Gestão de Segurança da Informação

Paulo Silva
Tracker Segurança da Informação

PauloSilva@TrackerTI.com

Roteiro

1. Fundamentos de Segurança da Informação
2. Ativos de Informação
3. Identificação e Avaliação de Ameaças
4. Identificação e Avaliação de Vulnerabilidades
5. Avaliação do Risco

6. Política de Segurança da Informação
7. Plano de Continuidade de Negócio

1. Conceitos Fundamentais de Segurança da Informação

As empresas dependem de seus

Ativos de Informação?

ERP

ENTERPRISE RESOURCE PLANNING

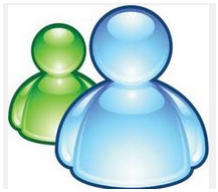
Digitalização de Documentos

GED

BPM

(Business Process Management)

BSC



Cloud

Dependência !?

- Quanto dependemos dos Sistemas de Informação? (caso do ERP sem backup)
- Quanto dependemos dos Projetos Industriais?
- Quanto dependemos de Informações dos Clientes? (caso do representante comercial)

Cenário Atual

- Operação dependendo de Ativos de Informação
- Gestão dependendo de Ativos de Informação
- Informação valendo mais do que ativos físicos
- **Mais Dependência!**

- Sistemas mais distribuídos
- Sistemas mais integrados
- Uso de tecnologias mais complexas
- **Mais Riscos!**

Dependemos das Informações!

mas...

Quais são os riscos?

Riscos Não Intencionais

- Falha de rede, hardware ou software
- Eventos naturais (chuvas, ventos, etc)

- Usuário pouco capacitado
  - (caso do compartilhamento do financeiro)
- Processo mal projetado

- Desconhecimento de questões legais
  - direitos de propriedade intelectual
  - direitos de clientes, fornecedores e colaboradores

Riscos Intencionais

- Mal uso de recursos (ex. facebook)
  - caso do download de filmes fora do expediente
- Sabotagem interna ou externa
  - caso da exclusão de arquivos na rede
- Espionagem interna ou externa
  - caso do roubo e venda de projetos industriais
- Vírus, worms, spams (impactos menores)

Quais são as conseqüências?

- Desperdício de recursos tecnológicos
- Roubo ou Vazamento de informações

- Parada de processos (prejuízo operacional)
- Perda de informações (caso da perda de desenhos de clientes)

- Processos judiciais
- Prejuízos para a imagem da empresa

PERDAS FINANCEIRAS!!!

Pequenas Perdas Financeiras

Incidentes Temporais	Horas/Dia	Dias/Mês	Custo/Hora	Usuários	Custo/Mês
Mal Uso de Recursos	1	1	R$ 15,00	5	R$ 75,00
Spam	1	1	R$ 15,00	5	R$ 75,00
Vírus, Worms e Afins Parada de Estação de Trabalho	1	1	R$ 15,00	5	R$ 75,00
Parada de Servidor Negação de Serviços	1	1	R$ 15,00	15	R$ 225,00
Falha de Hardware Falha de Software Falha da Rede	1	1	R$ 15,00	10	R$ 150,00
Total					R$ 600,00

Muitas empresas não registram seus incidentes!!!

Grandes Perdas Financeiras

Incidentes de prejuízo potencialmente elevado.

Outros Incidentes
Violação direitos autorais software
Violação direitos autorais de audio
Vazamento de informações
Fraudes
Roubo de Hardware
Incidentes ambientais
Falha processo backup
Acesso indevido de informações (espionagem)
Imagem da empresa

E estes riscos realmente acontecem?

Evolução dos ataques

- Antigamente:
  - Alto conhecimento, tempo e persistência

- Atualmente:
  - Popularização das ferramentas de ataque
  - Pouco conhecimento e tempo
  - Basta querer!

Crimes virtuais podem se tornar mais lucrativos do que tráfico de drogas

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Ataques no Brasil

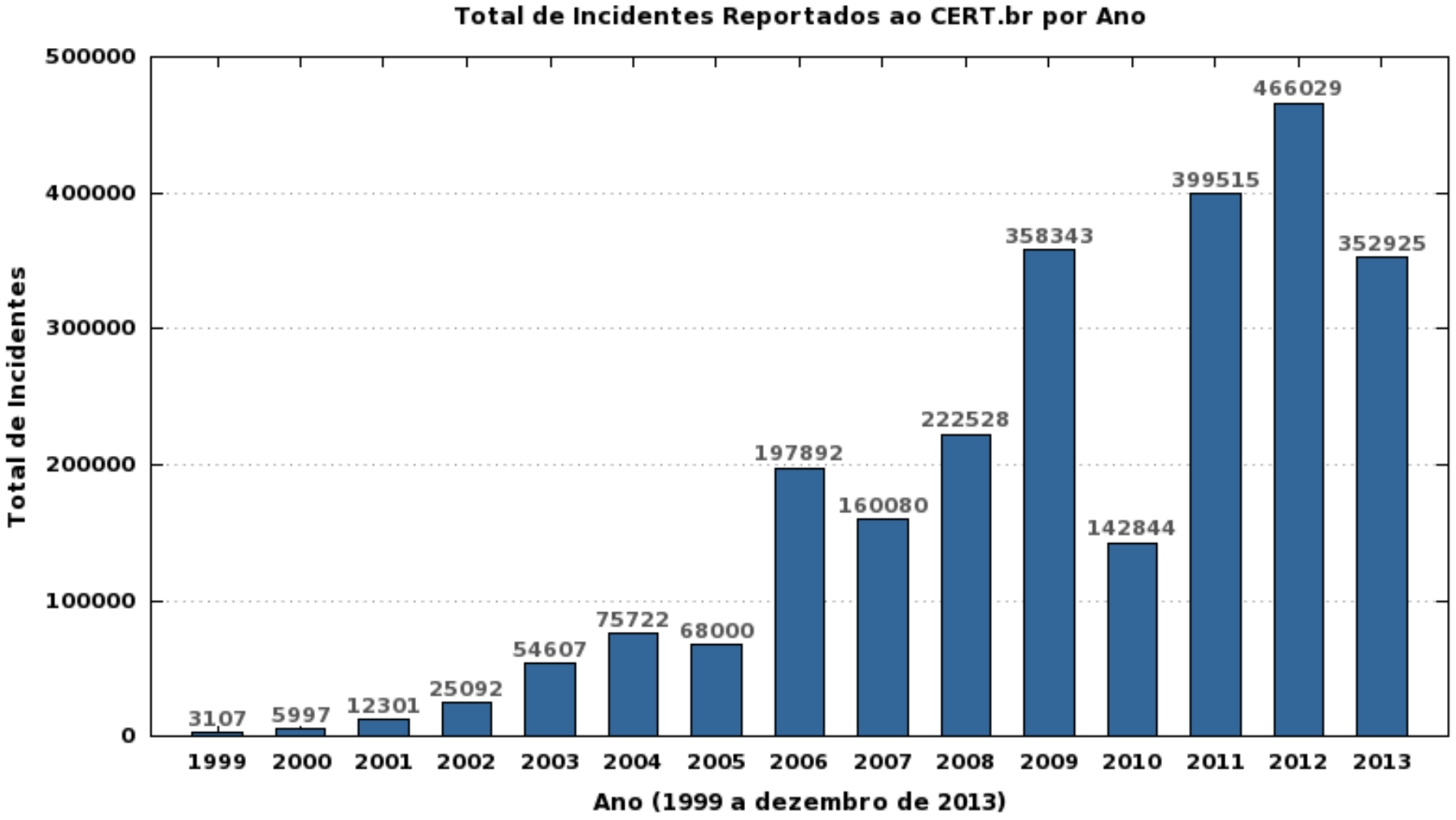
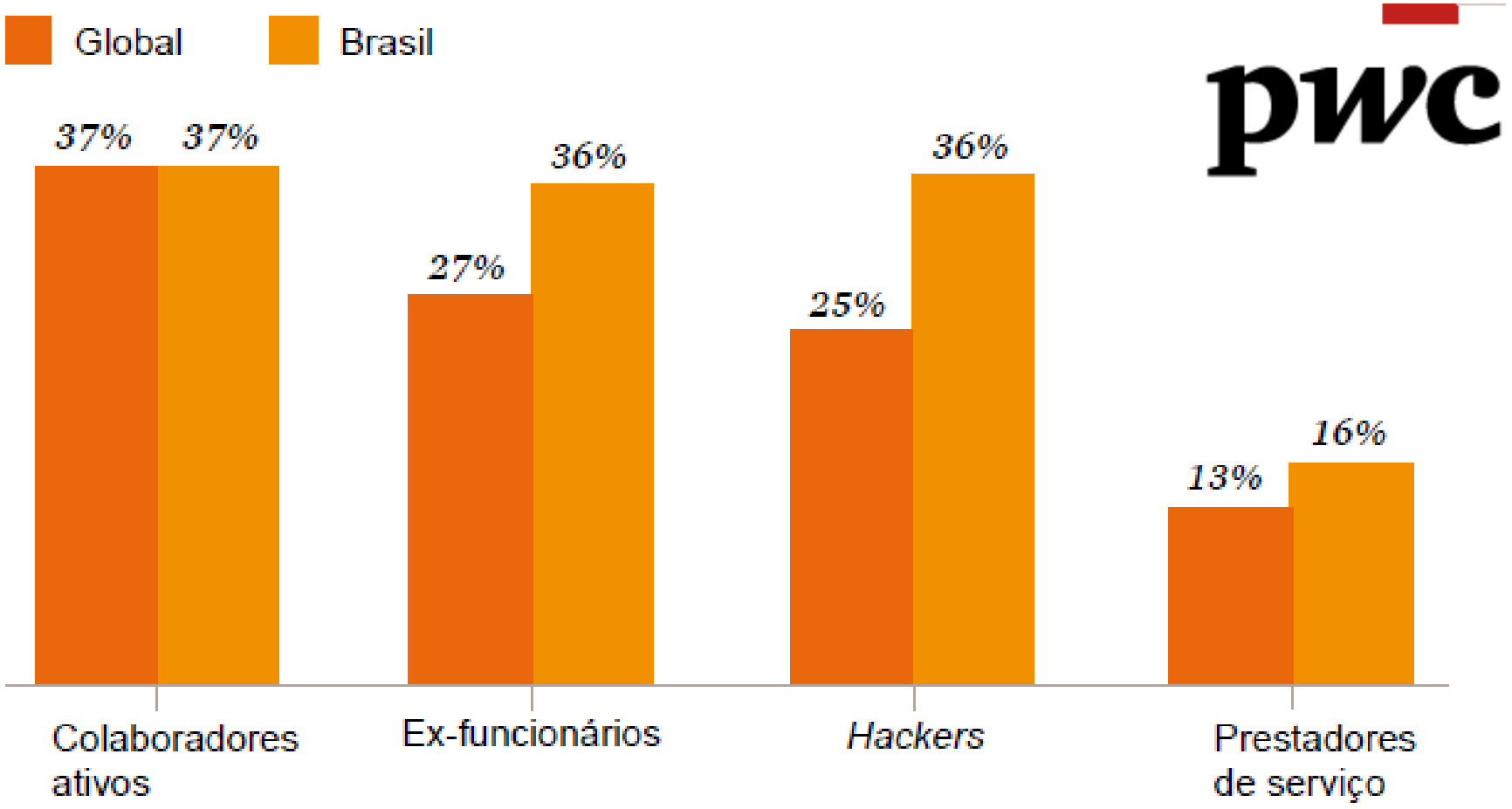


Figura 25: Principais origens dos incidentes de segurança da informação



Problemas Comuns...

