

# MBA EM GESTÃO EMPRESARIAL

## FOCO EM TECNOLOGIA DE INFORMAÇÃO



**UNIVERSIDADE FEDERAL FLUMINENSE**



## Gestão da Segurança da Informação

Prof. Fred Sauer, D.Sc.  
[contato@fredsauer.com.br](mailto:contato@fredsauer.com.br)

- Fred Sauer
  - Professor de MBA desde 1999
    - Redes de Computadores
    - Tecnologia Internet
    - Tecnologias Específicas e Emergentes
    - Gestão da Segurança da Informação
  - Security Officer da área de pesquisa estratégica da MB desde 1993
  - Membro da Comissão Permanente de Auditoria de SegInfo da MB desde 2001.

- Relacionamento de Segurança com o Negócio
- Visão Geral da ISO 27.001
- Definição da Política de Segurança
- Gerenciamento da Continuidade
- Gestão de Riscos de Segurança.

- Conceito de Risco e suas componentes
- Mensurabilidade do Risco
- Gestão do Risco
- Elementos para identificação de riscos
- Atributos da Informação
- *Security Office* e FSI (ou CGSI)
- Plano de Continuidade (PAC, PCO e PRD)
- Política de Segurança (Diretrizes, Normas e Procedimentos).

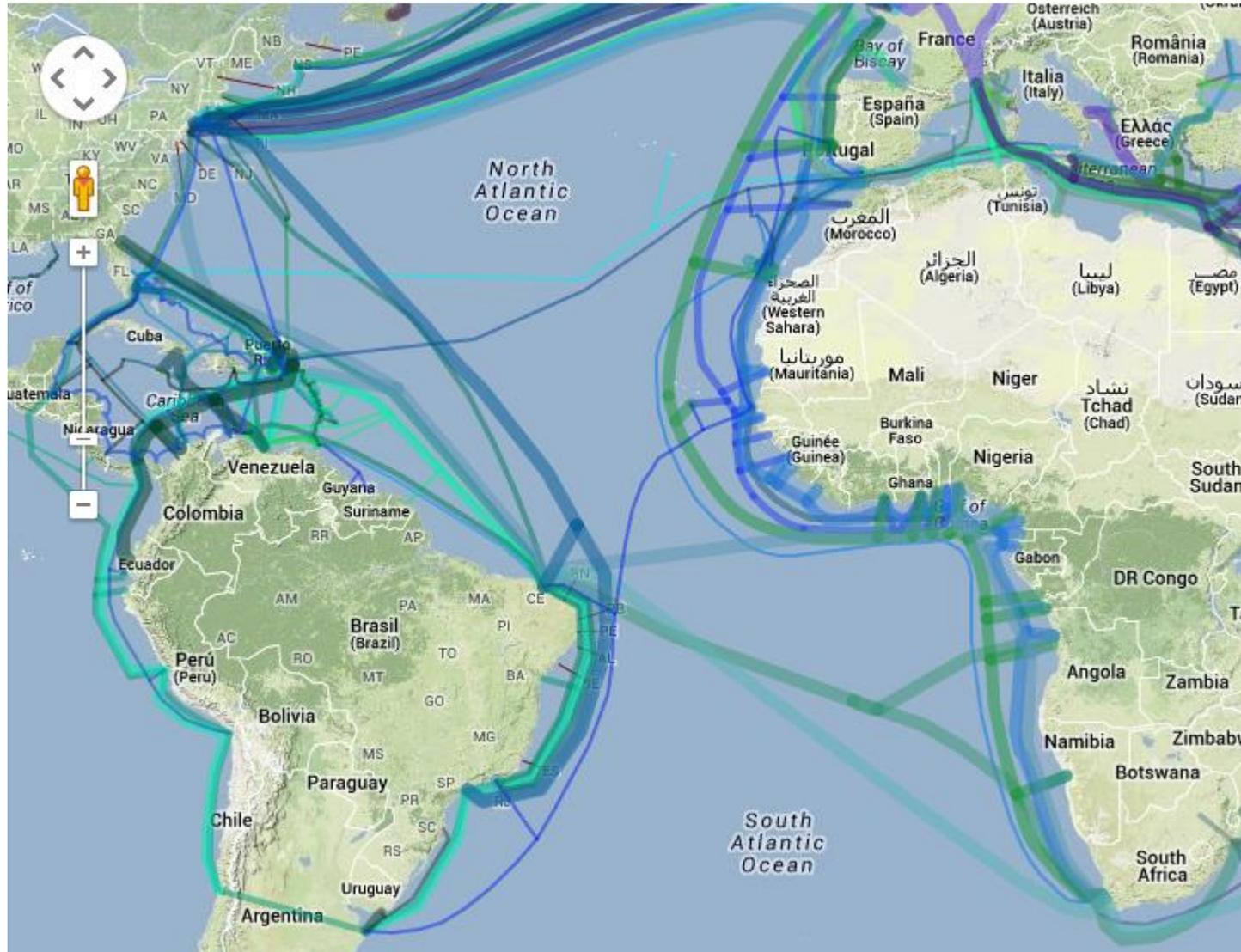
# Segurança é a palavra da moda...



- Palavras-chave:
  - Edward Snowden
  - NSA, FBI, CIA
  - Prism



# Como eles conseguem ?



TOP SECRET//SI//ORCON//NOFORN

Gmail

facebook

Hotmail

YAHOO!

Google



skype

paltalk.com

You Tube

AOL mail

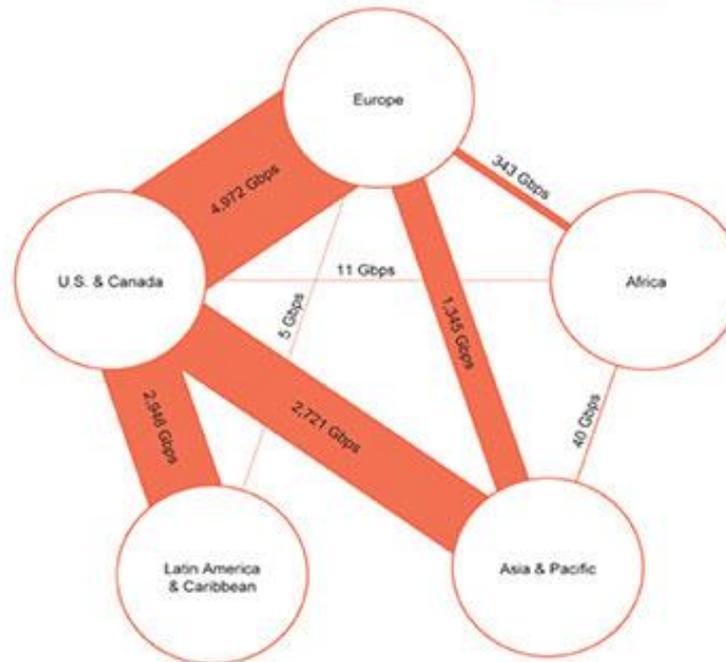


## (TS//SI//NF) Introduction

*U.S. as World's Telecommunications Backbone*



- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.

