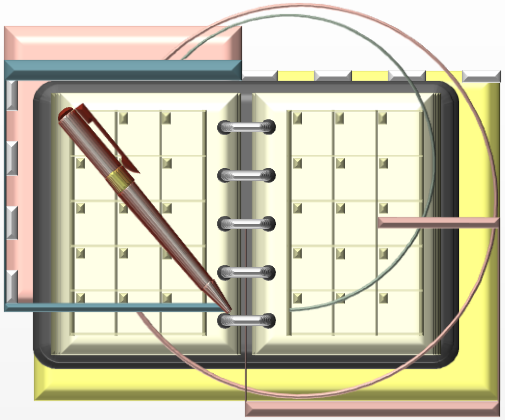
ISO/IEC 27005

Exemplificada

Fernando Fonseca
fernando@segurancaobjetiva.com

Agenda



- Case: Vírus Funlove em grande rede
- Normas e a Série 27000
- Riscos
- O Sistema de gestão da ISO 27005
- Solução "Tiroteio de Cegos"
- Solução "A Arte da Guerra"
- Conclusão

Segurança Objetiva

Case: Vírus Funlove em grande rede

Para ilustrar o processo de gestão de riscos segundo a ISO 27005, utilizaremos um case de uma empresa com presença em todo o Brasil e administrações regionais com relativa independência na tomada de decisões.

A empresa possui um gerente de TI e um domínio em cada região do Brasil, mas todas as unidades (1 ou mais por estado) são interligadas na mesma rede frame-relay

Segurança Objetiva

Normas

O que é norma?

É um documento estabelecido por consenso e aprovado por um organismo reconhecido, que fornece, para uso comum e repetitivo, regras, diretrizes ou características para atividades ou seus resultados, visando à obtenção de um grau ótimo de ordenação em um dado contexto.

Definição internacional - Fonte: ABNT

Segurança Objetiva

Série ISO 27000

Norma	*Descrição*	*Estágio*
27000	Visão Geral e Vocabulário	FDIS
27001	Requisitos de Sistemas de Gestão de Segurança da Informação	Publicada 2005
27002	Código de prática para Gestão da Segurança da Informação	Publicada 2005
27003	Diretrizes para Implementação de Sistemas de Gestão de Segurança da Informação	DIS
27004	Métricas de Sistemas de Gestão de Segurança da Informação	DIS
27005	**Gestão de Riscos de Segurança da Informação**	**Publicada 2008**
27006	Requisitos para Acreditação das Partes - Sistemas de Gestão de Segurança da Informação	Publicada 2007
27007	Diretrizes para auditar Sistemas de Gestão de Segurança da Informação	WD

Riscos

- "Risco é o efeito da incerteza nos objetivos." ISO Guide 73

- Uma expectativa de perda expressada como a probabilidade de que uma ameaça em particular irá explorar uma vulnerabilidade em particular com um resultado danoso em particular.

  RFC 2828 (Internet Security Glossary)

Segurança Objetiva

Percepção de Risco

- Maneira como a parte envolvida percebe o risco
- A percepção reflete as necessidades, problemas e conhecimento da parte envolvida.
- A percepção de um risco pode diferir dos dados reais e objetivos relacionados a este risco.

Segurança Objetiva

Definição do Contexto

- Entrada: Todas as informações relevantes
- Definição de escopo e limites
- Coleta de dados

Escopo

- Conjunto de ativos, ameaças e vulnerabilidades que serão cobertos pelo Sistema de Gestão de Risco