- Mal uso de recursos
- Violação da propriedade intelectual

- Compartilhamento de senhas
- Usuários sem consciência dos riscos

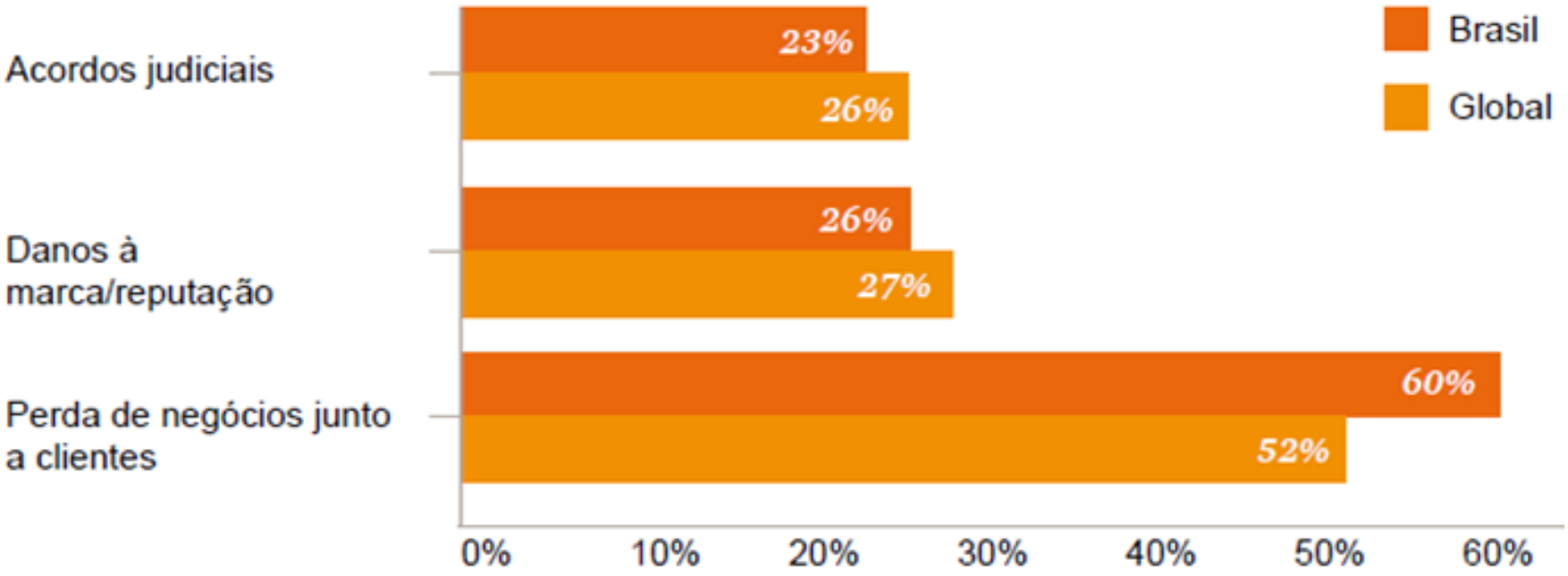
- Sistemas desatualizados
- Ativos importantes desprotegidos

Problemas Comuns...

- Alguns mais específicos:
  - Usuário com direitos de ADMIN
  - O compartilhamento “TEMP”
  - Dispositivos pessoais na empresa
  - Dispositivos pessoais para trabalho
  - O acesso dos terceiros
  - Direitos de acesso na demissão

Consequências $ $ $

Figura 7: Fatores incluídos no cálculo das perdas financeiras decorrentes de falhas de segurança



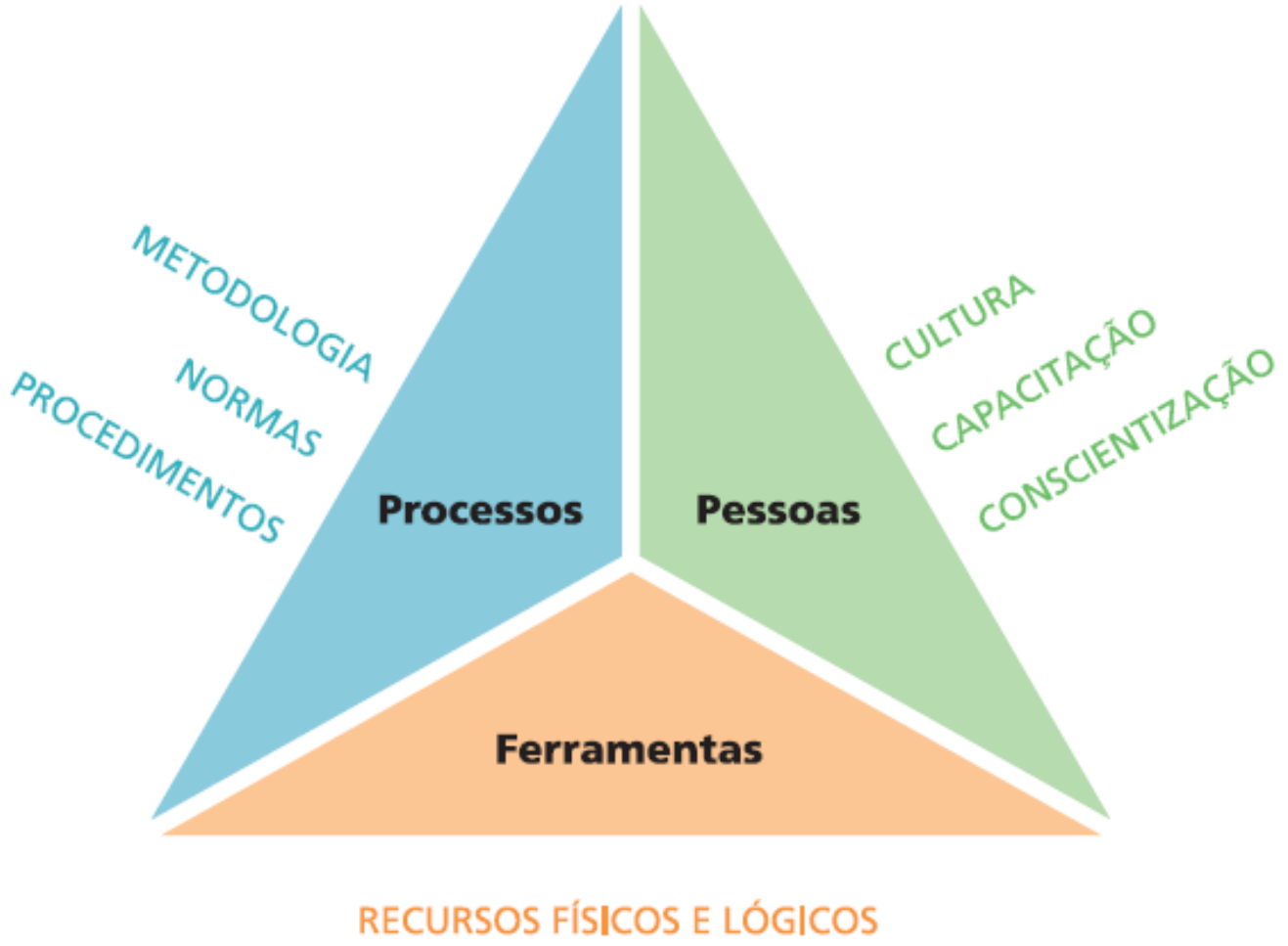
pwc

Incidentes acontecem…

mas...

Como se proteger?

Gestão de Segurança...