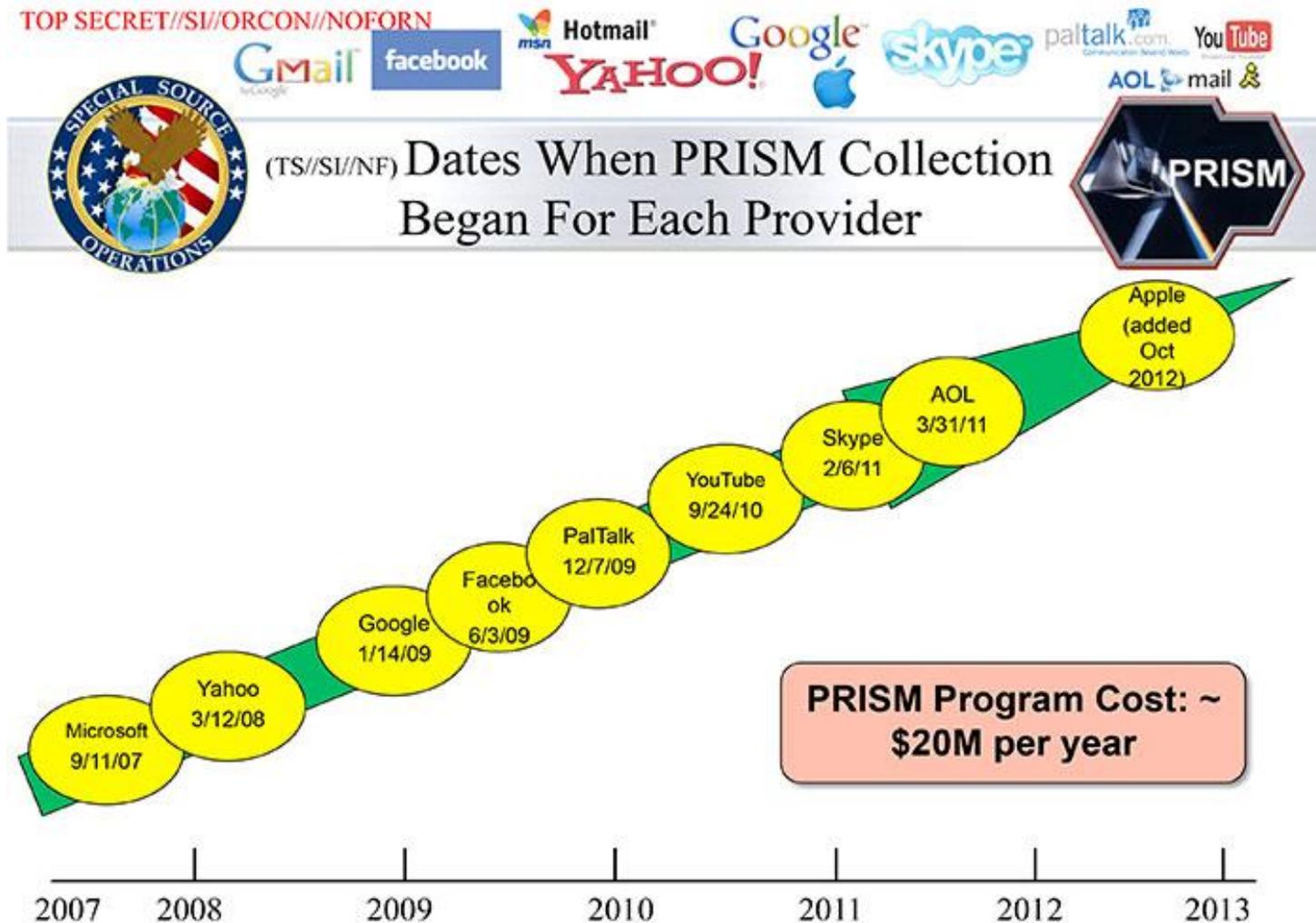


International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

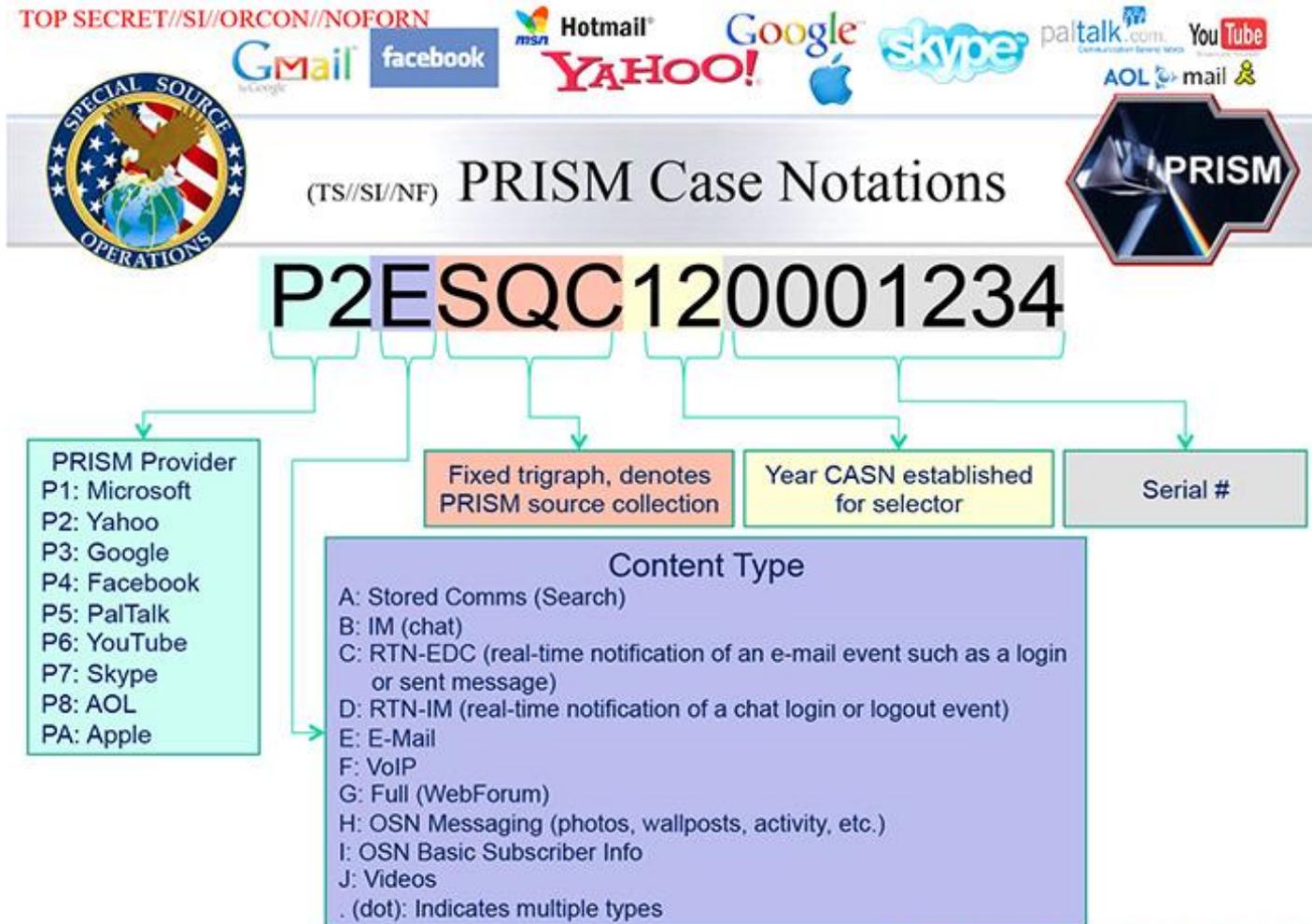
TOP SECRET//SI//ORCON//NOFORN

# Quando começaram ?



TOP SECRET//SI//ORCON//NOFORN

# O que eles veem ?



TOP SECRET//SI//ORCON//NOFORN

# Mas estamos Surpresos !



Editorias | Economia | Sua região | Na TV | Serviços | VC no G1 | Princípios editoriais

02/09/2013 16h44 - Atualizado em 03/09/2013 11h42

## Violação da soberania brasileira pelos EUA é 'inaceitável', diz governo

Brasil quer resposta por escrito do governo dos EUA em uma semana. Cardozo e Figueiredo não quiseram responder se Dilma viajará aos EUA.

Priscilla Mendes  
Do G1, em Brasília

1060 comentários | [Tweeter](#) 92 | [Recomendar](#) 1,3 mil



José Eduardo Cardozo (Justiça) e Luiz Figueiredo (Itamaraty) em coletiva sobre espionagem dos EUA (Foto: Valter Campanato/ABr)

## Por que os Estados Unidos espionam o Brasil (ou: como você não pensou nisso antes?)

[Tweeter](#) 24 | [Curtir](#) 184 | [Submit](#) | [Share](#) 1 | [+1](#) 10

Postado em 28 set 2013 por : Kiko Nogueira



14/10/2013 16h45 - Atualizado em 14/10/2013 17h35

## Novo sistema de e-mails vai 'livrar governo da espionagem', diz Serpro

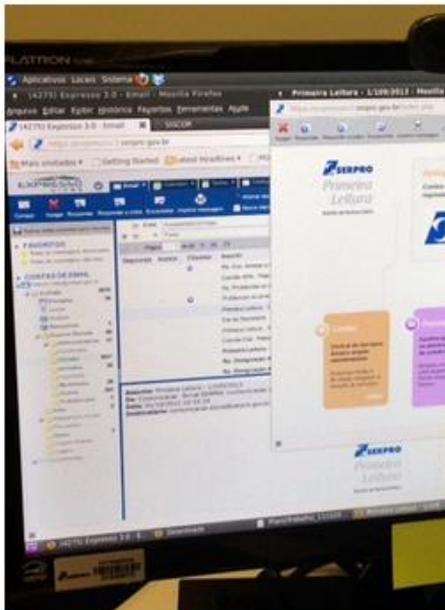
Segundo presidente do órgão, toda tentativa de invasão será identificada. Tecnologia deverá ser instalada na Presidência em novembro deste ano.

Nathalia Passarinho  
Do G1, em Brasília

345 comentários

Tweetstar 156

Recomendar 1,9 mil



Tela de e-mail protegida pelo software Expresso V3, desenho Passarinho/G1

## Petrobras vai investir R\$ 21 bi em segurança

- Cifra supera valor destinado à exploração do pré-sal até 2017

Recomendar 14

Tweet 6

+1 0

Enviar

MÔNICA TAVARES (EMAIL)

Publicado: 18/09/13 - 22h23 Atualizado: 18/09/13 - 23h01

BRASÍLIA - A Petrobras vai investir R\$ 21,2 bilhões (equivalente a US\$ 9,2 bilhões) em segurança da informação entre 2013 e 2017, sendo R\$ 3,9 bilhões este ano. O valor total é uma vez e meia os US\$ 5,8 bilhões que a estatal investirá na exploração do pré-sal no período. A maior parte destes recursos será investida no centro de dados da empresa, que funciona no Rio. Nele estão guardados os principais dados e aplicações da companhia, "o conhecimento explícito da empresa", disse a presidente da Petrobras, Graça Foster, que participou nesta quarta-feira de audiência no Senado. As informações críticas são armazenadas com criptografia.

02/09/2013 18h46 - Atualizado em 02/09/2013 18h54

## Correios podem ter e-mail gratuito e criptografado, diz ministério

Serviço dificultaria espionagem como a feita pelo governo dos EUA. Estatal pode financiar projeto por meio de venda de anúncios.

Tweetstar 175

Recomendar 744

o ministro das Comunicações, Genildo Lins, disse nesta segunda-feira (2) que o projeto de criação de um serviço público e gratuito de e-mail que contaria com criptografia para dificultar a espionagem como a realizada pelo governo dos Estados Unidos.

A ideia de criar o serviço foi discutida em uma reunião que aconteceu antes de o ministro viajar para os Estados Unidos. Lins disse que brasileiros têm mensagens de e-mail e informações telefônicas armazenadas nos servidores dos Estados Unidos.

mail não é dos EUA

ira pelos EUA

quer sistema

O objetivo dos Correios, disse ele, é criar uma certificação digital, serviço pago que funciona como uma espécie de carimbo que garante a veracidade de documentos enviados pela internet. Para proteger esses documentos, a estatal quer criptografá-los. Num passo seguinte, a mesma tecnologia poderia ser utilizada para oferecer e-mail gratuito à população.

# Relação da Segurança com o Negócio

- Riscos de TI são tratados como Riscos ao Negócio
- Riscos de TI então devem ser expressos pelos impactos causados aos objetivos do negócio e a estratégia do negócio
- O ponto de partida é entender o significado de risco e a importância da informação para o negócio.

- Instrumento declaratório do comprometimento da direção em apoiar a Segurança da Informação
- Para que isso aconteça, é necessário um trabalho preliminar para:
  - Provar que o investimento é necessário
  - Alinhar os objetivos e prioridades com o negócio
  - Esclarecer os papéis e responsabilidades de todos.

- Por quê investir em Segurança ?
- Qual é o significado de Risco ?