Segurança Objetiva

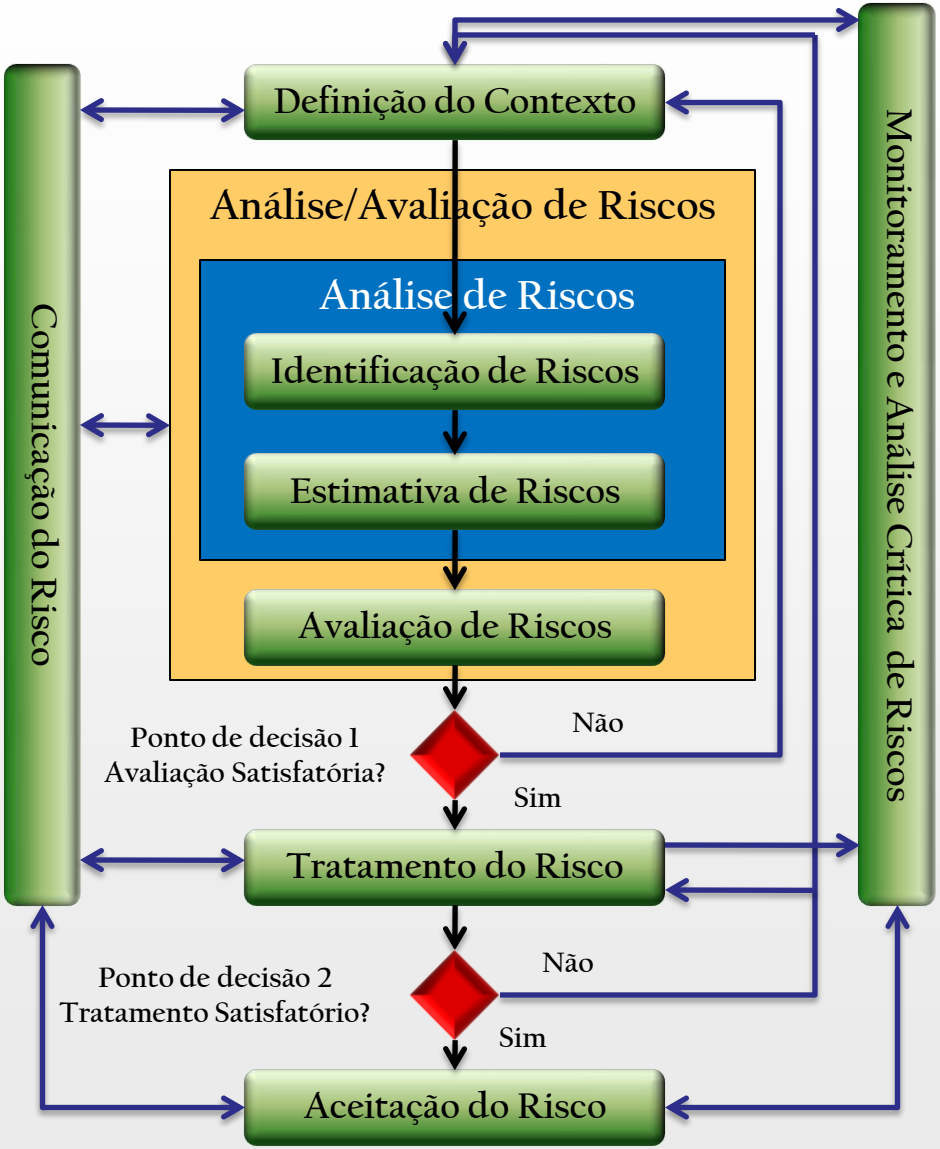
Coleta de Dados

- Coletar através dos questionários, entrevistas e outras ferramentas informações sobre o ambiente, ameaças, proteções existentes

Segurança Objetiva

Sistema de gestão da ISO 27005

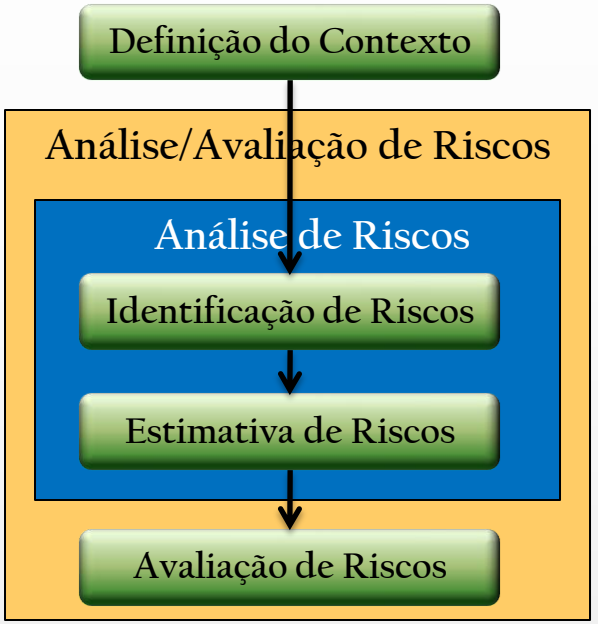
- Atividades de análise/avaliação podem ser realizadas mais de uma vez
- Atividades de tratamento também