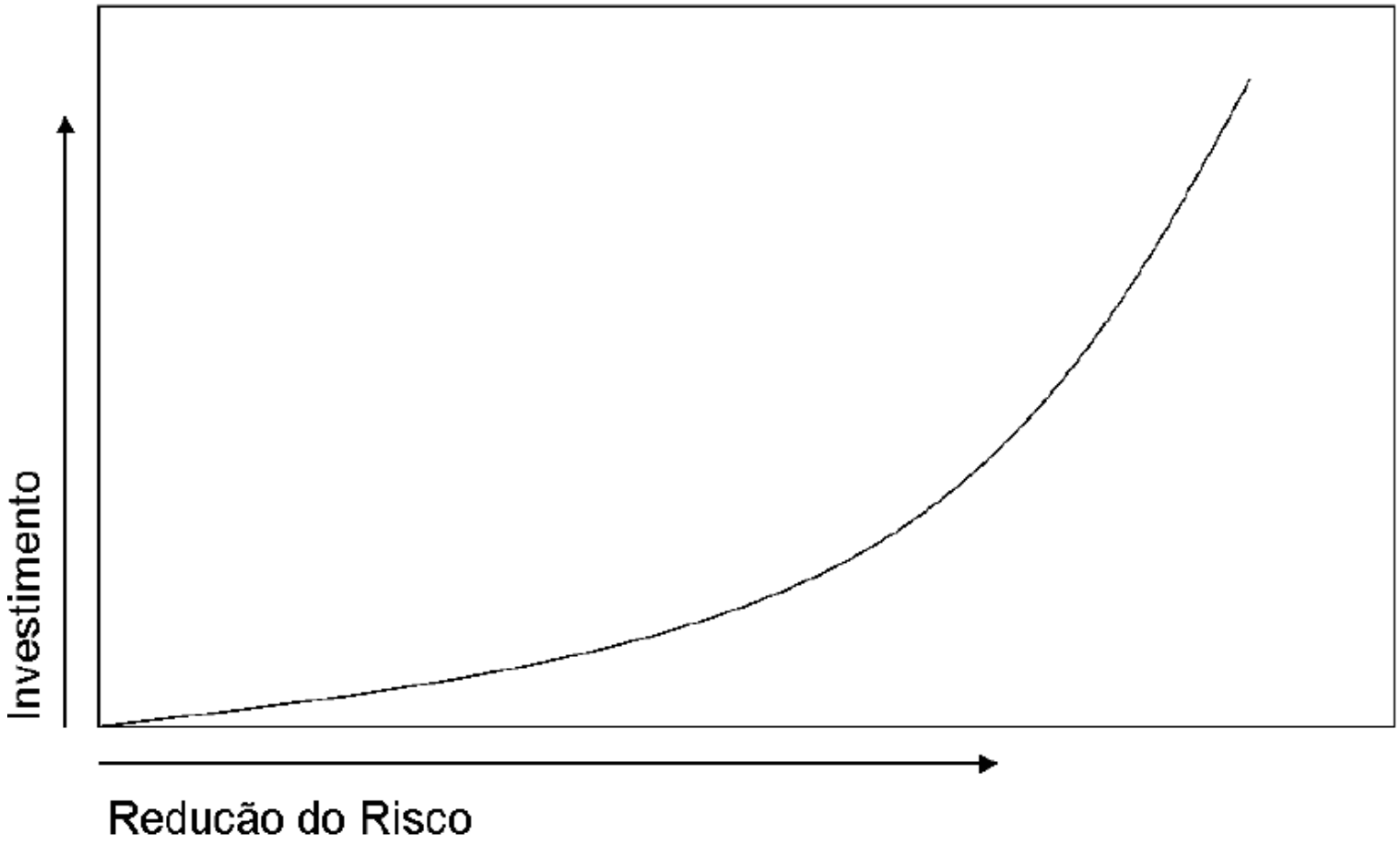


A Análise de Risco

1. Tecnologias
2. Processos
3. Ambientes
4. Usuários

Ameaça	Vulnerabilidades	Prob.	Impacto	Ocor.	Risco
Invasor externo	Software sem atualização	90%	50%	0,55%	46,85%
Invasor interno	Falta de controle de acesso físico	55%	50%	0,27%	35,09%
Vírus	Antivírus não atualizado	80%	50%	1,10%	43,70%
Variação de energia	Falta de no-break	40%	50%	1,10%	30,37%
Invasor externo	Software sem atualização	53%	60%	0,82%	37,94%
Invasor interno	Falta de controle de acesso físico	60%	60%	0,00%	40,00%
Vírus	Antivírus não atualizado	70%	60%	0,82%	43,61%
Variação de energia	Falta de no-break	50%	60%	1,37%	37,12%
Invasor externo	Software sem atualização	35%	78%	1,10%	38,03%
Invasor interno	Falta de controle de acesso físico	78%	78%	0,00%	52,00%
Vírus	Antivírus não atualizado	70%	78%	1,10%	49,70%
Variação de energia	Falta de no-break	69%	78%	0,55%	49,18%

A Análise de Risco – Ações



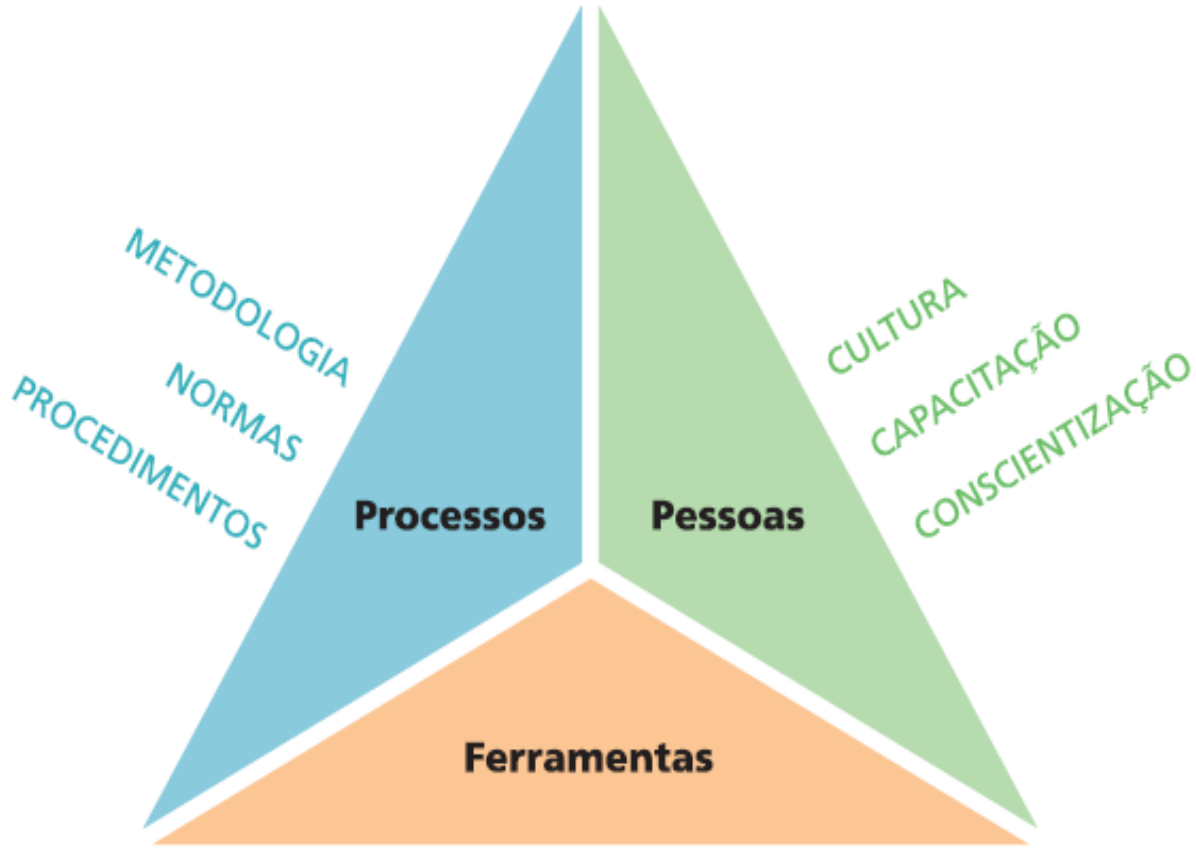
Política de Segurança da Informação

- Define o posicionamento da empresa
- Gera conscientização dos usuários
  - previne incidentes por "*desconhecimento*"
- Permite a cobrança de responsabilidades

Plano de Continuidade de Negócio

- Quais as necessidades de continuidade dos processos de negócio?
- A estrutura atual atende a estas necessidades?
  - (caso da indústria de fertilizantes)
- Desenvolvimento de estratégias e planos de continuidade!

Auditorias de Segurança



2. Identificação e Avaliação de Ativos

O que é um Ativo de Info.?

- É qualquer informação que tem valor para a organização.

- É qualquer informação onde um incidente possa causar prejuízos:
  - Perda de confidencialidade
  - Perda de integridade
  - Perda de disponibilidade

Inventário de Ativos de Inf.

- Listagem dos Principais ativos de informação.
- Define responsável pela informação
- Define a localização da informação
- Define a classificação da informação

Inventário de Ativos de Inf.

- O inventário é dinâmico
- Deve ser constantemente atualizado
- Gera melhoria contínua nos processos de segurança da informação
- Serve de base para políticas e análises

Identificação dos Ativos

- Relacione as principais informações envolvidas com seu trabalho ou setor
  - Físicas e lógicas

- A informação possui:
  - Algum grau de disponibilidade?
  - Algum grau de confidencialidade?
  - Algum grau de integridade?

Posso agrupar ativos?

- Sempre que um conjunto de ativos tiver o mesmo:
  - Objetivo de negócio
  - Responsável e localização
  - Classificação de segurança
- Exemplo:
  - Documentos de RH do colaborador.
  - Documentos fiscais.
  - Certificados de software.

Tipos de Ativos de Inf.

- Processos de Negócio
- Informação (lógica ou física)

- Hardware de suporte
- Software de suporte
- Ambientes físicos
- Pessoas
- Etc...

Avaliação de Ativos

- Deve-se determinar o valor do ativo para a organização

- Pode ser feito segundo vários parâmetros:
  - Custo de reparo
  - Custo de reposição
  - Tempo previsto de parada, etc

Avaliação de Ativos

- Estratégia muito usada é:
  - Confidencialidade
  - Integridade
  - Disponibilidade

Avaliação de Ativos

- Deve-se determinar uma escala:

LEGENDA		Pontuação
	1-Crítico	4
	2-Alto	3
	3-Moderado	2
	4-Baixo	1
	5-Nulo	0

Avaliação de Ativos

- Deve-se definir critérios para avaliação dos ativos

- Exemplo de critérios:
  - Imagem da organização no mercado
  - Parada de processos operacionais
  - Prejuízos financeiros
  - Abrangência dos efeitos
    - Ex.: processo, setor, organização, mercado

Avaliação de Ativos

- Exemplo de critérios:
  - Efeitos legais e contratuais
  - Custo de reposição
  - Perda confiança

  - Perda vantagem competitiva
  - Etc, etc, etc....

Classif. Confidencialidade

- Qual o impacto para a organização caso o ativo seja acessado por alguém não autorizado?

  – Crítico: efeitos negativos extremos
  – Alta: efeitos negativos severos
  – Moderada: efeitos negativos sérios
  – Baixa: efeitos negativos limitados
  – Nula: sem efeitos negativos

Classif. Integridade

- Qual o impacto para a organização caso o ativo seja alterado (fraudado, corrompido) indevidamente?

  – Crítico: efeitos negativos extremos
  – Alta: efeitos negativos severos
  – Moderada: efeitos negativos sérios
  – Baixa: efeitos negativos limitados
  – Nula: sem efeitos negativos

Classif. Disponibilidade

- Qual o impacto para a organização caso o ativo seja perdido ou fique “fora do ar” por tempo indeterminado?