## – RISCO

- Vulnerabilidades
- Ameaças
- Impactos

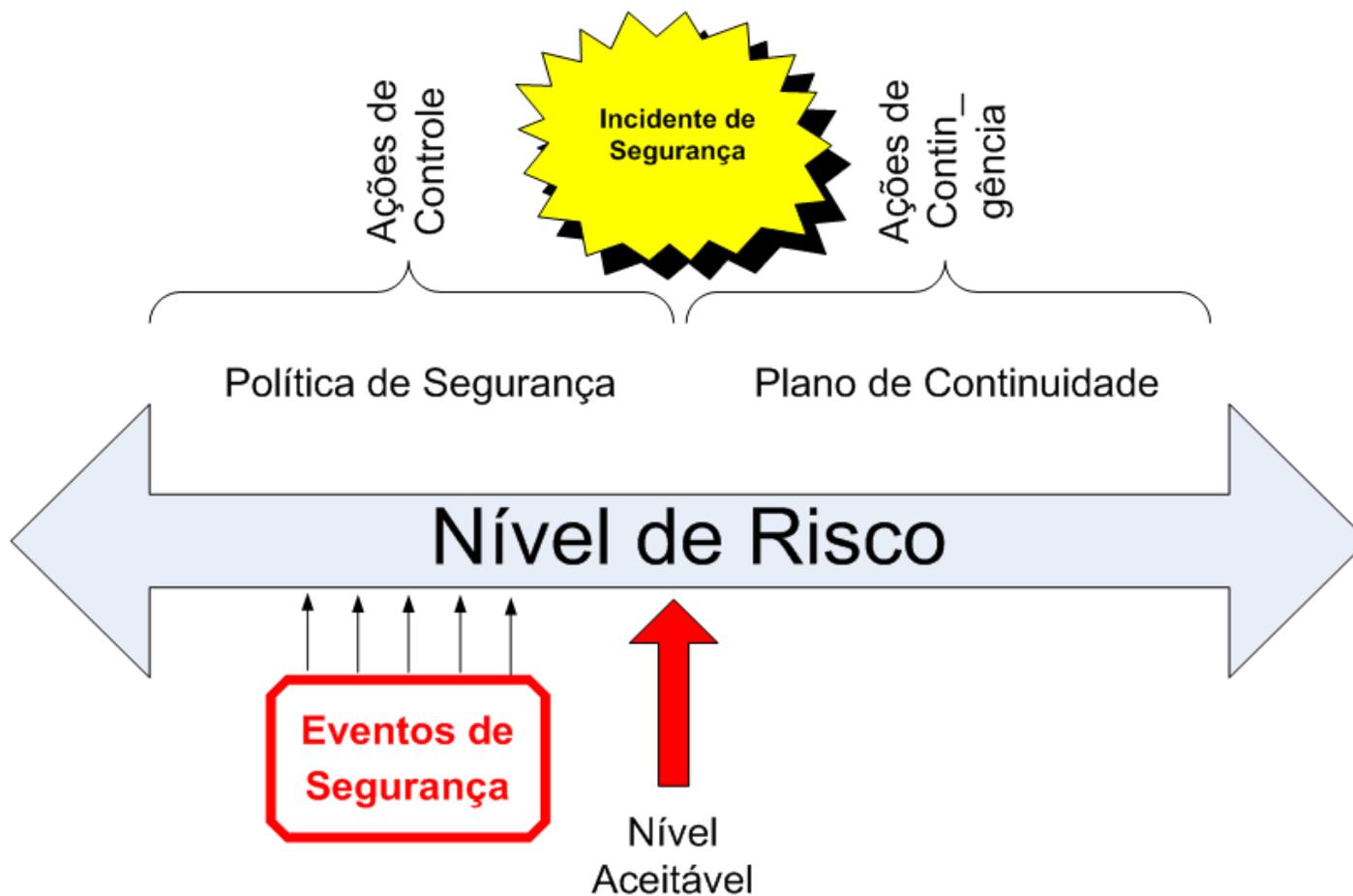
$$R = \frac{V \times A \times I}{M}$$

## – CONTROLES (Variável M – Mecanismos)

- Mecanismos para controlar o Risco, de acordo com uma estratégia .

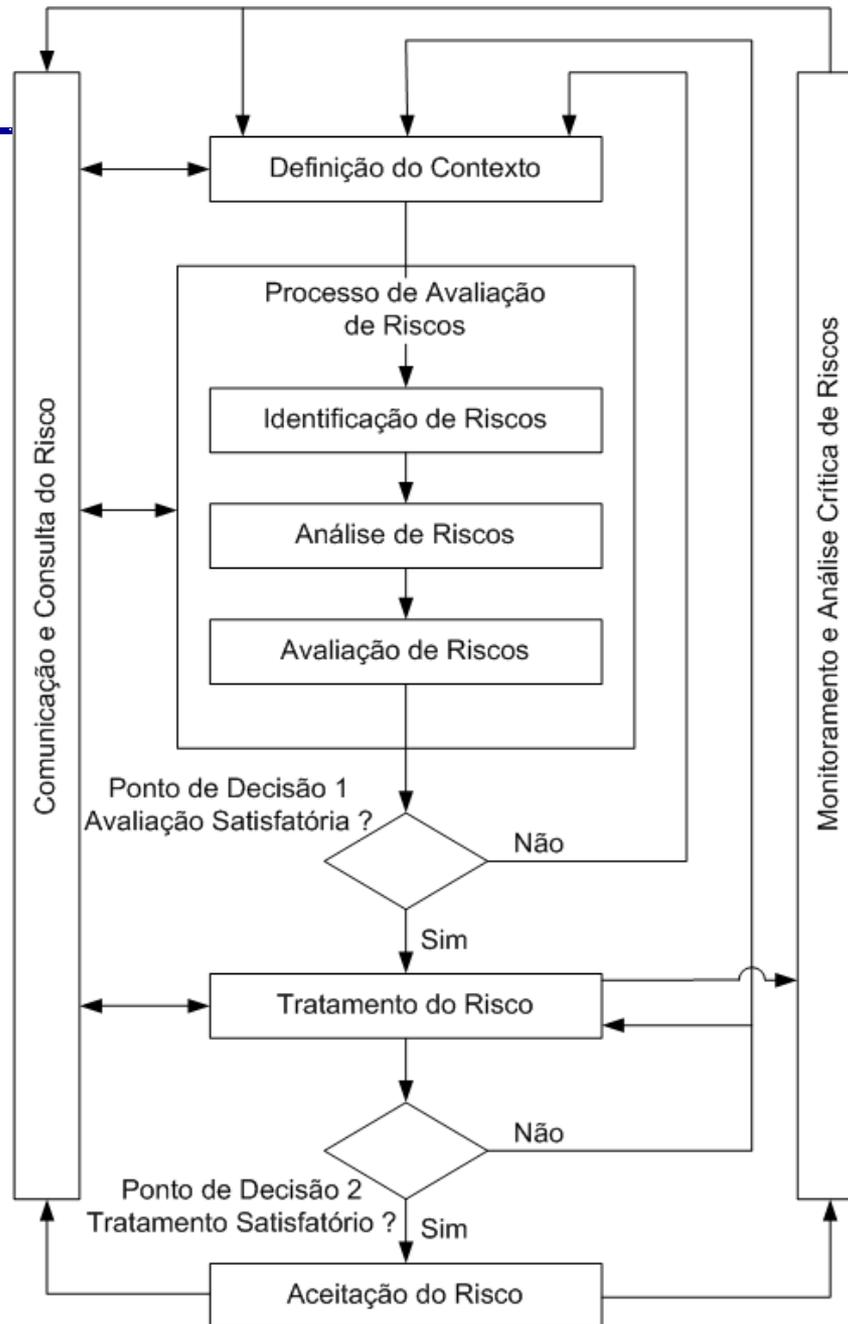
- O que são vulnerabilidades ?
- O que são ameaças ?
- Quão impactante pode ser um Incidente de Segurança ?
- Como podemos controlar este risco ?

# Desafio da Gestão do Risco



- Uma das mais críticas fases da definição do SGSI, deve expressar claramente qual é o limite de impacto aceitável pela direção
- Fatores a considerar:
  - Requisitos do negócio, legais e regulamentares
  - Aspectos operacionais e tecnológicos
  - Aspectos financeiros
  - *Branding*
  - Aspectos sociais e humanitários.

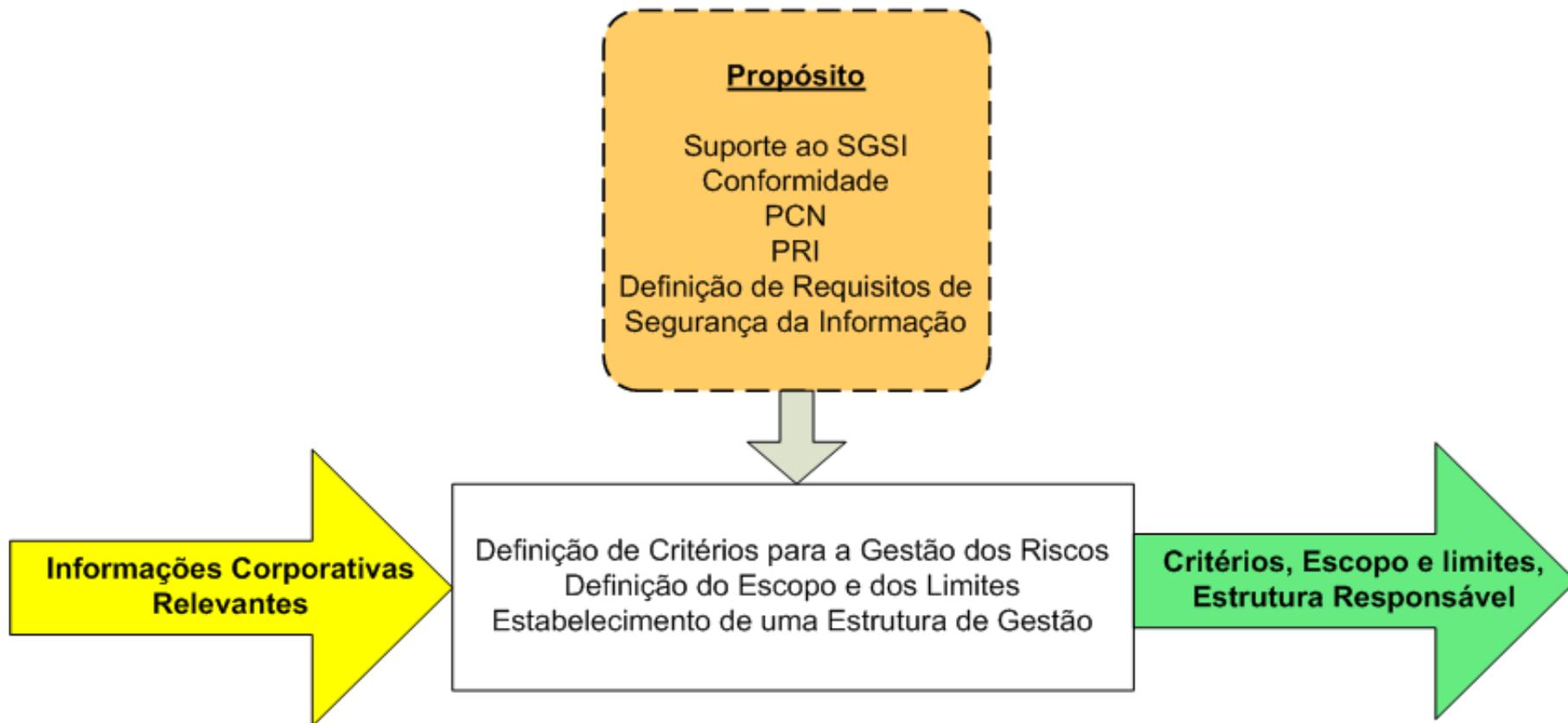
# ISO 27005 Risk Management



# PDCA do Risco

Processo do SGSI	Processo de Gestão de Riscos de Segurança da Informação
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

# Definição do Contexto



- Identificação dos Riscos
  - Ameaças e Vulnerabilidades → Probabilístico
  - Impactos
- Análise dos Riscos
  - Qualitativa ou Quantitativa
- Avaliação dos Riscos
  - Comparação dos riscos evidenciados com os critérios de Aceitação de Riscos.

