MBA EM GESTÃO EMPRESARIAL

FOCO EM TECNOLOGIA DE INFORMAÇÃO

UNIVERSIDADE FEDERAL FLUMINENSE

Gestão Estratégica da Segurança da Informação

Prof. Fred Sauer, D.Sc.
contato@fredsauer.com.br

Apresentação do Palestrante

- Frederico Sauer
  - Doutor em Sistemas Computacionais (UFRJ)
  - Professor FGV-Management 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
  - Sócio-diretor da Sauer Security

Roteiro da Palestra

- Estratégia para a gestão racional da SegInfo
- Normas adotadas
- Conceitos básicos
- Exemplos

Cenário Atual

- As empresas investem em Segurança da Informação...
- Mas continuam sofrendo reveses decorrentes de Incidentes previsíveis !

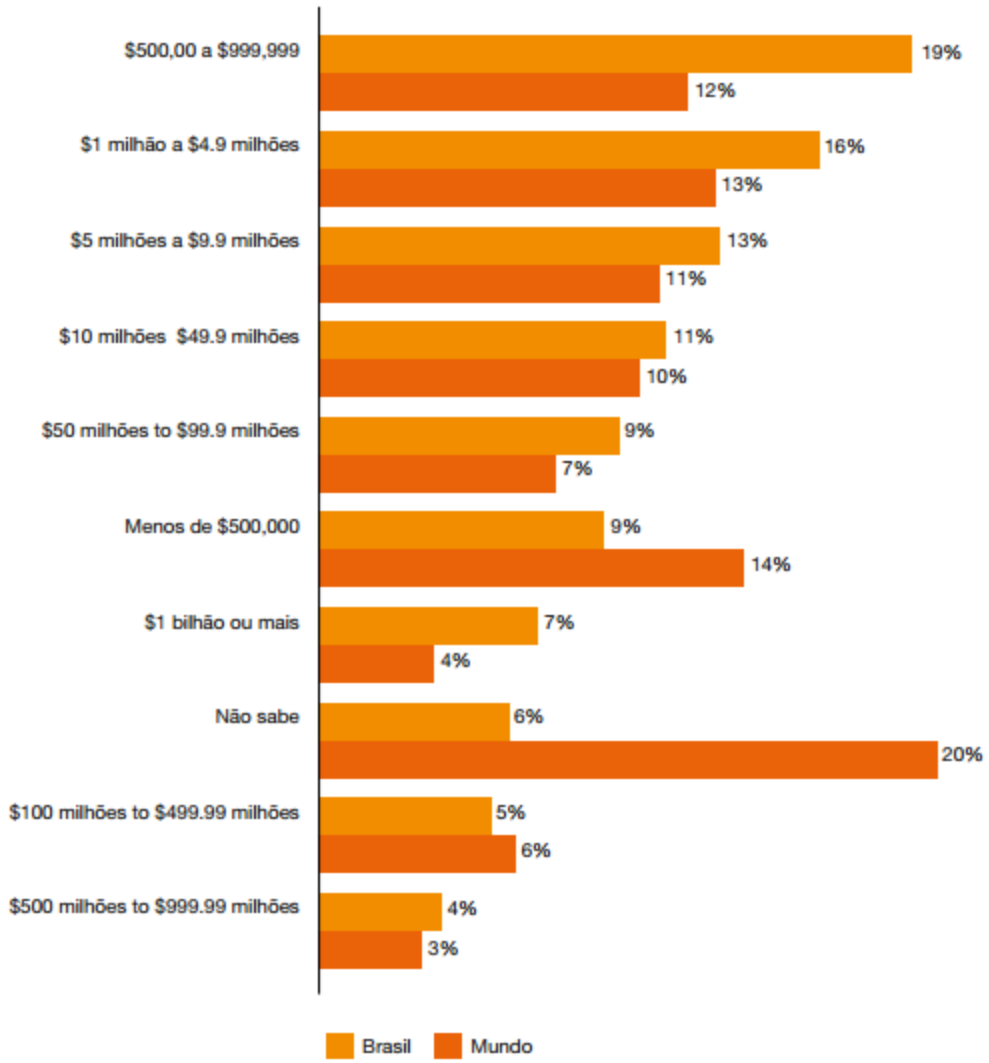
Investimentos vultosos

Investimentos em segurança da informação

No Brasil, o orçamento destinado à segurança da informação ainda é fortemente condicionado pela situação econômica do país, conforme indicado por 47,8% dos respondentes.