  – Crítico: efeitos negativos extremos
  – Alta: efeitos negativos severos
  – Moderada: efeitos negativos sérios
  – Baixa: efeitos negativos limitados
  – Nula: sem efeitos negativos

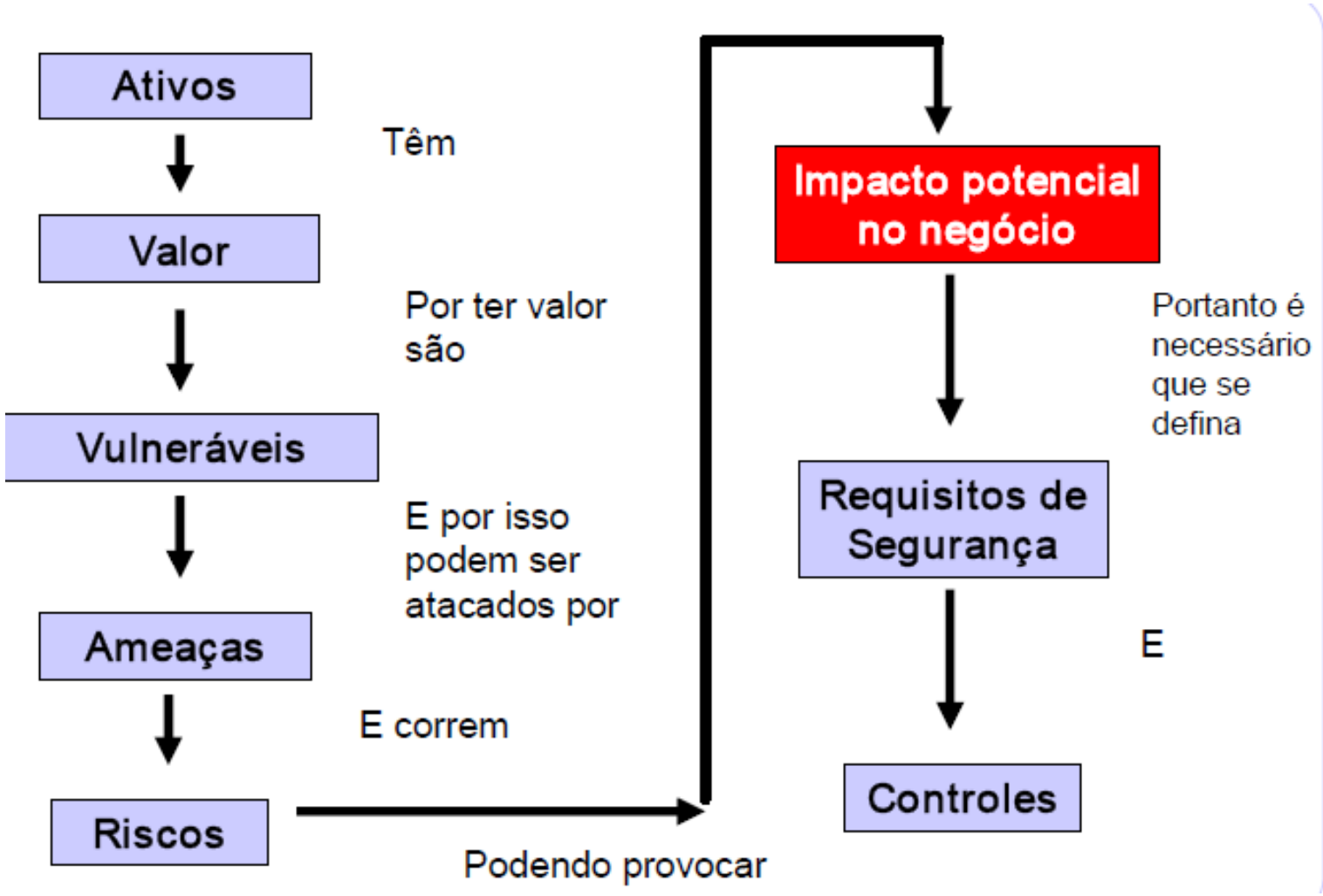
Atividade 1

- Definir pelo menos dois ativos :
  - Informação lógica
  - Informação física
  - Hardware
  - Software
  - Ambiente físico

- Avaliar os ativos sob as variáveis de:
  - Confidencialidade
  - Integridade
  - Disponibilidade

3. Identificação e Avaliação de Ameaças

O papel das Ameaças



Identificação de Ameaças

- Ameaças são:
  - Agentes ou condições
  - Exploram vulnerabilidades
  - Causam incidentes
  - Perda de confidencialidade, integridade e disponibilidade
  - Causam impacto nos negócios da organização.

Identificação de Ameaças

- Ameaças exploram vulnerabilidades para realizar incidentes.

- Tentativa de quebras as propriedades de:
  - Confidencialidade
  - Integridade
  - Disponibilidade

Identificação de Ameaças

- As ameaças sempre existirão:
- Independente dos controles de segurança
- Os controles atuam sobre as vulnerabilidades
- Para neutralizar as ameaças

Identificação de Ameaças

- Classificação das ameaças:
  - Intencionais;
  - Acidentais;
  - Internas;
  - Externas;

Identificação de Ameaças

- **As ameaças internas são importantes**:
  - Procedimento inadequado de funcionários;
  - Funcionários mal treinados;
  - Contaminação por vírus;
  - Pirataria;
  - Roubo de informações;
  - Fraudes de funcionários;
  - Outras ações intencionais;

Exemplos...

Tipo	Ameaças
Dano físico	Fogo
	Água
	Poluição
	Acidente grave
	Destruição de equipamento ou mídia
	Poeira, corrosão, congelamento
Eventos naturais	Fenômeno climático
	Fenômeno sísmico
	Fenômeno vulcânico
	Fenômeno Meteorológico
	Inundação
Paralisação de serviços essenciais	Falha do ar condicionado ou do sistema de suprimento de água
	Interrupção do suprimento de energia
	Falha do equipamento de telecomunicação
Distúrbio causado por radiação	Radiação eletromagnética
	Radiação térmica
	Pulsos eletromagnéticos
Comprometimento da informação	Interceptação de sinais de interferência comprometedores
	Espionagem à distância
	Escuta não autorizada
	Furto de mídia ou documentos
	Furto de equipamentos
	Recuperação de mídia reciclada ou descartada
	Divulgação indevida
	Dados de fontes não confiáveis
	Alteração do hardware
	Alteração do software

Exemplos...

Tipo	Ameaças
Falhas técnicas	Falha de equipamento
	Defeito de equipamento
	Saturação do sistema de informação
	Defeito de *software*
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
Ações não autorizadas	Uso não autorizado de equipamento
	Cópia ilegal de *software*
	Uso de cópias de *software* falsificadas ou ilegais
	Comprometimento dos dados
	Processamento ilegal de dados
Comprometimento de funções	Erro durante o uso
	Abuso de direitos
	Forjamento de direitos
	Repúdio de Ações
	Indisponibilidade de recursos humanos

Avaliação de Ameaças

- Deve-se avaliar as ameaças sob determinado critério e escala.

- Grau de exposição:
  - Determina o quanto a organização está exposta à ameaça.

LEGENDA		Pontuação
	1-Crítico	4
	2-Alto	3
	3-Moderado	2
	4-Baixo	1
	5-Nulo	0

Avaliação de Ameaças

- Critérios de avaliação:
  - Histórico de incidentes
  - Experiência do analista
  - Natureza do negócio
  - Catálogo de ameaças
    - Fontes diversas

Avaliação de Ameaças

- Critérios de ameaças intencionais:
  - Motivações do atacante
  - Competências do atacante
  - Poder atrativo dos ativos

Avaliação de Ameaças

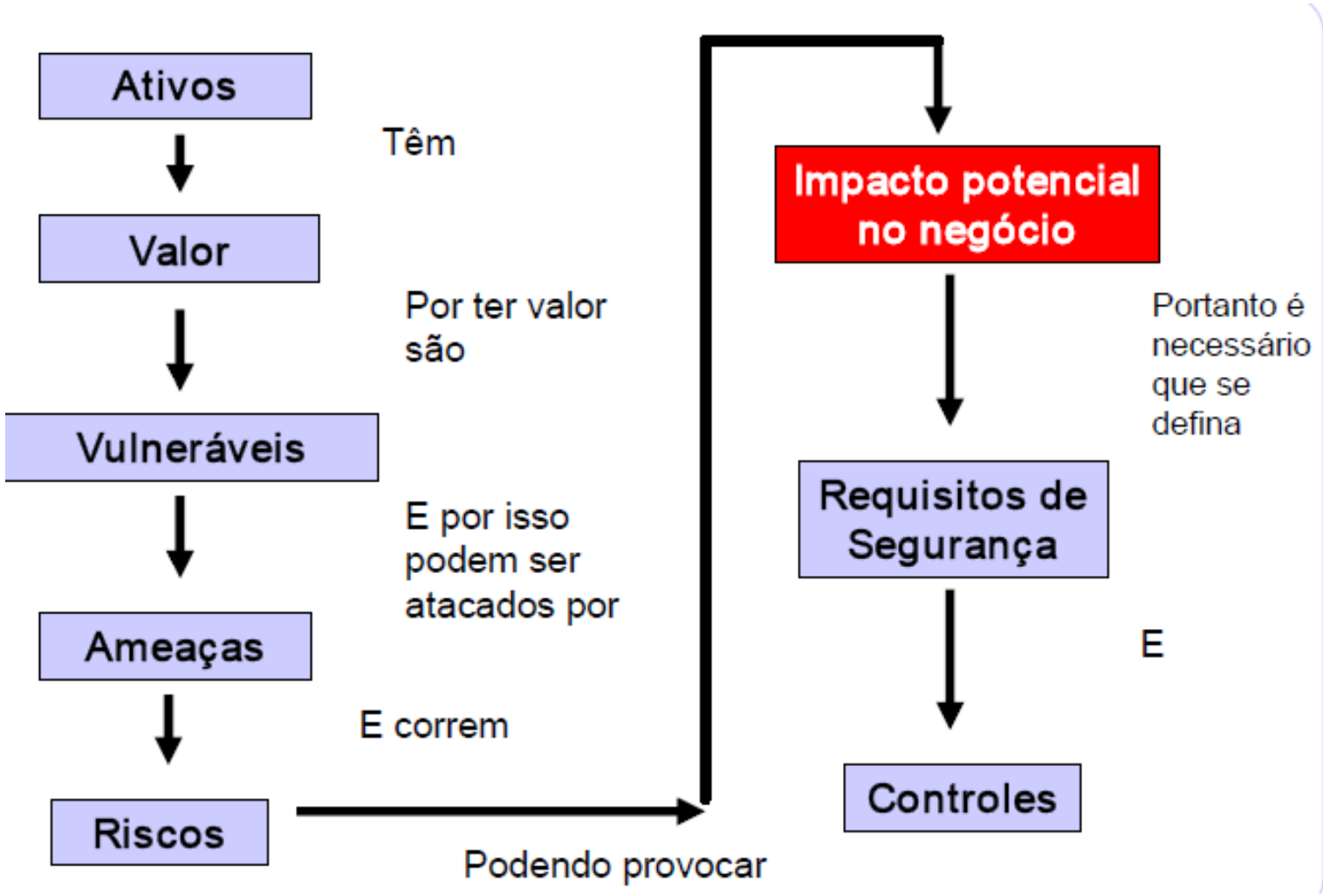
- Critérios de ameaças acidentais:
  - Proximidade com fábricas e depósitos
  - Possibilidade de eventos climáticos
  - Fatores causadores de erros humanos
    - Ex. insalubridade
  - Fatores causadores de falha em equipamentos

Atividade 2

- Identificar duas ameaças de diferentes tipos.
- Determinar o Grau de Exposição para as ameaças de seu grupo.
- Justificar com critérios.