Segurança Objetiva

Análise/Avaliação de Riscos

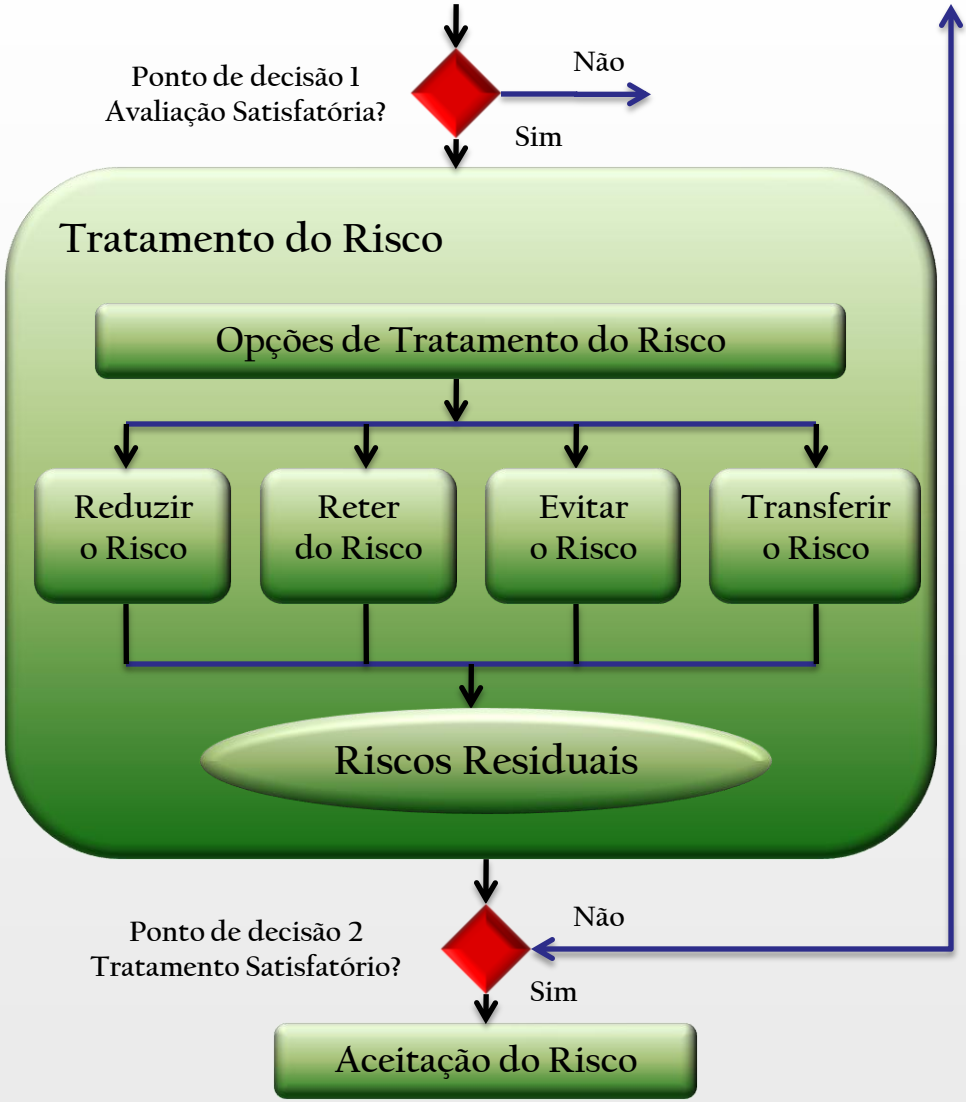
- Identificação dos Riscos
- Estimativa de Riscos
- Avaliação de Riscos



Segurança Objetiva

Tratamento do Risco

- Iniciado somente se a avaliação for satisfatória
- Utiliza a ação definida na avaliação de riscos



Segurança Objetiva

"Tempos de paz"

Segurança
Objetiva

"Tempos de paz"

- Critérios de impacto:
  - Impacto? Isso não vai acontecer, fique tranquilo...
  - Aceitação de riscos: Se acontecer algo, a culpa é do gerente de TI.

"Tiroteio de Cegos"

Segurança
Objetiva

"Tiroteio de Cegos"

- Definição do Contexto:
  - Escopo: estações e servidores da rede Windows

    Aproximadamente 10.000 estações (a maioria Windows 95 e 98) e 500 servidores Windows NT 4.0

.

"Tiroteio de Cegos"

- Definição do Contexto:
  - Apesar de usarmos um antivírus "X", estamos com uma infecção em 80% do parque de estações pelo vírus "Funlove";

Nota: A Infecção persiste por mais de um mês

"Tiroteio de Cegos"

- Análise/Avaliação:
  - Ameaça: perda de dados e indisponibilidade.
  - Controles existentes: Antivírus sem console de gerenciamento e considerado "mediano" por especialistas
  - Vulnerabilidades: Antivírus não consegue bloquear ataque do "Funlove"

"Tiroteio de Cegos"

- Opção de tratamento:

  Erradicar o vírus

  - Fazer um mutirão, desconectar todas estações no Brasil e desinfetá-las offline.