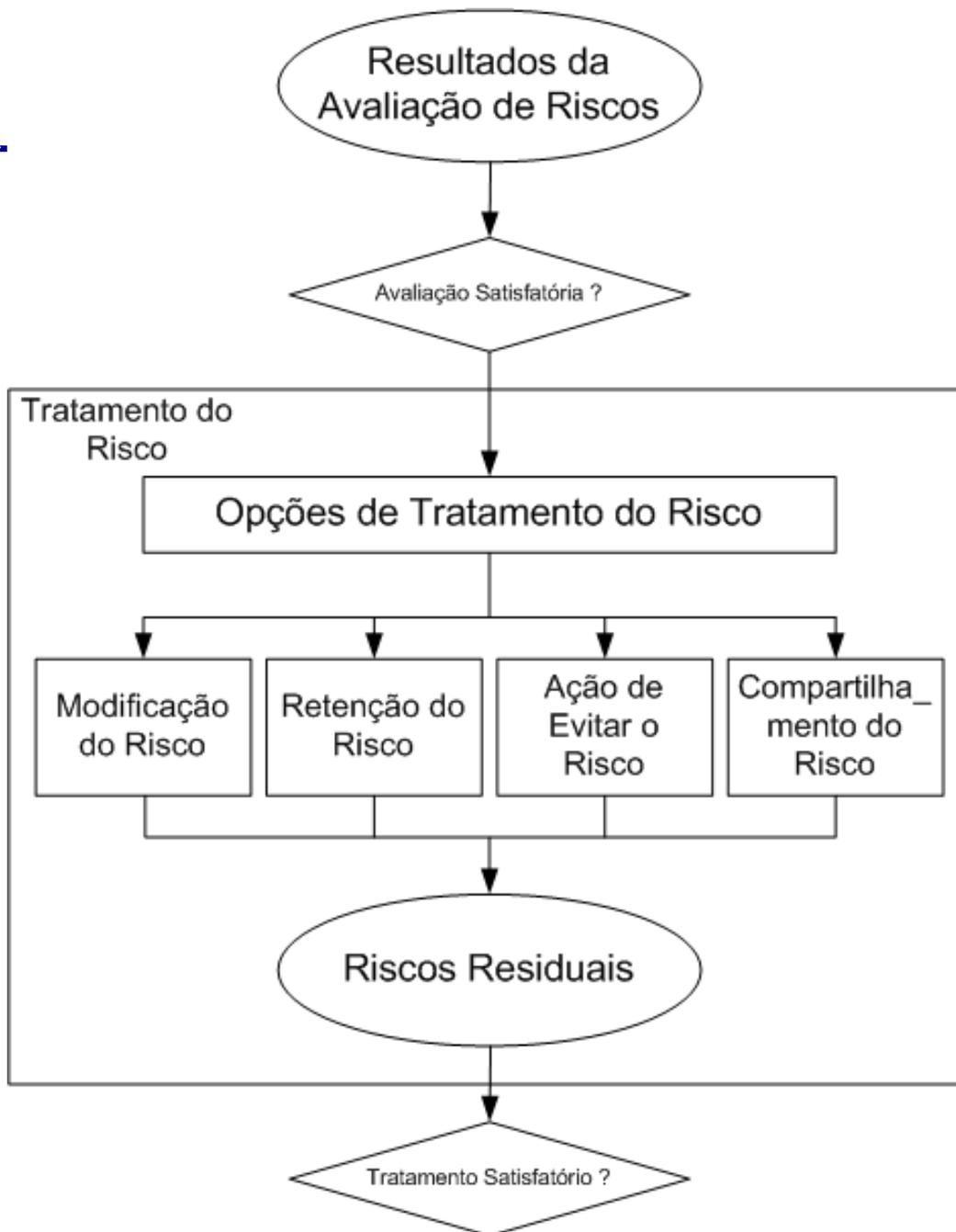
- Critérios para Avaliação
  - Valor estratégico do processo
  - Criticidade dos Ativos
  - Requisitos Legais e Regulatórios
  - Importância da CID para o negócio
  - Expectativas dos stakeholders e a imagem.

# Caso

- Arbitrar critérios qualitativos para aceitação de risco
- A Análise de Riscos será feita após a análise CIDADAL, GUT e BIA

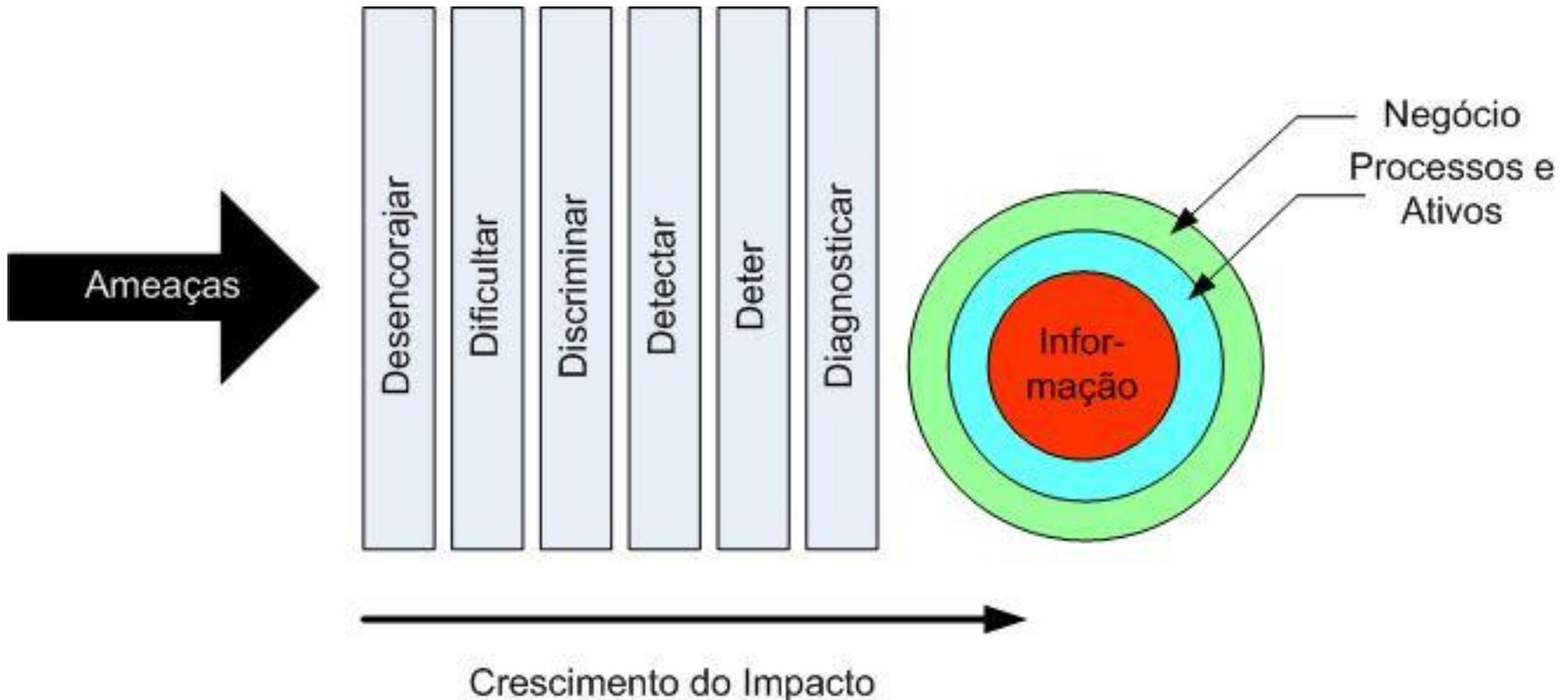
- Para o caso, considerar que o processo “Loja Virtual” é o principal da empresa em questão, representando a maior parcela do faturamento; e
- Considerar também que a imagem da empresa junto aos clientes é estrategicamente prioritária, de forma que a confidencialidade dos dados dos clientes deve ser protegida.

- Traduza as orientações dadas pelo negócio em frases objetivas, passíveis de serem usadas para a avaliação de um risco quanto a sua aceitabilidade
- Exemplo (qualitativo): Os impactos decorrentes de um incidente de segurança não devem comprometer o faturamento da empresa de forma a provocar o seu endividamento
- Exemplo (quantitativo): Os impactos decorrentes de um incidente de segurança não devem ultrapassar o limite de R\$ 100.000,00 em um único mês.