4. Identificação e Avaliação de Vulnerabilidades

O papel das Vulnerabilidades



Ident. de Vulnerabilidades

- São fragilidades ou falhas nos ativos
- São exploradas por ameaças para realização de incidentes
- Afetam confidencialidade, integridade e disponibilidade

Ident. de Vulnerabilidades

- Vulnerabilidades são passivas
- São problemas em potencial
- A vulnerabilidade sozinha não é um problema

- Vulnerabilidade precisa ser explorada
- Agente causador ou condição favorável:
  - **A Ameaças!!!**

Ident. de Vulnerabilidades

- Classificação das Vulnerabilidades:
  - Físicas;
  - Naturais;
  - De hardware;
  - De software;
  - Humanas;
  - Organizacionais;
  - Etc...

Ident. de Vulnerabilidades

- **Vulnerabilidades Físicas**:
  - Instalações prediais fora do padrão;
  - CPD mal planejado;
  - Falta de extintores de incêndio;
  - Detectores de fumaça;
  - Proximidade com depósitos;
  - Manutenções mal feitas
  - Etc...

Ident. de Vulnerabilidades

- **Vulnerabilidades Naturais**:
  - Falta de prevenção para:
    - Enchentes;
    - Terremotos;
    - Acúmulo de poeira;
    - Umidade;
    - Temperatura;

Ident. de Vulnerabilidades

- **Vulnerabilidades de Hardware**:
  - Desgaste de peças;
  - Falha de recurso;
  - Erro de instalação;
  - Má utilização;
  - Falta de manutenção;
  - Etc...

Ident. de Vulnerabilidades

- **Vulnerabilidades de Software**:
  - Erros de instalação;
  - Erros de configuração;
  - Defeitos de software;
  - Falta de requisitos de segurança;

Ident. de Vulnerabilidades

- **Vulnerabilidades Humanas**:
  - Falta de treinamento;
  - Falta de conscientização;
  - Não executar procedimentos de segurança;
  - Erros ou omissões;
  - Greves;

Ident. de Vulnerabilidades

- **Vulnerabilidades de organização**:
  - Inexistência de controles físicos
  - Inexistência de monitoramentos
  - Inexistência de Política de Segurança
  - Inexistência de Plano de Continuidade
  - Inexistência de auditorias
  - Inexistência de análises críticas
  - Indefinição de responsabilidades
  - Etc...

Ident. de Vulnerabilidades

- Técnicas de identificação (tecnologia):
  - Ferramentas automatizadas de vulnerabilidades
  - Testes de invasão
  - Análise da segurança de sistemas
  - Etc...

Ident. de Vulnerabilidades

- Técnicas de identificação (gestão):
  - Entrevistas com gerentes e usuários
  - Questionários de segurança
  - Inspeção física
  - Análise de documentos
  - Análise GAP ISO 27001
  - Etc...

Avaliação de Vulnerabilidades

- Deve-se avaliar as vulnerabilidades sob determinado critério e escala.

- Grau de Deficiência:
  - Determina o tamanho da deficiência gerada pela vulnerabilidade

LEGENDA		Pontuação
	1-Crítico	4
	2-Alto	3
	3-Moderado	2
	4-Baixo	1
	5-Nulo	0

Avaliação de Vulnerabilidades

- **Critérios de avaliação de checklist:**

  – Atendimento total
  – Atendimento parcial
  – Atendimento informal
  – Não atendimento
  – Controle não relevante

Avaliação de Vulnerabilidades

- **Critérios de avaliação de boas práticas:**
  - Faz sempre
  - Faz freqüentemente
  - Faz raramente
  - Não faz
  - Prática não relevante

Avaliação de Vulnerabilidades

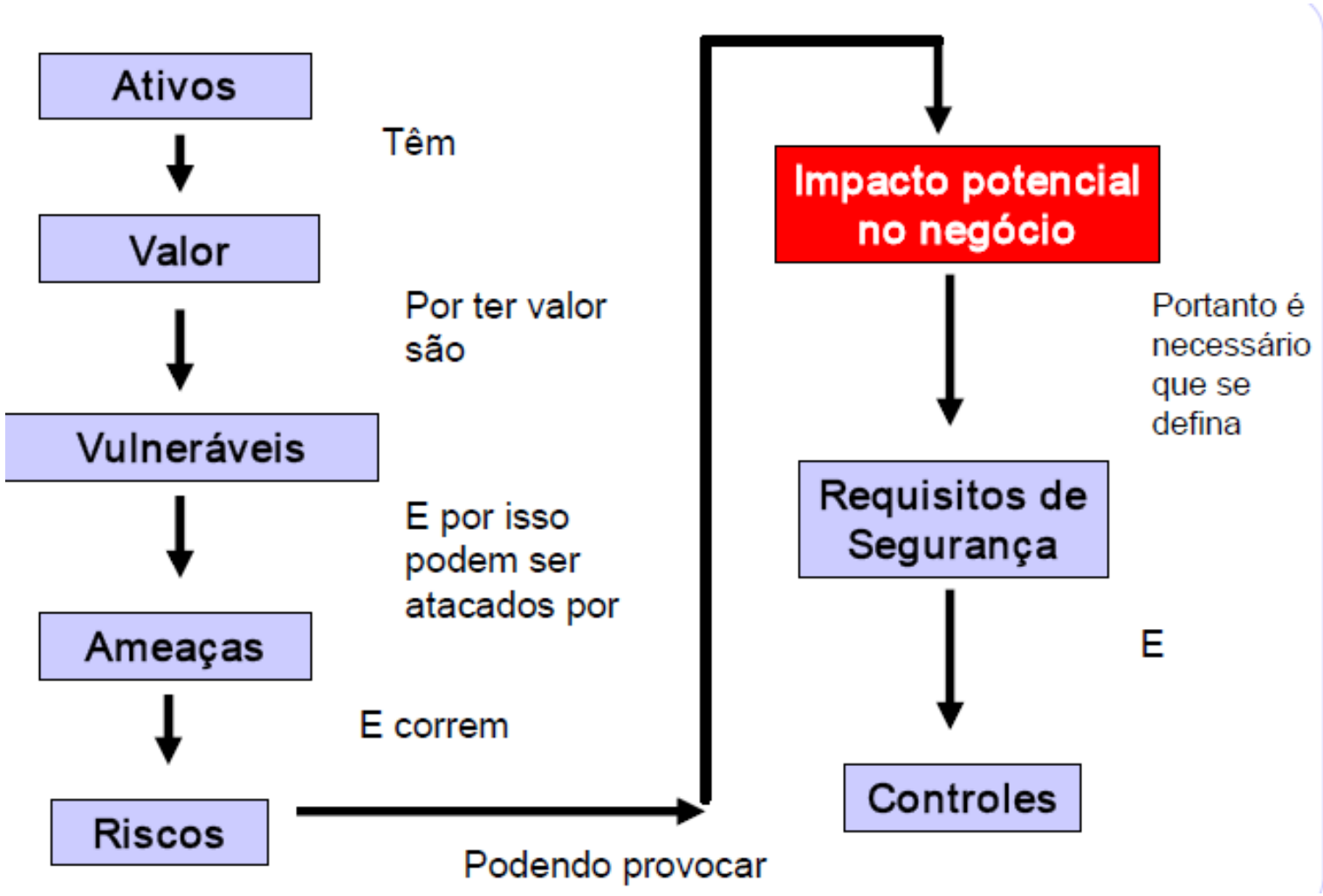
- **Critérios de avaliação de tecnologias:**
  - Controle total do ativo
  - Permite alterar informações
  - Permite copiar informações
  - Permite indisponibilizar o ativo
  - Falha não relevante

Atividade 3

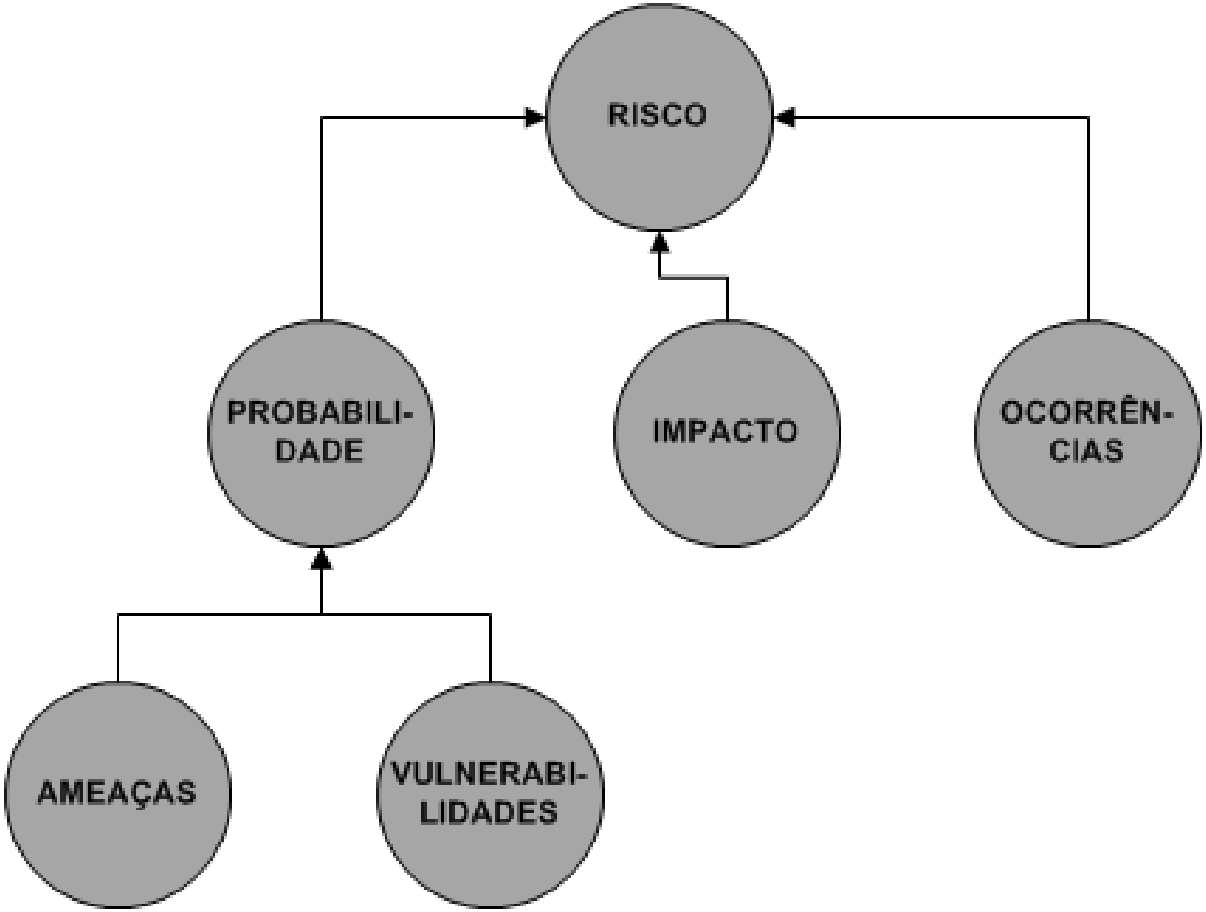
- Identificar vulnerabilidades de diferentes tipos
- Para as ameaças definidas por seu grupo
- Determinar o Grau de Deficiência para as vulnerabilidades de seu grupo
- Justificar com critérios.