Segurança Objetiva

"Tiroteio de Cegos"

- Tratamento do risco

  Após um final de semana com pessoas em todas as cidades do Brasil, todas as estações e servidores foram "limpas"

- Tratamento não satisfatório

  Nova infecção em nível nacional dias depois

Segurança Objetiva

"Tiroteio de Cegos"

- Redefinição do Contexto:
  - Apesar do mutirão, o vírus persiste na rede.
  - O Antivírus é incapaz de proteger as estações

"Tiroteio de Cegos"

- Análise/Avaliação:
  - Ameaça: perda de dados e indisponibilidade.
  - Controles existentes: Antivírus sem console de gerenciamento e considerado "medíocre" pela crítica
  - Vulnerabilidades: Antivírus não consegue bloquear ataque do "Funlove"

"Tiroteio de Cegos"

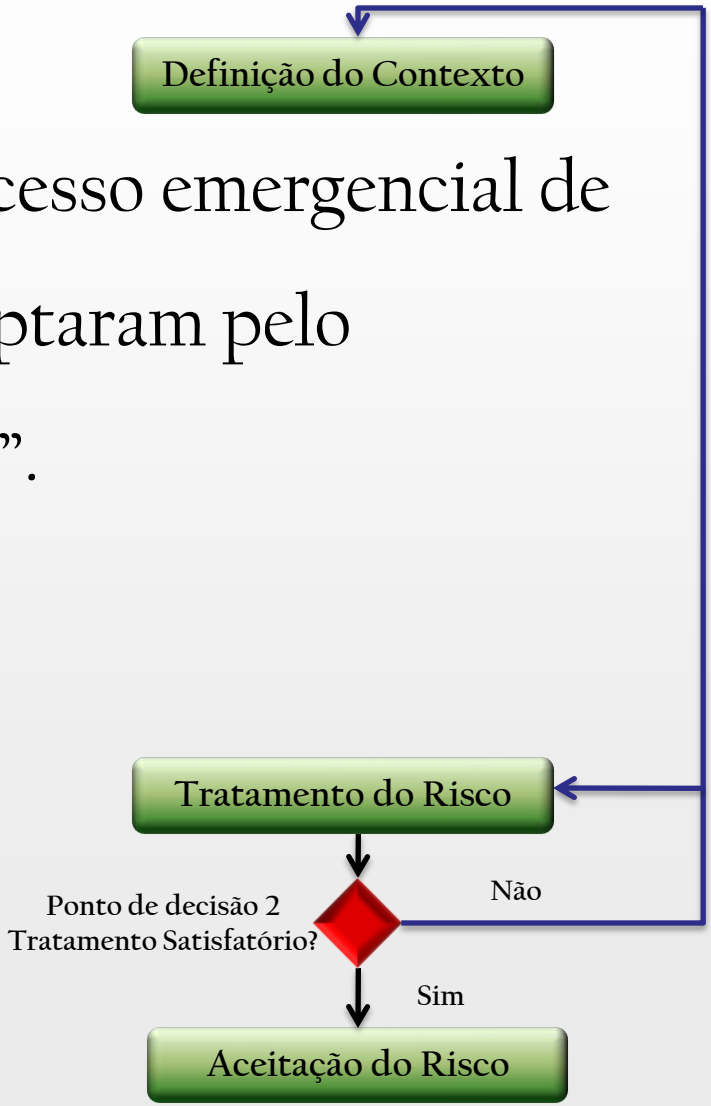
- Tratamento do risco
  - Substituir o Antivírus

Segurança Objetiva

"Tiroteio de Cegos"

- Tratamento do risco
  - Cada regional iniciou um processo emergencial de compra, sendo que algumas optaram pelo fabricante "y" e outros pelo "z".
- Tratamento não satisfatório

  Os novos antivírus não evitaram a propagação do vírus.