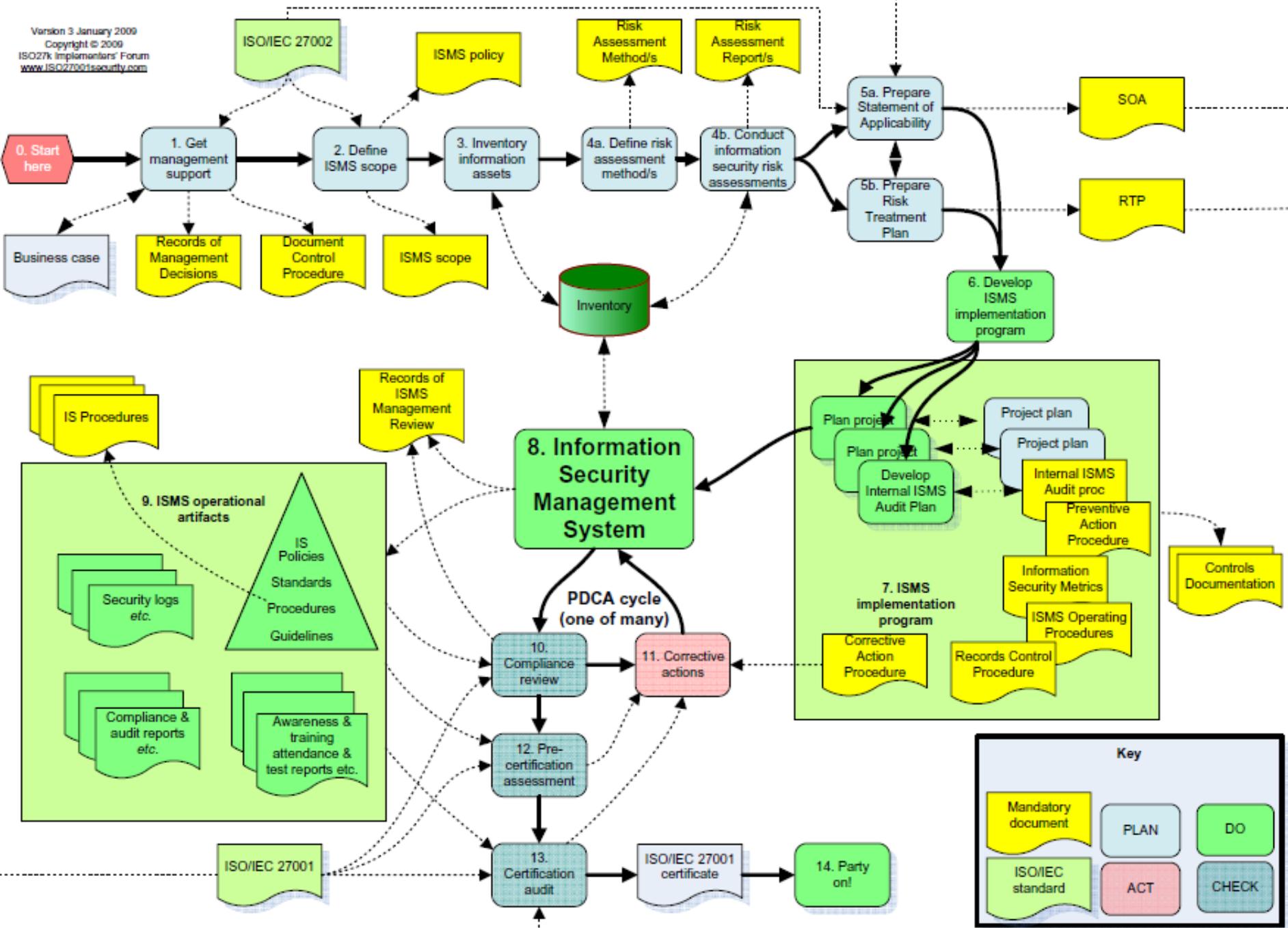
## Tratamento dos Riscos

- Modificação do Risco
  - Inclusão, exclusão ou alteração de controles



- Retenção do Risco
  - Controles já adotados satisfazem aos critérios
- Ação de Evitar o Risco
  - Quando os Riscos são muito altos e os custos dos controles são inexequíveis, com a eliminação da atividade (todo ou parte) ou a mudança nas condições de operação
- Compartilhamento do Risco
  - Repasse da atividade para uma entidade externa que possa gerenciá-la com risco aceitável
  - Pode criar novos riscos e não exime de questões legais.

- Define os Requisitos para Sistemas de Gestão da Segurança da Informação
- Propõe uma mudança radical na forma atual de implementar SegInfo, normalmente atrelada exclusivamente à TI da empresa
- Visa garantir a Confidencialidade, Integridade e Disponibilidade da informação, de forma a preservar os ativos e o negócio da empresa.

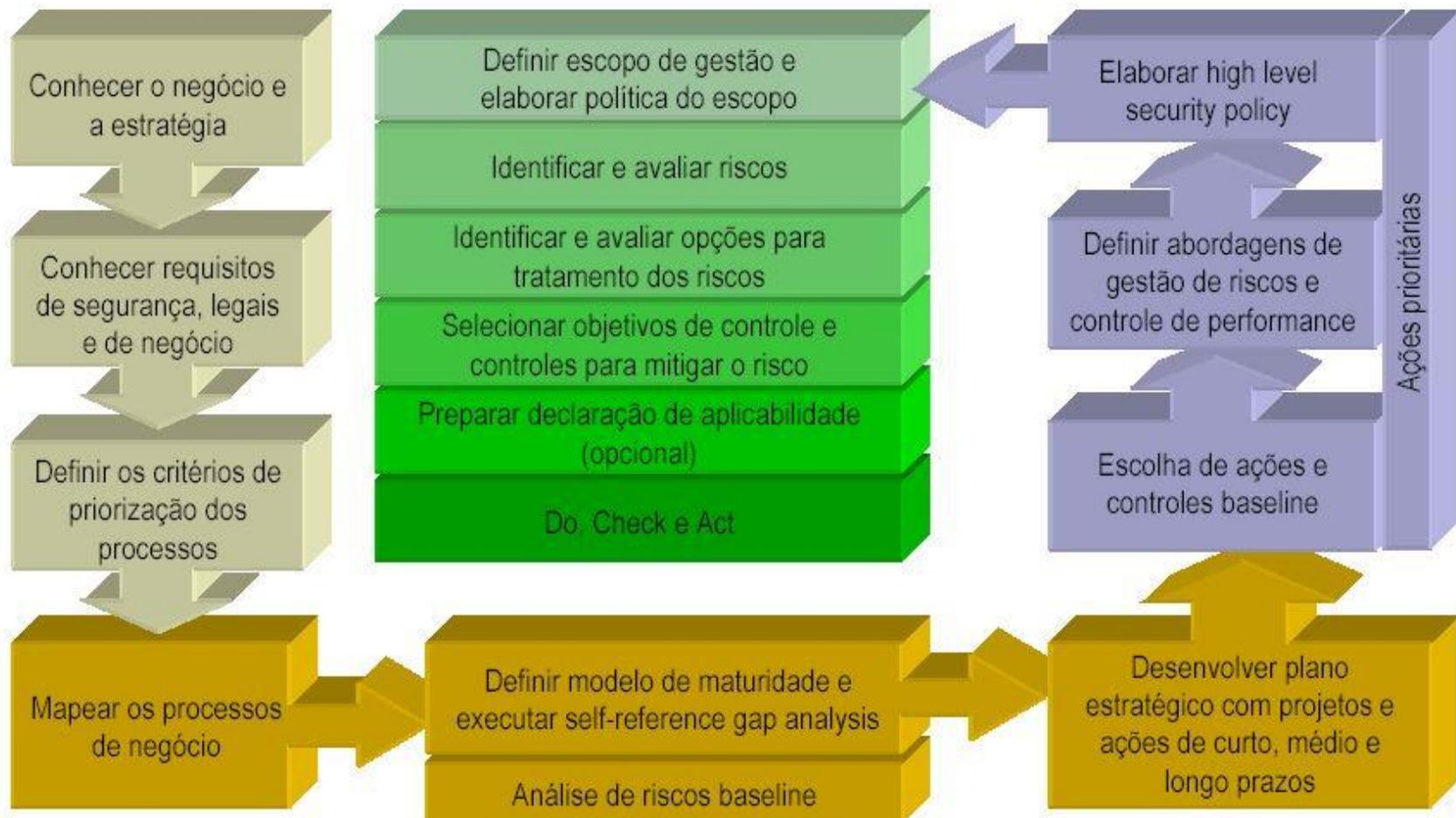


**Key**

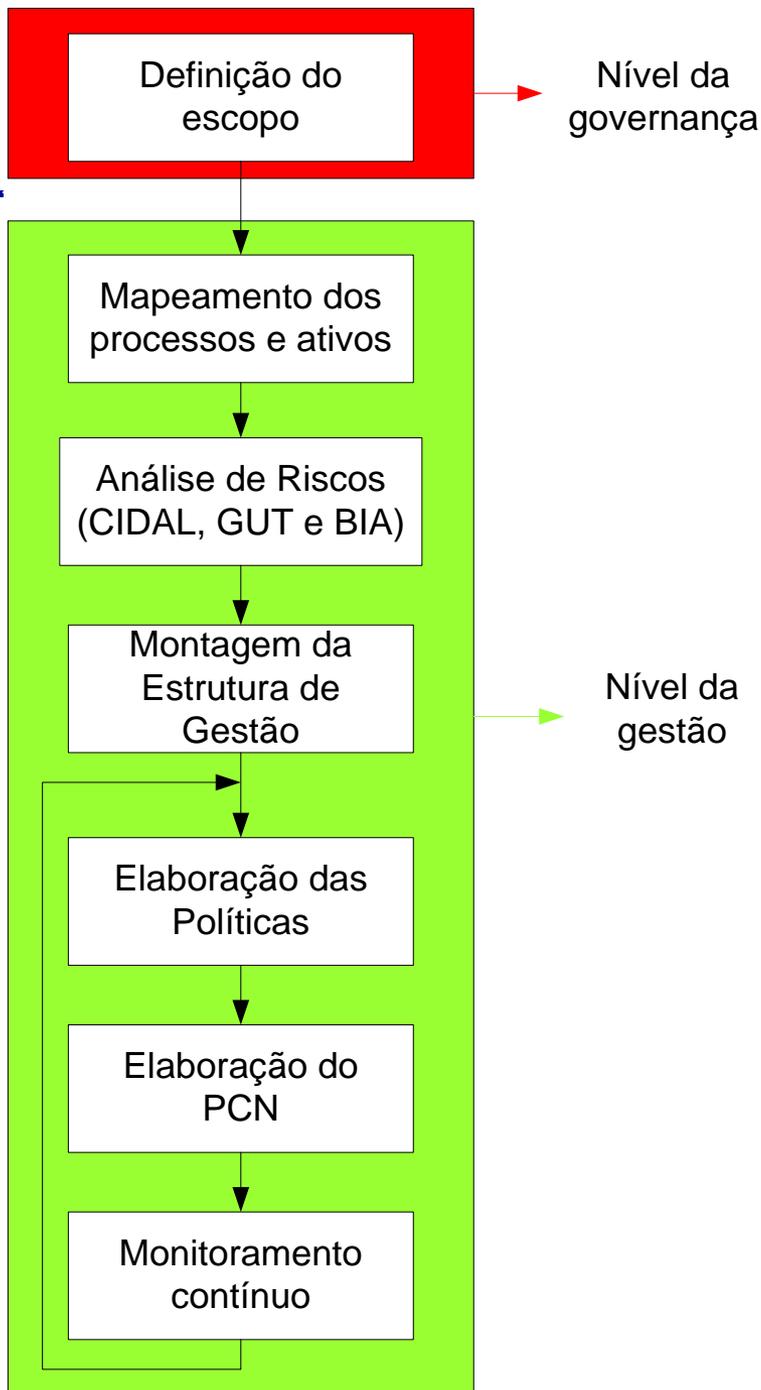
Mandatory document	PLAN	DO
ISO/IEC standard	ACT	CHECK

# Proposta de Trabalho

## Visão funcional Planejamento Estratégico



- Metodologia prática:
  - Comportamento humano típico
    - Adere apenas ao que concorda
    - Concorda com o que lhe dê vantagens
    - Reage a mudanças abruptas, mas se adapta a novos ambientes que lhe pareçam favoráveis
  - Passo-a-passo metodológico:
    - Conhecimento
    - Envolvimento
    - Comprometimento.