5. Avaliação do Risco e Consequências

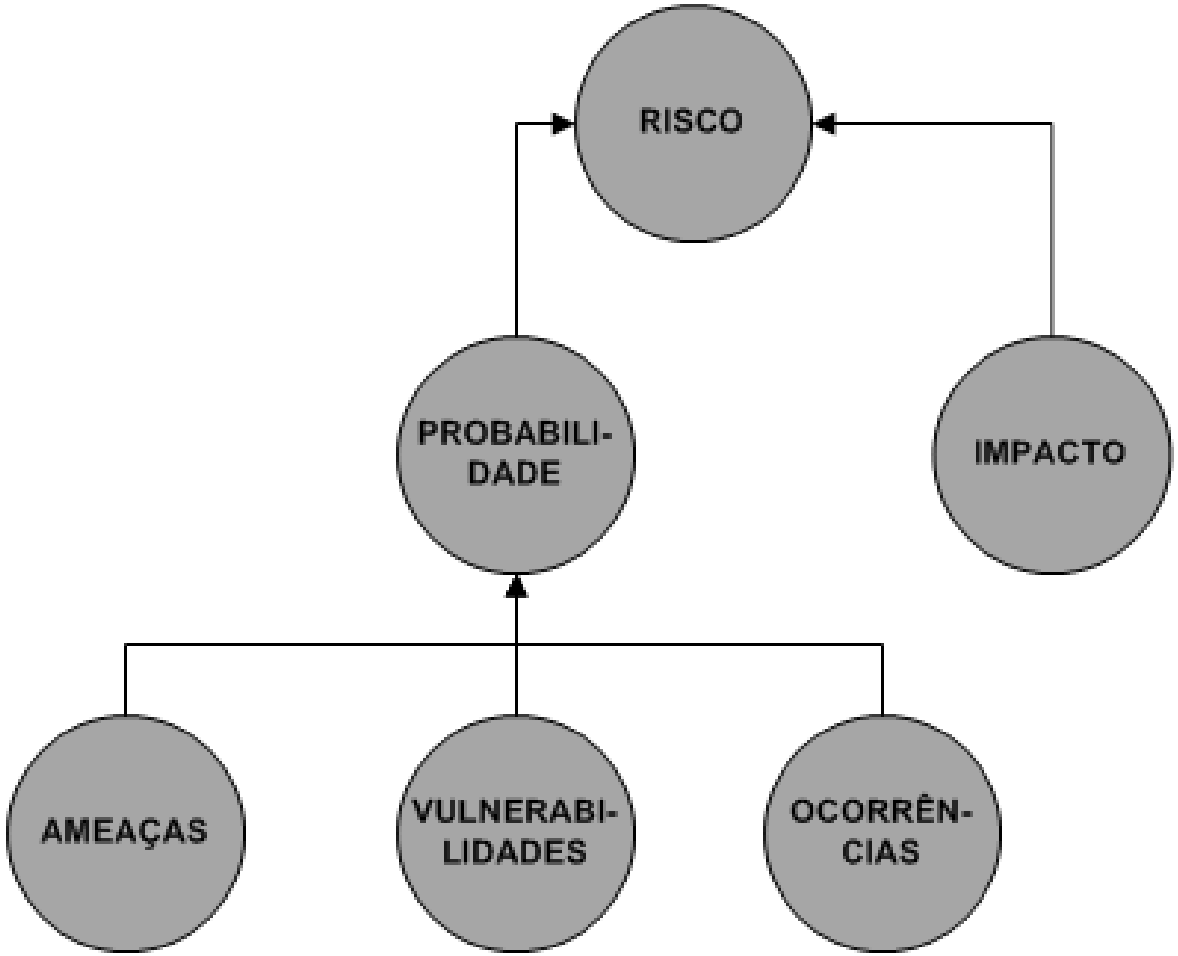
Avaliação do Risco



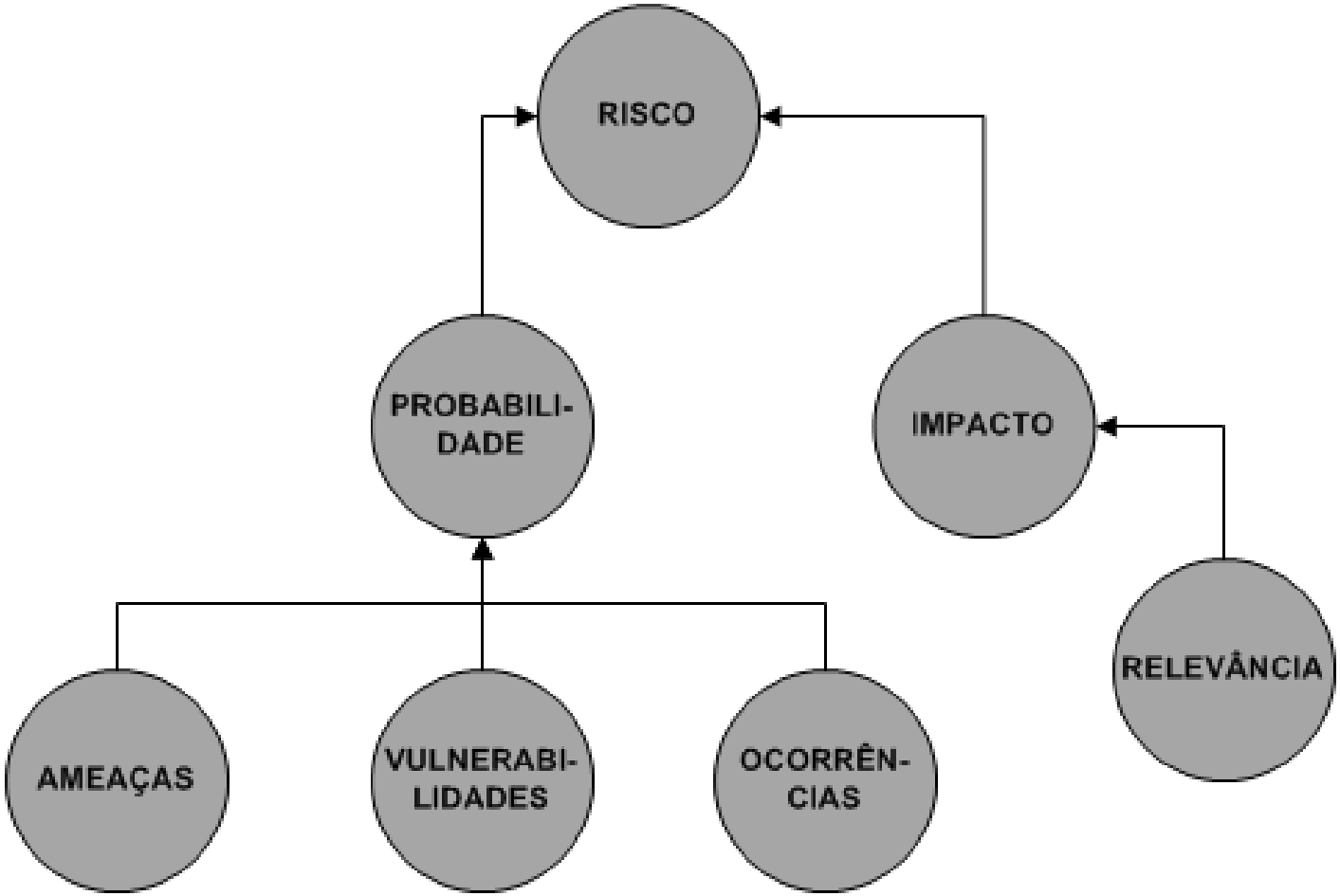
Parâmetros de Risco



Parâmetros de Risco



Parâmetros de Risco



Cálculo do Risco

Ativo	Ameaça	Vulnerabilidades	Prob.	Impacto	Ocor.	Risco
Firewall	Invasor externo	Software sem atualização	90%	50%	0,55%	46,85%
	Invasor interno	Falta de controle de acesso físico	55%	50%	0,27%	35,09%
	Vírus	Antivírus não atualizado	80%	50%	1,10%	43,70%
	Variação de energia	Falta de no-break	40%	50%	1,10%	30,37%
Servidor de arquivos	Invasor externo	Software sem atualização	53%	60%	0,82%	37,94%
	Invasor interno	Falta de controle de acesso físico	60%	60%	0,00%	40,00%
	Vírus	Antivírus não atualizado	70%	60%	0,82%	43,61%
	Variação de energia	Falta de no-break	50%	60%	1,37%	37,12%
Sistema Administrativo	Invasor externo	Software sem atualização	35%	78%	1,10%	38,03%
	Invasor interno	Falta de controle de acesso físico	78%	78%	0,00%	52,00%
	Vírus	Antivírus não atualizado	70%	78%	1,10%	49,70%
	Variação de energia	Falta de no-break	69%	78%	0,55%	49,18%

