A análise de impacto nos negócios, deve contemplar:

- identificação das maiores e principais áreas funcionais da organização
- análise das ameaças associadas a cada área funcional identificada;
- determinação do risco associado a uma ameaça
- determinação da consequência que a perda de um ativo de informação pode trazer aos negócios
- construção de uma matriz detalhando o impacto nos negócios
- preparo de uma relação de recursos e de aplicações que suportam as funções do negócio

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Determinação da classificação

- indica a classificação e os controles de segurança adequados
- deve ser de fácil compreensão e claramente descrita
- devem ser adotadas por todos

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Determinação

- a) Pública/informação não classificada
- b) informação interna
- c) informação confidencial
- e) informação secreta

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Responsabilidades

- a) proprietário da informação = executivo ou gerente
- b) custodiante = pessoa de TI
- c)proprietário de aplicação = gerente de unidade
- d) gerente do usuário = superior imediato de um funcionário que terá acesso a informação

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

- E) administrador de rede
- f) analista de segurança
- g) analista de controle de mudança
- h) analista de dados
- i) usuário final

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Proprietários da informação

Critérios para identificação:

- a) deve ser pessoa de negócio
- b) o suporte dos altos executivos é essencial
- c) deve ser considerada a participação de mais de um executivo

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Critérios auxiliares ao processo de classificação da informação pelos proprietários:

- a) informações para auditoria (custo, onde se encontra etc)
- b) segregação de funções necessárias
- c) serão usados métodos criptográficos?
- D) como é realizado o controle de acesso?
- e) os procedimentos e controle são documentados?
- f) onde é armazenada a documentação

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Treinamento e conscientização

- Fases
- a) identificação do escopo, metas e objetivos
- b) identificação de instrutores
- c) identificação de público alvo
- d) motivação dos funcionários e da alta administração
- e)administração do programa
- f)continuidade do programa
- g) avaliação do programa

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Desenvolvimento de política

- **Tipos de políticas**
- a) regulatória = descreve com grande detalhe o que deve ser feito; geralmente não é distribuída fora da organização
  - vantagens: assegura o cumprimento dos procedimentos, normas e padrões
  - proporciona conforto à organização na execução de suas atividades
- b) consultiva = sugere a realização de ações/atividades cotidianas da organização. Oferece conhecimentos básicos
  - desvantagens: aumento da possibilidade de omissão de informação importante; falhas no processo de comunicação com a alta administração; perda de prazos em compromissos importante
- c) informativa = possui carater apenas informativo

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Desenvolvimento de política

- Fatores comuns entre as políticas

a) especificação da política
b) declaração da alta administração
c) autores/patrocinadores
e) referências a outras políticas ou regulamentos
f) procedimentos para requisição de exceções
g) procedimentos para a mudança da política
h) punições para violações
i) data de publicação, validade e revisão

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Técnicas para desenvolver uma política de segurança

- a) linguagem simples, sem termos técnicos ou jargões
- b) tecnicas e métodos para execução de atividades
- c) pessoas para contato
- d) abrangência política
- e) monitoramento e compliance

- Manutenção

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Características

- a) ser verdadeira - exprimir o pensamento da empresa e estar de acordo com as ações
- b) ser complementada com a disponibilidade de recursos
- c) ser válida para todos
- d) ser simples
- e) comprometimento da alta direção

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

- Penalidades da violação da política de segurança
- Estabelecida e aplicada a todos os funcionários, obedecendo as exigências impostas pela cultura organizacional.

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Benefícios

- a) curto prazo
  - formalização e documentação dos procedimentos adotados
  - implementação de novos procedimentos e controles
  - prevenção de acessos não autorizados
  - maior segurança no negócio

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Benefícios

- b) médio prazo
  - padronização dos procedimentos
  - adaptação segura de novos processos de negócios
  - qualificação e quantificação do sistema de resposta a incidentes
  - conformidade com os padrões de segurança

POLÍTICA, PADRÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Benefícios

- c) longo prazo
  - retorno de investimento devido a redução de problemas
  - consolidação da imagem institucional