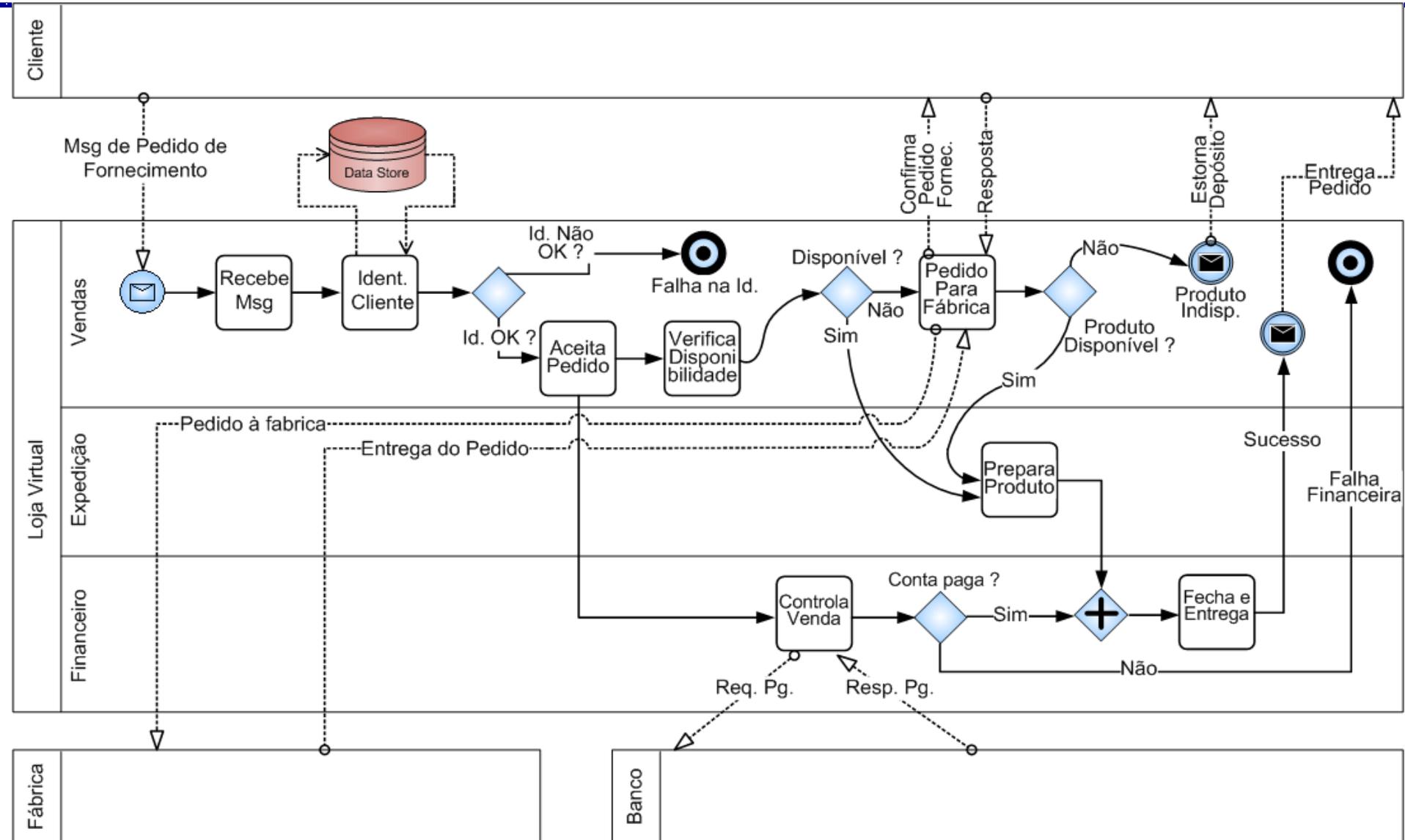
- Visão Holística do Risco
- Identificação de Influências entre processos
- Orientação básica:
  - Evitar a visão míope
  - Foco na Informação
  - Ilustrada pelos gestores (a situação “real”, e não “a desejada”).

- Isolar o fluxo de informações
- Identificar dependências funcionais entre os Processos
- Ferramenta de verificação de conformidade com a realidade
- Identificar pontualmente os gaps de risco.

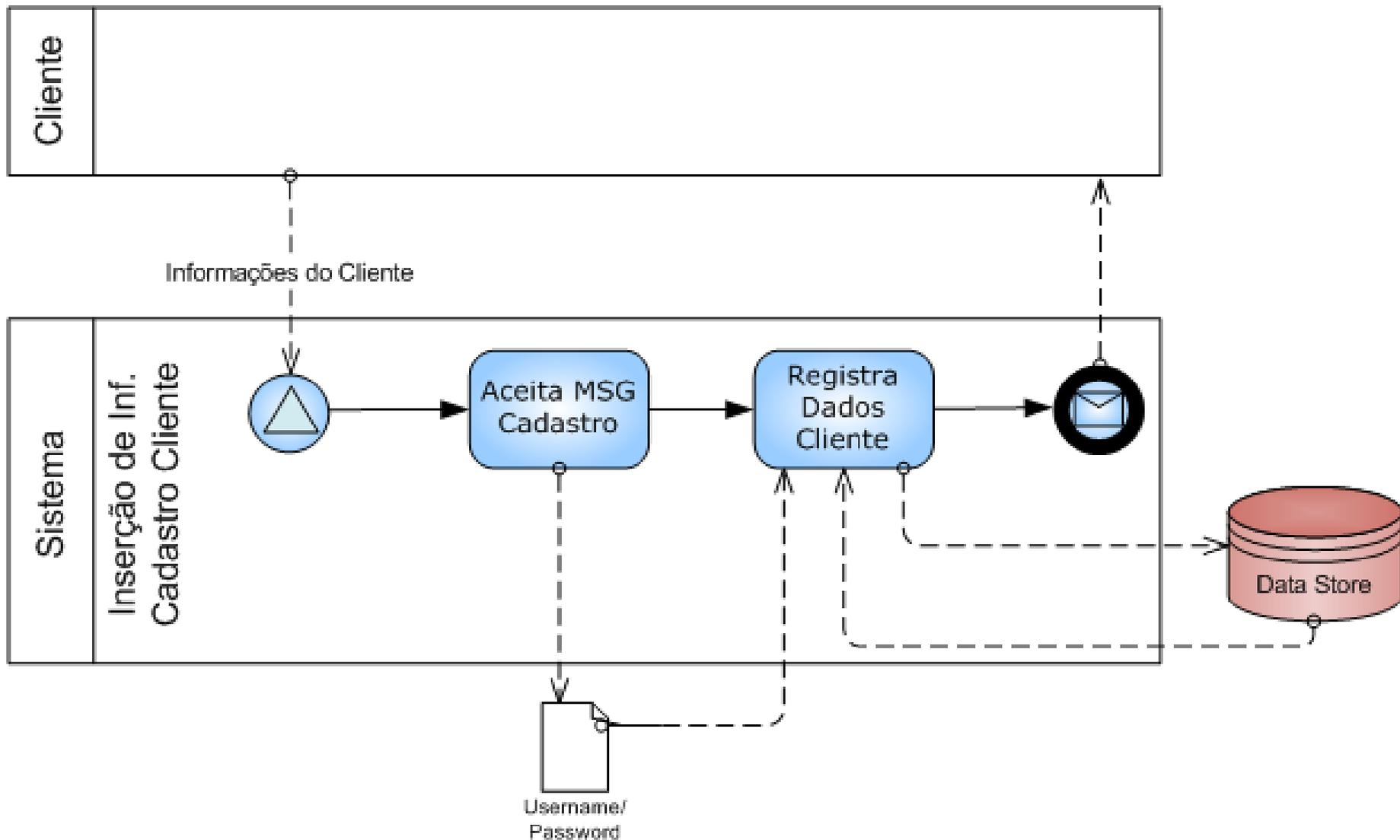
# Caso

- Compreender o mapeamento do Processos de Negócio.

# Processo de Pedido de Fornecimento



# Processo de Cadastro de Cliente



# Segundo Passo

- Mapeamento de Ativos
  - Significado de Ativo
  - Taxonomia
    - Físicos
    - Tecnológicos
    - Humanos.

# Segundo Passo

- Ciclo de Vida da Informação
  - Manipulação
  - Armazenamento
  - Transporte
  - Descarte.

# Objetivo desta etapa

- A correlação entre os ativos, informações e fase o ciclo permite:
  - Identificar controles apropriados à natureza do ativo
  - Planejar treinamentos apropriados
  - Proteger a informação em todo o seu ciclo de vida, através dos ativos
  - Evitar investimentos inadequados para os reais riscos.

- Elaboração do quadro de ativos para o Estudo de Caso

Ativo	Tipo	Fase Ciclo	Informações
BD	Tecnológico/Físico	Armazenamento	Cadastro Clientes, estoque, lista de preços

Escolha um ativo físico e um humano, com suas respectivas fases do ciclo de vida e informações sensíveis relacionadas.

# Terceiro Passo: Análise de Riscos

## Baseline



- Principais Riscos
  - Casos Reais já ocorridos
  - Estatísticas com empresas semelhantes
  - Observação especialista
- Busca o envolvimento.