Matriz de Risco

MATRIZ DE RISCO POR PERCENTUAL						
	Probabilidade	1-Crítica	2-Alta	3-Moderada	4-Baixa	5-Nula
Impacto sobre os ativos	1-Crítico	100	87,5	75	62,5	50
	2-Alto	87,5	75	62,5	50	37,5
	3-Moderado	75	62,5	50	37,5	25
	4-Baixo	62,5	50	37,5	25	12,5
	5-Nulo	50	37,5	25	12,5	0

LEGENDA		Pontuação
	1-Crítico	4
	2-Alto	3
	3-Moderado	2
	4-Baixo	1
	5-Nulo	0

Matriz de Risco

	Probabilidade da ocorrência - Ameaça	Baixa			Média			Alta		
	Facilidade de Exploração	B	M	A	B	M	A	B	M	A
Valor do Ativo	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Matriz de Risco

	Probabilidade do cenário de incidente	Muito baixa (Muito improvável)	Baixa (Improvável)	Média (Possível)	Alta (Provável)	Muito Alta (Frequente)
Impacto ao Negócio	Muito Baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito Alto	4	5	6	7	8

Critérios para Prática

- Impacto sobre o ativo = (Conf + Int + Disp)/3
- Probabilidade = (GE + GV)/2
- Risco = (Impacto + Probabilidade)

Critérios para Prática

MATRIZ DE RISCO POR SOMATÓRIO						
	Probabilidade	1-Crítica	2-Alta	3-Moderada	4-Baixa	5-Nula
Impacto sobre os ativos	1-Crítico	8	7	6	5	4
	2-Alto	7	6	5	4	3
	3-Moderado	6	5	4	3	2
	4-Baixo	5	4	3	2	1
	5-Nulo	4	3	2	1	0

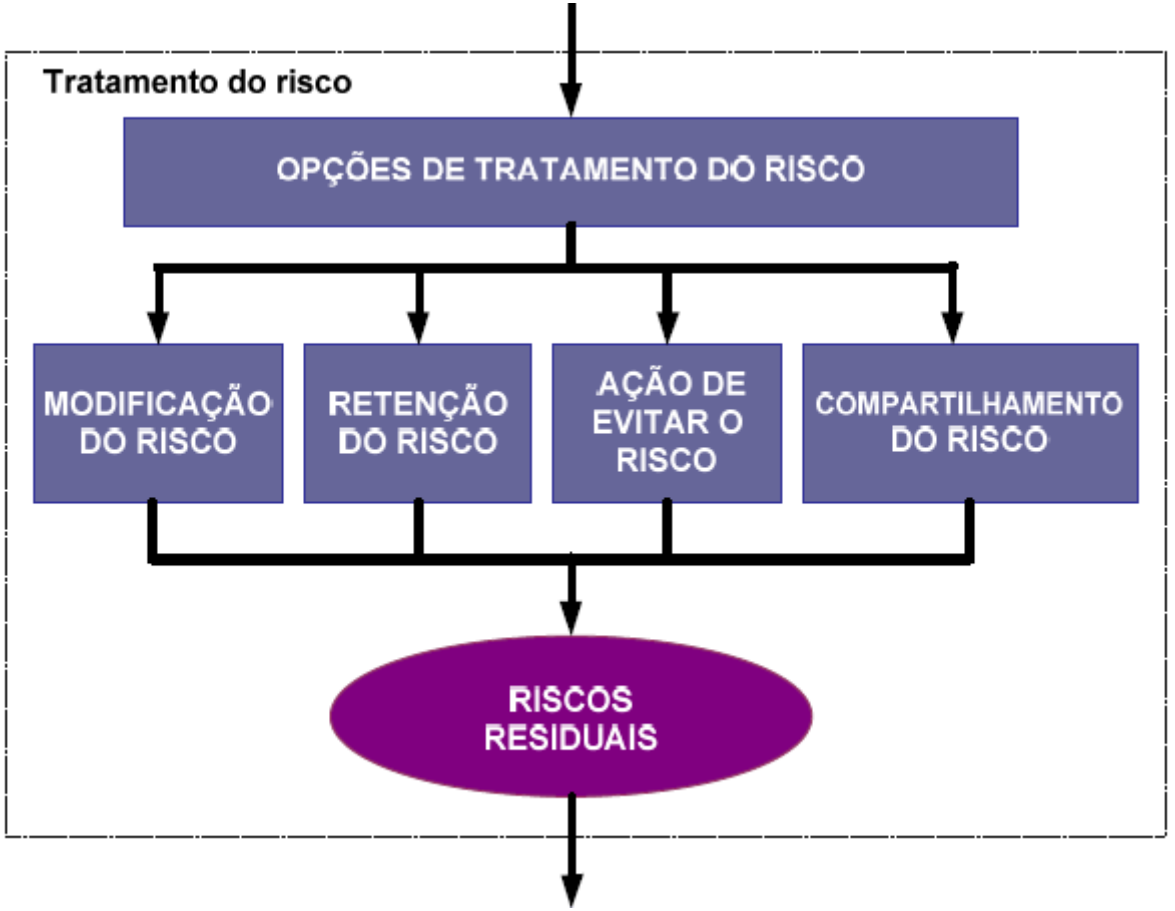
LEGENDA		Pontuação
	1-Crítico	4
	2-Alto	3
	3-Moderado	2
	4-Baixo	1
	5-Nulo	0

Atividade 4

- Calcular o risco para os ativos, ameaças e vulnerabilidades de seu grupo.

- Classificar o risco conforme matriz de risco.

Tratamento dos Riscos



Tratamento dos Riscos

- Modificar através da implantação de controles.
- Aceitar o risco.
- Evitar o risco: ex. mudar a empresa de local geográfico
- Compartilhar: ex. contratar seguros.

6. Política de Segurança da Informação

Importância da Política de Segurança

- Segurança baseada em controles tecnológicos!?

- Não conscientiza usuários na proteção dos ativos!
- Não permite punições!
  - caso do monitoramento do e-mail corporativo

- Gera a cultura: "***Se consigo, logo posso!!!***"

Conceitos Básicos

- Qual o objetivo da Política?

Conceitos Básicos

- Conjunto de regras;
- Determina como as informações são geridas;
- Deve ser ampla e simples;
- Revisão contínua;
- Apoio da alta administração;

Conceitos Básicos

- Aplicada a toda a organização;
- Define objetivos;
- Define responsabilidades;
- Define escopo;
- Define punições;
- Cita leis e regulamentos;

Conceitos Básicos

- Não existem modelos prontos de política;
- Não existe política certa ou errada;
- A política deve ser definida de acordo com cada organização;

Comitê de Segurança

- Deve ser formada pelo comitê de segurança
- Representantes de todas as áreas
- O comitê discute e define as políticas

Comitê de Segurança

- **A TI deve fazer os outros setores "comprarem" o projeto da PSI!!!**

- A TI coordena o comitê de segurança
  - Não criar regras ilegais
  - Não criar regras inseguras
  - Não criar regras inviáveis
  - Não criar regras discriminatórias
  - Não criar regras genéricas

Estrutura da PSI

- Introdução
  - Apresentação
  - Objetivos
  - Declaração da Administração
  - Definições
  - Autores
  - Divulgação e Distribuição
  - Versão e Revisão
  - Manutenção da Segurança da Informação

Estrutura da PSI

- Segurança Lógica
  - Acesso à internet
  - Acesso à rede interna
  - Armazenamento de Informações
  - Propriedade Intelectual
  - Uso de Sistemas Corporativos
  - Uso de E-mail
  - Uso de Senhas
  - Sistemas de Troca de Mensagens
  - Uso da Telefonia

Estrutura da PSI

- Segurança Física
  - Gestão da Segurança Física
  - Ambientes de Segurança Física
  - Controle de Acesso Físico
  - Uso de Chaves e Alarmes

- Incidentes e Punições
  - Notificação de Incidentes
  - Punições

Implantação da PSI

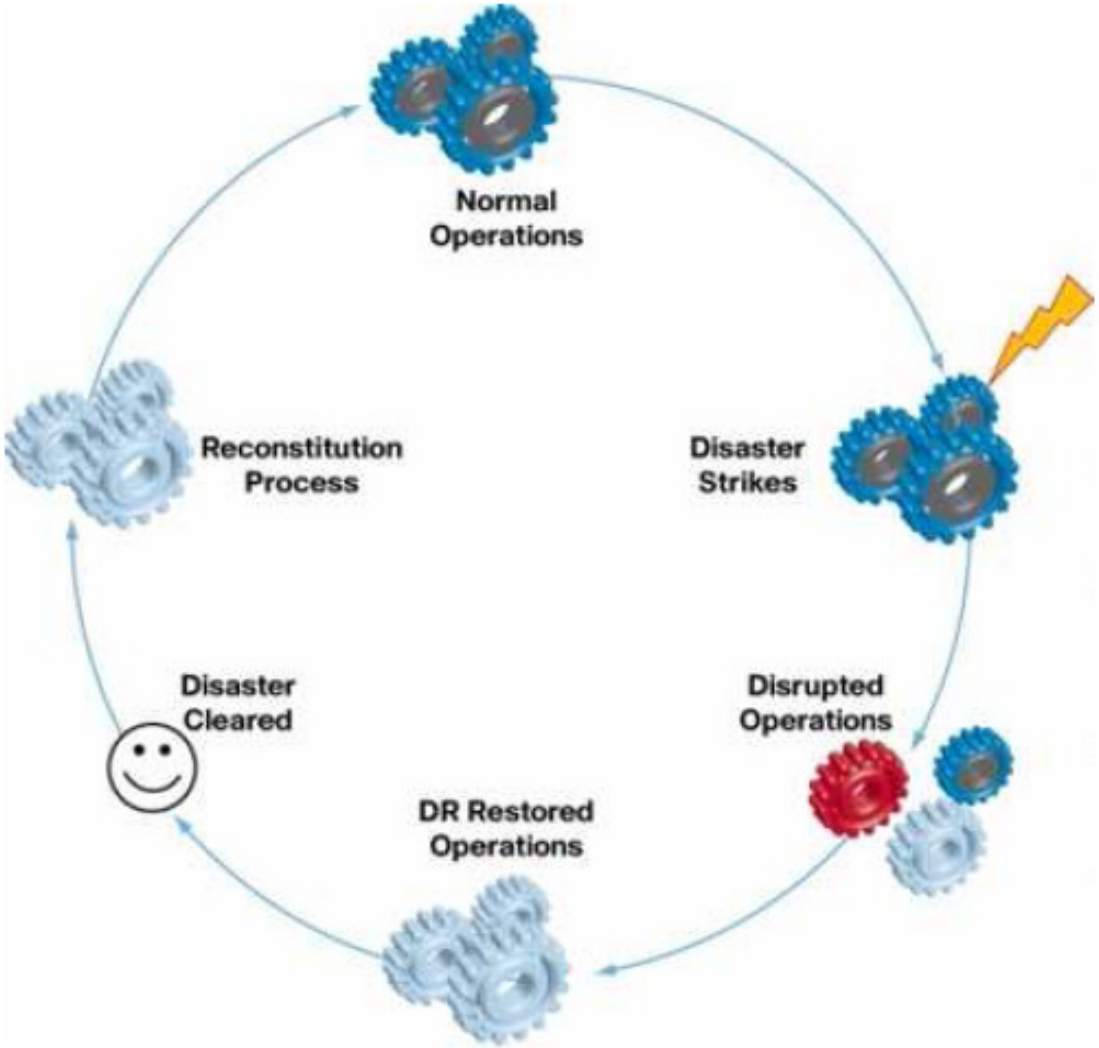
- Homologação da PSI
- Desenvolvimento de Processos