"A Arte da Guerra"

Conheça seu inimigo

Segurança Objetiva

"A Arte da Guerra"

- Redefinição do Contexto:
  - Uma regional resolveu manter o antivírus "x" e estudar o agente de ameaça: O vírus "Funlove";
  - Parque com milhares de estações Windows 95 e 98 compartilhando dados entre si sem controle de acesso adequado;
  - Vírus com características de "Worm" infectando executáveis através de compartilhamentos

"Tiroteio de Cegos"

- Análise/Avaliação:
  - Ameaça: perda de dados e indisponibilidade.
  - Controles existentes: Antivírus sem console de gerenciamento e considerado "medíocre" pela crítica
  - Vulnerabilidades: Compartilhamentos;
  - Alta probabilidade de novos vírus atacarem a mesma vulnerabilidade comum "payload" mais destrutivo.

"A Arte da Guerra"

- Plano de tratamento
  - Instalar um file server com Windows 2000 e proibir o compartilhamento de pastas em estações.
  - Alterar permissões NTFS em todos executáveis em pastas compartilhadas, deixando direito de escrita somente nos arquivos de dados. Ex: DBF

"A Arte da Guerra"

- Tratamento do risco
  - Instalação do File Server
  - Busca de compartilhamentos na rede
  - Transferência dos programas para o File Server
  - Atribuição de permissões NTFS adequadas
  - Monitorar compartilhamentos na rede
  - Palestra de conscientização

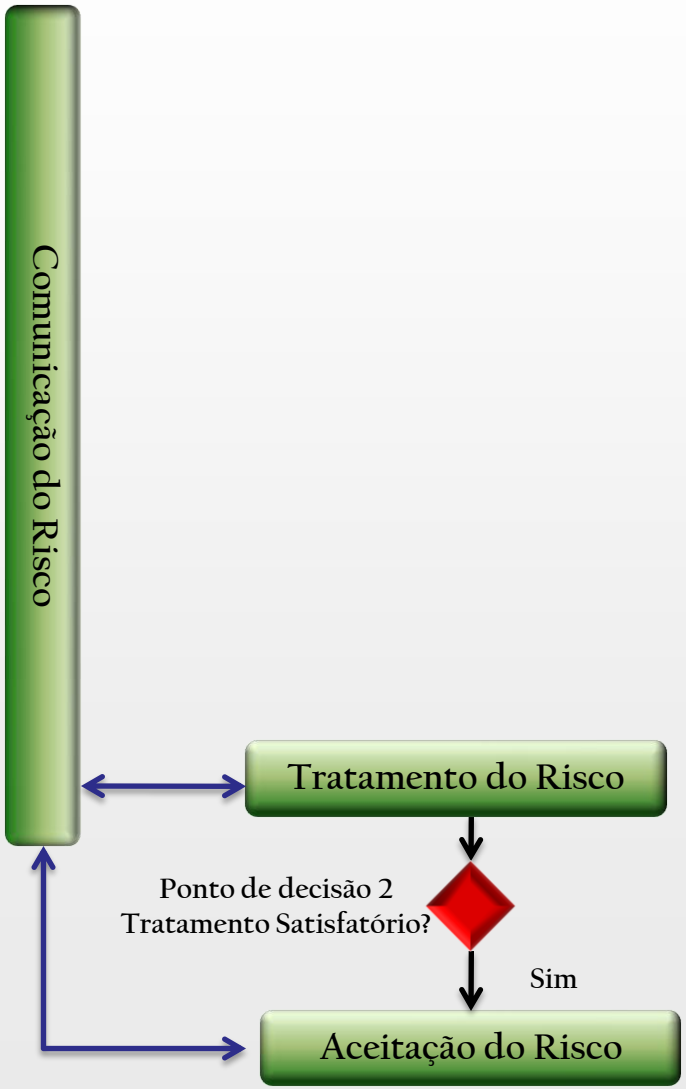
"A Arte da Guerra"

- Tratamento Satisfatório
  - A Regional conseguiu praticamente eliminar o vírus de suas estações, e apesar disso continuava a receber tentativas de infecção vindas de outras regionais
  - Solução foi replicada para outras regionais

Segurança Objetiva

"A Arte da Guerra"

- Aceitação do Risco
  - Risco Residual: Alguns usuários poderiam contrariar a nova política, compartilhar pastas em seu Windows, e ser infectado antes que a área de TI agisse.
  - O Risco foi considerado aceitável



Segurança Objetiva

Conclusão

Segurança
Objetiva

Conclusão

- Vírus poderia ser eliminado (eficácia) com custo muito menor (eficiência) se fosse feita uma análise de risco visando entender as ameaças e vulnerabilidades

- Após o tratamento adequado a organização ficou imune a vírus semelhantes porém mais agressivos como o "Ninda" e o "Sircan"

Dúvidas?

Fernando Fonseca
fernando@segurancaobjetiva.com

Segurança Objetiva