# Objetivos da Análise de Riscos

## Baseline



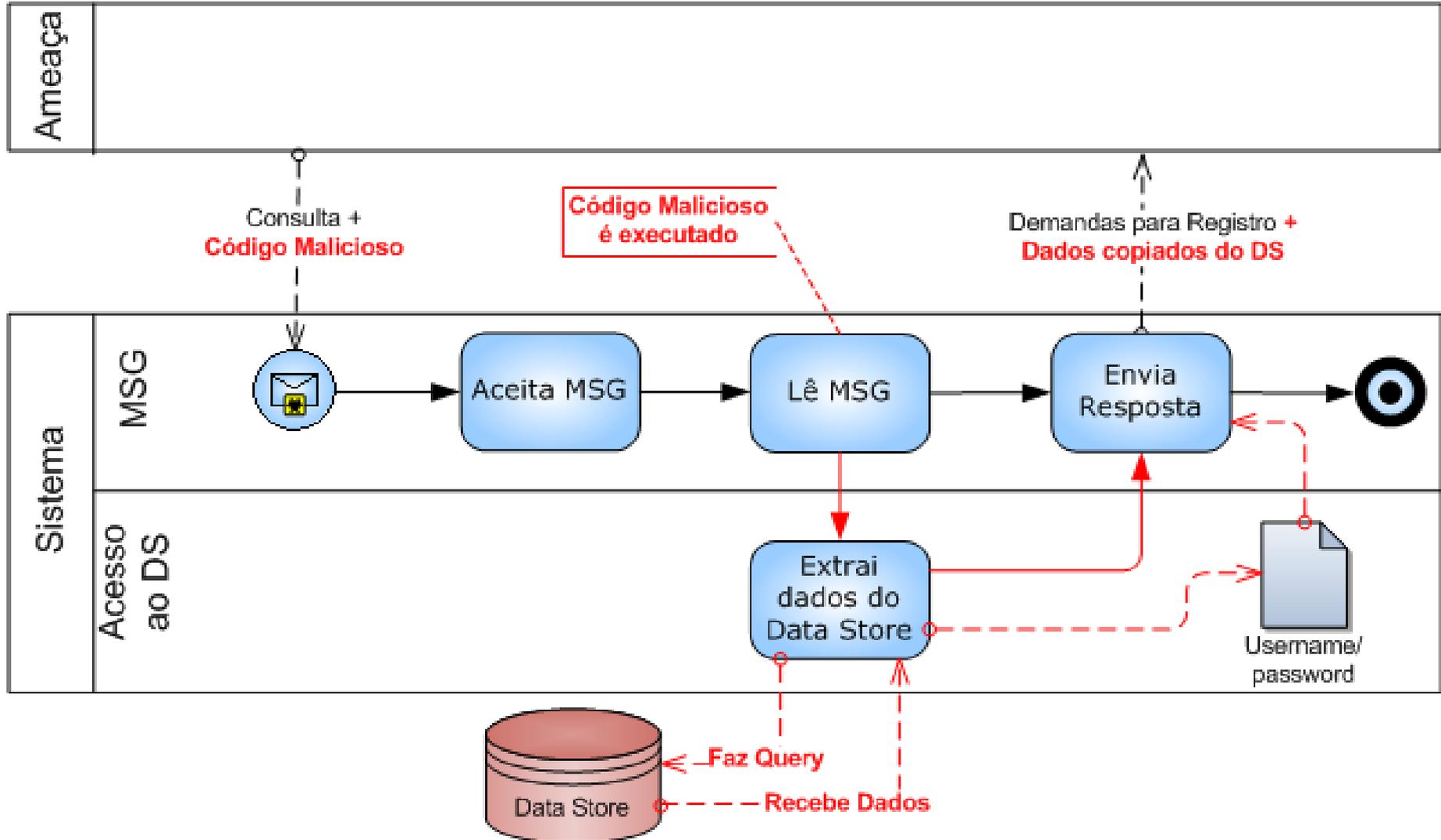
- Incidentes já ocorridos tem grande probabilidade de voltar a ocorrer
- Ainda não conhecemos o problema o suficiente
- A aderência à Política será favorecida pelo envolvimento
- Inicia-se um processo de aculturamento.

- Análise de Riscos *baseline* do Estudo de Caso
- Destacar 3 situações de risco, incluindo a evidenciada pelo gestor da TI (ataque cibernético com roubo de informações)

Vulnerabilidade	Ameaça	Possíveis Impactos
Código vulnerável	Hacker	Roubo de dados do BD

Para os ativos que você indicou na fase anterior, identifique situações de risco visíveis, através das vulnerabilidades de cada ativo e ameaças que podem explorá-las. Indique impactos qualitativos relacionados com os critérios de aceitação do risco estabelecidos no primeiro passo.

# Processo de Cadastramento sob Ataque



# Análise CIDAL

- Agora que se sabe o que proteger (vulnerabilidades), e do que proteger (ameaças), e já evidenciei riscos, O QUE devo priorizar ?
- Níveis diferentes de SENSIBILIDADE dentro de cada requisito permitem direcionar as ações de forma prioritária.

# Quarto Passo: Avaliação da Sensibilidade



- Atributos da Informação (CIDAL)
  - Confidencialidade
  - Integridade
  - Disponibilidade
  - Autenticidade
  - Legalidade.

# Caso

- Com a tabela de métricas fornecida, fazer o CIDAL para o Estudo de Caso
- As métricas devem ser construídas para atender os seguintes requisitos:
  - Foco na continuidade do negócio
  - Permitir uma comparação objetiva entre os processos, explorando a maior facilidade da avaliação qualitativa

# CIDAL

	C	I	D	A	L
Ataque cibernético	3	3	5	3	3

Para os ataques que você identificou na fase anterior, atribua pontuações para cada atributo da informação que pode ser comprometido, em função da intensidade do impacto decorrente. Use as definições da tabela do próximo slide

# Métricas para o Estudo de Caso

Nível	Enquadramento
<b>1 - Não Considerável</b>	A ocorrência de um incidente de segurança (IS) neste PN é absorvida integralmente através de um Plano de Continuidade sem prejuízo algum à atividade produtiva, de acordo com os critérios de aceitação do risco
<b>2 - Relevante</b>	A ocorrência de um IS no PN em análise demanda ações reativas programadas com redução da capacidade produtiva, podendo causar impactos de intensidade moderada, como pequenos atrasos ou prejuízos financeiros absorvíveis, de acordo com os critérios de aceitação do risco
<b>3 - Importante</b>	Um IS no PN em avaliação demanda ações reativas programadas com redução da capacidade produtiva, podendo causar impactos de intensidade média, causando prejuízos diários. Demanda redirecionamento de recursos para que a extensão de seus impactos não afetem outros PN da empresa e metas da empresa. Fica no limiar dos critérios de aceitação de risco.
<b>4 - Crítico</b>	Os impactos de um IS são de intensidade alta e podem ser percebidos em vários PN, demandando iniciativas reativas não previstas anteriormente, causando a necessidade de esforços adicionais e redução da capacidade produtiva de toda ou grande parte da empresa. Compromete metas. A ausência ou demora na reação pode transformar o evento em vital. Ultrapassa o limite de aceitação do risco.
<b>5 - Vital</b>	A ocorrência de um IS deste tipo no PN em análise pode atingir toda a empresa, clientes e parceiros, causando impactos possivelmente irreversíveis e demandando ações emergenciais <i>ad-hoc</i> que envolvem desde o setor estratégico até o operacional. Se persistente, pode provocar a falência da empresa. Está bem acima do limite de aceitação do risco.

- Ferramenta GUT
  - Usa os resultados da fase anterior
  - Agrega sensibilidade temporal em crise e na evolução do negócio
  - Permite maior priorização usando a multiplicação dos índices (no CIDAL é a média).

- Usando a tabela abaixo, elaborar o GUT do Estudo de Caso, e em seguida faça a Avaliação do Risco

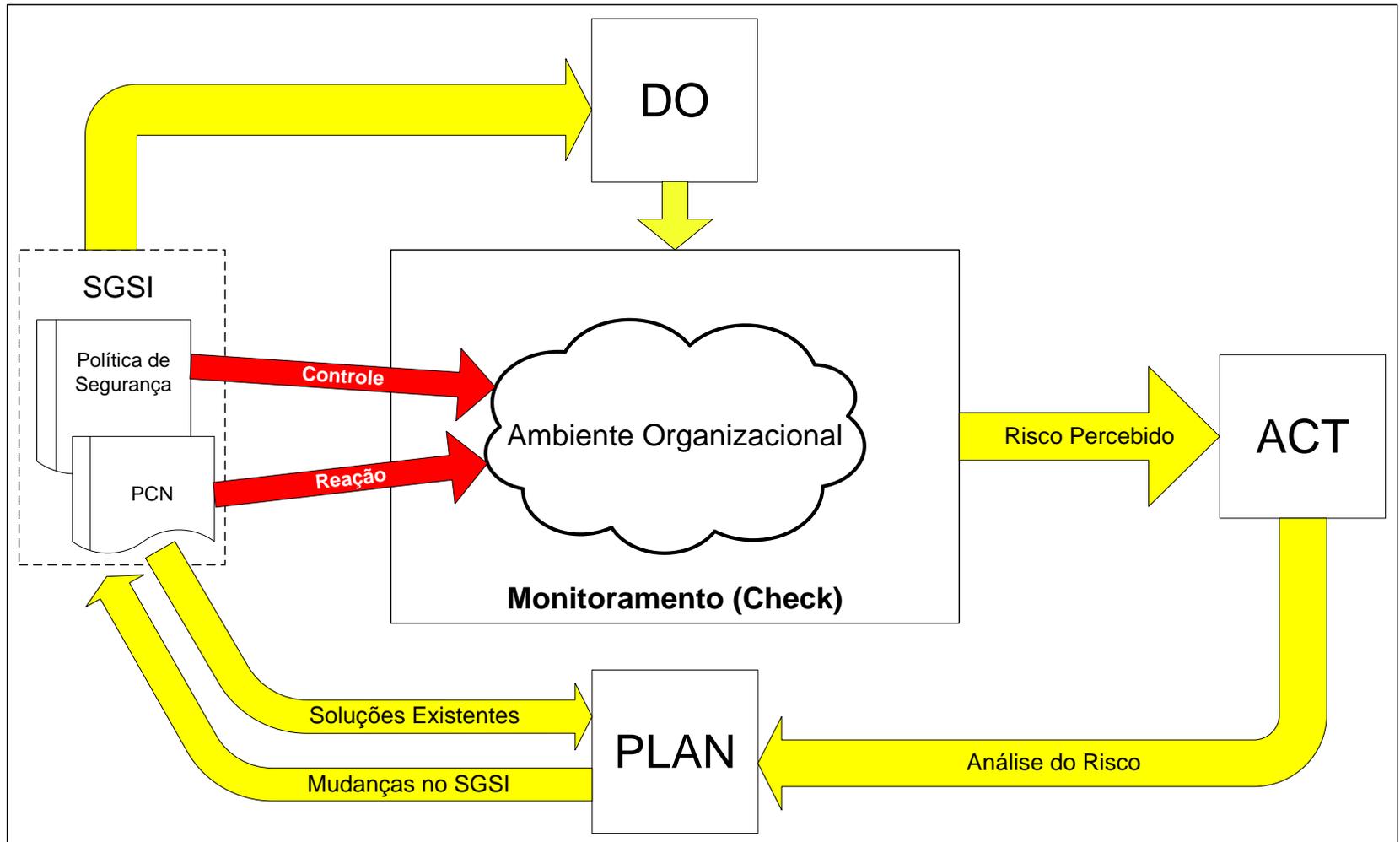
Nível	Gravidade*	Urgência**	Tendência***
1	$1 \leq C \leq 2,3$	Alta tolerância	Sem previsão de mudança
2	$2,4 \leq C \leq 3,7$	Tolerância Média	Com possibilidade de mudança
3	$3,8 \leq C \leq 5$	Baixa Tolerância	Com previsão de mudança

Avalie qualitativamente a tolerância temporal para recuperação após os ataques que você evidenciou. Para a tendência, neste caso vamos considerar que não há previsão de mudança. Compare os resultados obtidos até aqui com os critérios de aceitação do risco (Avaliação do Risco).