- Treinamento
- Avaliação do Treinamento

- Campanha de Conscientização
- Registro dos Incidentes

7. Plano de Continuidade de Negócio

Visão Geral de PCN



PCN – ISO 27001

- Objetivo:
  - Não reduzir a parada das atividade
  - Proteger os processos críticos
  - Assegurar a retomada em tempo hábil

- Garantir a recuperação a um nível aceitável:
  - Ações de prevenção e recuperação

Uma Proposta de Roteiro

- Etapa 1 – Análise do Impacto de Negócio
- Etapa 2 – Definir Estratégias
- Etapa 3 – Desenvolver os Planos
- Etapa 4 – Testes e Manutenção

Análise de Impacto de Negócio

- É a base para o desenvolvimento do PCN
- Define os processos essenciais e seus impactos em caso de parada
- O objetivo:
  - Definir o IMA - Interrupção Máxima Aceitável
  - Definir o nível mínimo de serviço aceitável

Análise de Impacto de Negócio

- Para cada processo essencial:
  - Classificar o processo
  - Identificar o impacto (financeiro, operacional e imagem)
  - Definir requisitos mínimos de contingência
  - Definir a Interrupção Máxima Aceitável
  - Definir dependências do processos

Análise de Impacto de Negócio

- É importante que os dados da BIA sejam revisados com:
  - Alta administração
  - Responsáveis pelo processo

- Pode ser feito através de:
  - Reuniões, workshops,
  - Questionários e entrevistas.

Etapas da BIA

1. Processos ou Atividades Essenciais

2. Definição dos Impactos

3. Definição das Dependências

Atividade 5 (extra)

- Defina um processo de negócio
- Defina seu IMA
- Defina seu impacto
  - Imagem
  - Operacional
  - Financeiro
- Defina suas dependências

Uma Proposta de Roteiro

- Etapa 1 – Análise do Impacto de Negócio
- Etapa 2 – Definir Estratégias
- Etapa 3 – Desenvolver os Planos
- Etapa 4 – Testes e Manutenção

Etapa 2 – Definir Estratégias

- Para onde nós iremos?
- Com que pessoas poderemos contar?
- Com quais recursos poderemos contar?
- Quais investimentos serão necessários para viabilizar estes recursos e serviços?

Etapa 2 – Definir Estratégias – sp800-34

- Documentação da configuração de sistemas
- Uso de componentes padrão
- Usar componentes interoperáveis
- Backup de dados
- Backup de aplicações
- Redundância de componentes críticos do sistema
- Fonte extra de energia

Etapa 2 – Definir Estratégias – sp800-34

- Implementar tolerância a falhas
- Implementar replicação de dados
- Coordenação com suporte de infraestrutura
- Coordenação com fornecedores
- Coordenação com equipe de resposta a incidentes
- Monitoramento de recursos críticos

Etapa 2 – Definir Estratégias– sp800-34

- **Cold Site**: tem apenas o espaço para o novo ambiente, porém não instalado

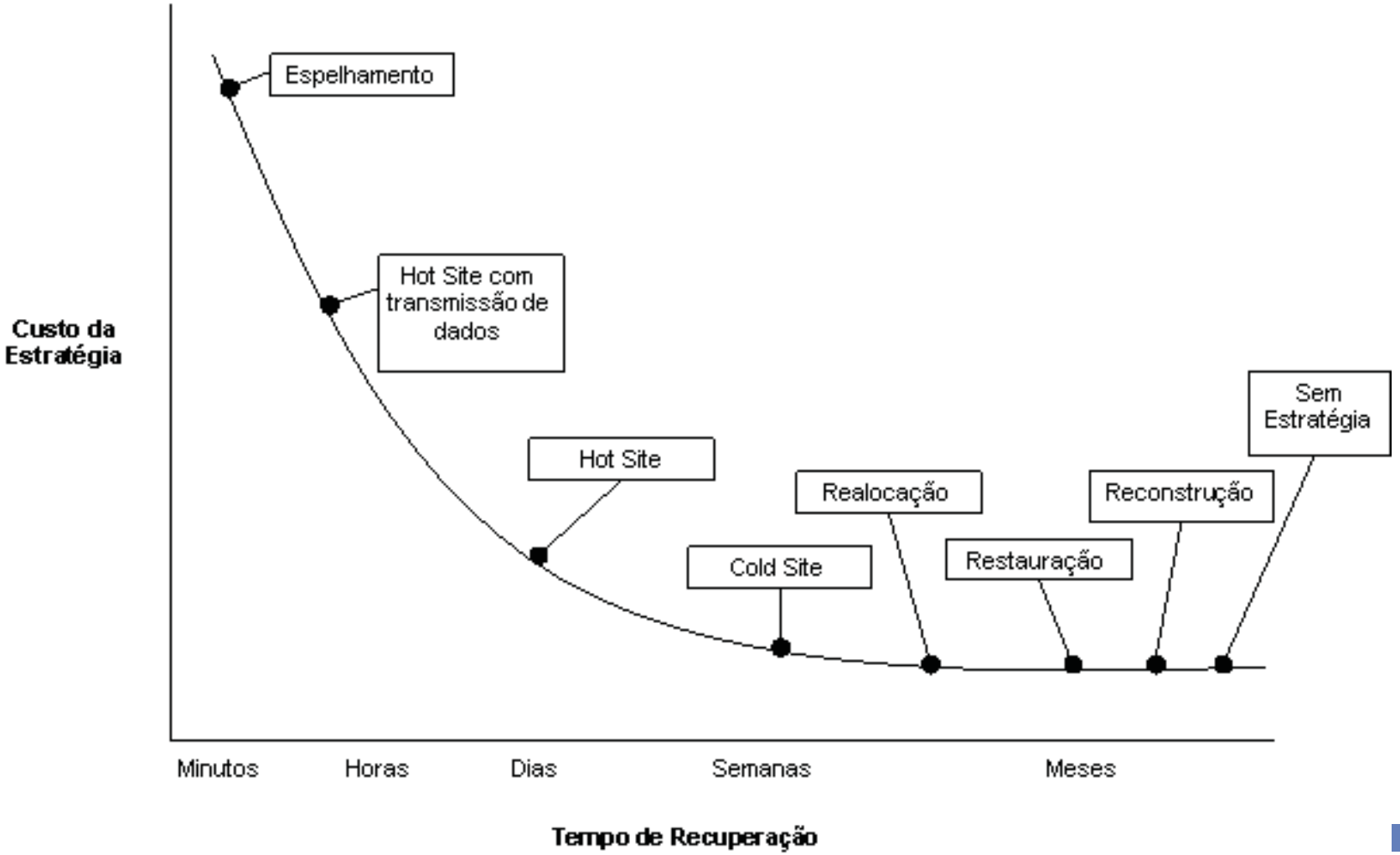
- **Warm Site**: contém espaço e equipamento, porém não contém o sistema a ser contingenciado. Normalmente serve para operação de outro sistema.

Etapa 2 – Definir Estratégias– sp800-34

- **Hot Site**: totalmente pronto para receber o sistema, porém depende do administrador.

- **Espelhamento**: ativação em tempo real.

Etapa 2 – Definir Estratégias– sp800-34



Atividade 6 (extra)

- Defina estratégias de continuidade para o processo previamente especificado

Uma Proposta de Roteiro

- Etapa 1 – Análise do Impacto de Negócio
- Etapa 2 – Definir Estratégias
- Etapa 3 – Desenvolver os Planos
- Etapa 4 – Testes e Manutenção

Exemplo Físico

- Contingência para rede de computadores:
  - **Ativação**: Para de equipamento de rede;
  - **Execução (1)**: substituir por equipamento sobressalente;
  - **Execução (2)**: desviar carga para outro equipamento previamente preparado;
  - **Reconstituição**: substituir equipamento danificado por outro permanente;

Exemplo Lógico

- Contingência para Sistema de Informação:
  - **Ativação**: Parada do sistema por mais de 10 minutos;
  - **Execução (1)**: restaurar cópia virtual do sistema e dados do backup em um servidor previamente definido;
  - **Execução (2)**: realizar procedimento em papel conforme plano pré-definido;
  - **Restauração**: reativar de modo permanente o servidor original ou com mesma configuração;

Uma Proposta de Roteiro

- Etapa 1 – Análise do Impacto de Negócio
- Etapa 2 – Definir Estratégias
- Etapa 3 – Desenvolver os Planos
- Etapa 4 – Testes e Manutenção

Etapa 4 – Testes e Manutenção

- Verificar o que não funciona;
- Reforçar o comprometimento dos envolvidos;

- Verificar a capacidade de recuperar;
- Validar compatibilidade técnica;

- Identificar oportunidades de melhorias.

Roteiro

1. Fundamentos de Segurança da Informação
2. Ativos de Informação
3. Identificação e Avaliação de Ameaças
4. Identificação e Avaliação de Vulnerabilidades
5. Avaliação do Risco

6. Política de Segurança da Informação
7. Plano de Continuidade de Negócio

Gestão de Segurança da Informação

Paulo Silva
Tracker Segurança da Informação

PauloSilva@TrackerTI.com