\* C é a criticidade aferida no estudo CIDAL \*\* Os níveis qualitativos “alto” a “baixo” devem considerar os critérios de aceitação de risco estabelecidos pelo negócio \*\*\* Para a tendência, convém consultar o Plano de Negócios

- Encerra-se assim a fase de levantamento das características do negócio
- Próxima etapa (quinto passo): Montagem de uma Estrutura de Gestão do Risco
  - FSI ou CGSI ?
    - É importante ser *top-down* ?
    - É importante ser abrangente e democrática ?
    - É importante haver um *Security Officer* ?
  - Início do PDCA.

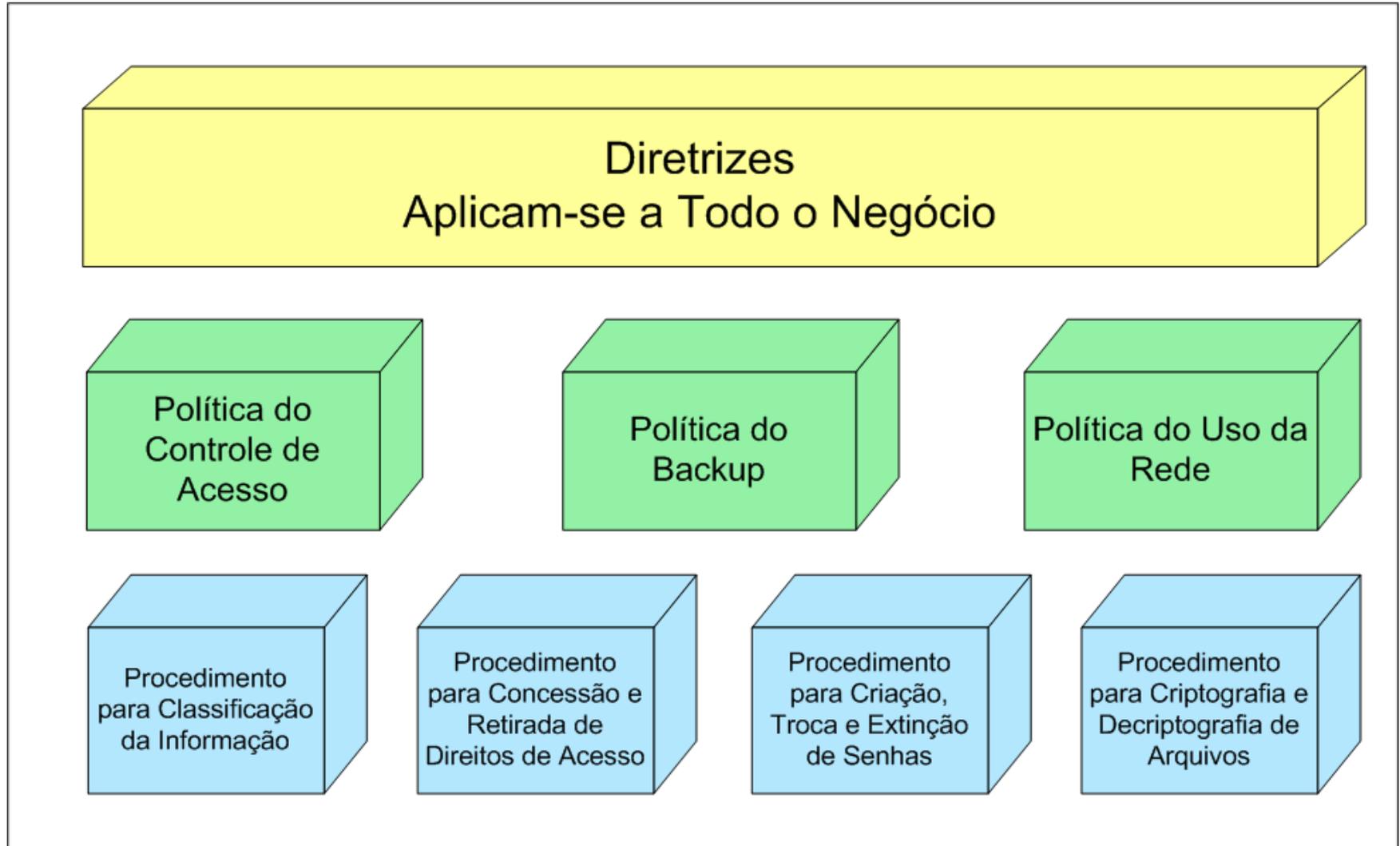
# PDCA Modificado



# Sexto Passo

- Política de Segurança (PolSeg)
  - É o dia-a-dia do controle do nível de risco
  - Depende de conscientização, treinamento e comprometimento *top-down*
  - Definida através de Diretrizes, Normas e Procedimentos
  - Deve focar objetivamente nos riscos evidenciados durante as fases anteriores
  - O Monitoramento demandará novas ações.

# Política de Segurança



# Objetivos da PolSeg

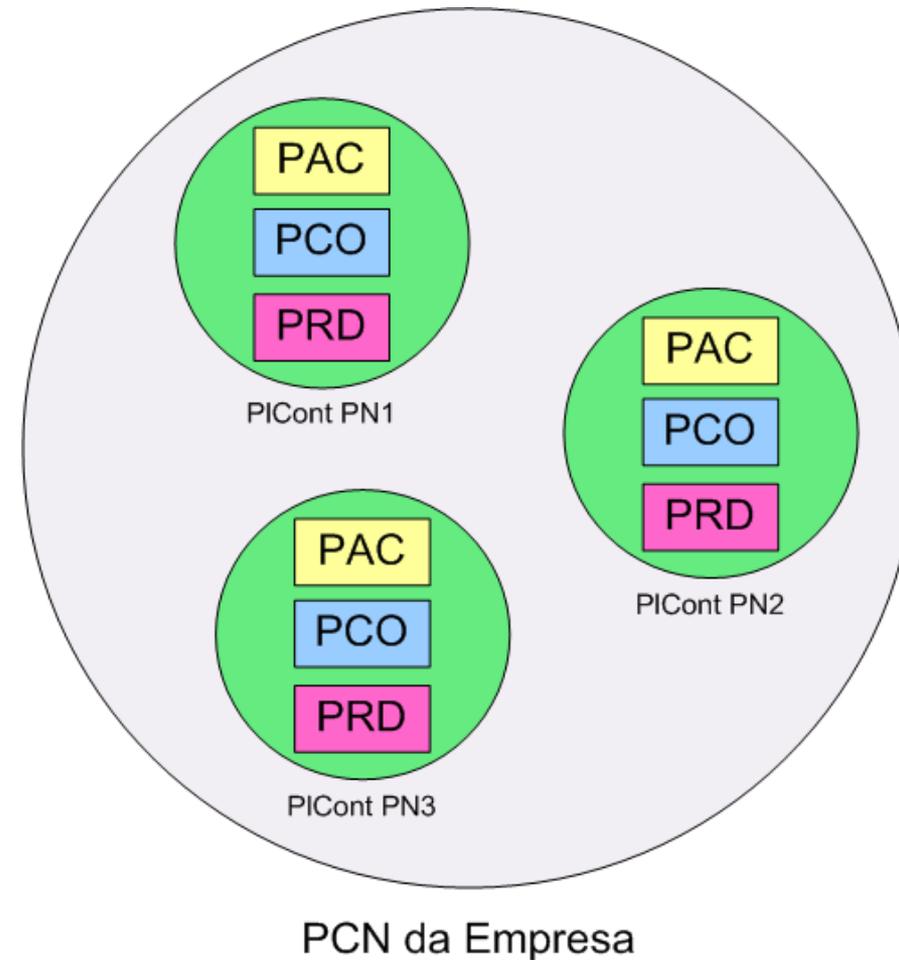
- Os itens da PolSeg constituem dispositivos para controle do nível de risco
- Estes itens devem ser do domínio de todos os envolvidos em cada risco evidenciado
- Um acordo deve ser assinado pelos colaboradores prevendo alinhamento com a Política
- Uma estratégia de capacitação deve garantir sua eficácia com eficiência.

- Elaboração de um esboço de Política para o caso.

A luz das prioridades em termos de risco, defina uma DIRETRIZ para a sua Política de Segurança.

- Plano de Continuidade dos Negócios
  - Contém os “Planos B” para as situações de risco de alta criticidade
  - Devem ser criados para os PN, e não para os ativos
    - são os “Planos de Contingência”
  - Devem ser organizados para missões distintas:
    - PAC – Plano de Administração de Crise
    - PCO – Plano de Continuidade Operacional
    - PRD – Plano de Recuperação de Desastres.

# Plano de Continuidade dos Negócios (PCN)



# *Business Impact Analysis*

- Ferramenta para priorização de processos de acordo com sua criticidade, tolerância temporal e impactos
- As ameaças mais relevantes devem ser evidenciadas para cada Processo de Negócio
- Assunto bem discutido na literatura, comum a cada tipo de negócio
- Maior dificuldade é a mensuração quantitativa dos impactos.

# Caso

- Exemplo de BIA

- Elaborado para as necessidades mais impactantes (BIA)
  - Deve, com o menor custo, garantir a funcionalidade do negócio dentro da tolerância temporal.
- Além de buscar garantia de manutenção da funcionalidade dentro da tolerância desejada, visa evitar novas ocorrências (PRD)
- Deve ser testado periodicamente (PDCA).

# Caso

- Sugira uma ação de PAC, PCO ou PRD do risco mais prioritário

# Próximo Passo

- Visando ativar o PDCA, o monitoramento contínuo e as auditorias permitem alterações nos PLCont e na PolSeg
- O nível de cultura neste ponto do trabalho certamente é maior que no início
- O envolvimento é maior
- Uma Análise de Riscos mais técnica agora pode ser feita com melhores resultados.

# Conclusão

- Segredo do Sucesso:
  - Comprometimento do setor executivo;
  - O uso de metodologias disponíveis;
  - Envolvimento de todos os Gestores;
  - Criação de mentalidade de segurança, para alcançar o comprometimento de todos; e
  - Postura proativa.
- Mãos à obra !!!!!