Quando perguntados sobre o investimento dedicado a segurança da informação, 28% dos respondentes estimam que seus orçamentos atinjam o teto de um milhão de dólares, o que pode ser considerado razoavelmente baixo quando comparado à perda financeira que uma ameaça pode causar à empresa, ao explorar uma vulnerabilidade.

Figura 25: Magnitude dos investimentos



Fonte: Pesquisa PWC 2014

Incidente de Segurança

ReclameAQUI nome da empresa, produto para reclamar ou pesquisar

veja também: todas as reclamações | não respondidas | respondidas | finalizadas

Falta de Segurança nas Operações Financerias

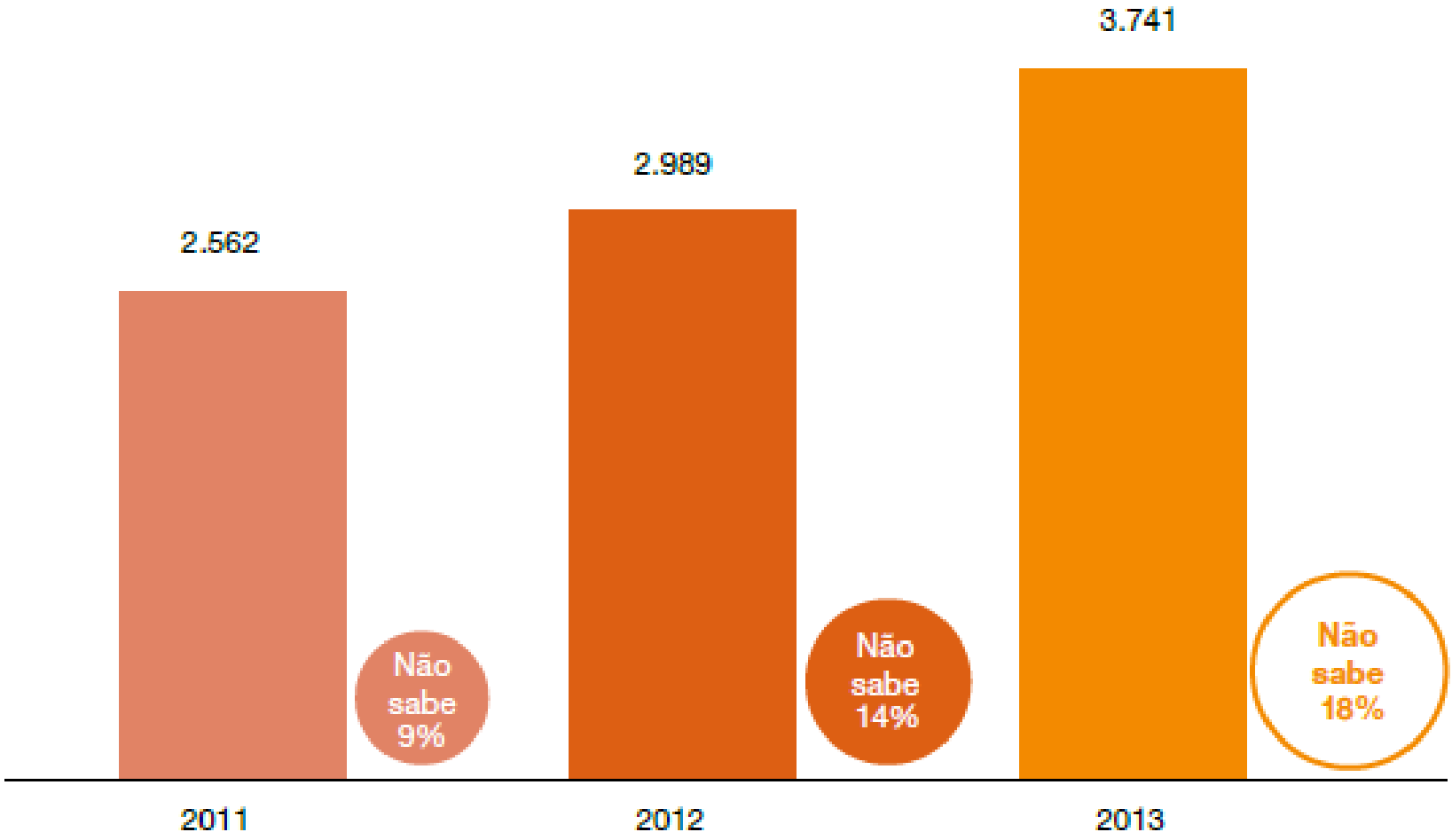
Banco Itaú S/A

São Paulo - SP Domingo, 17 de Novembro de 2013 - 20:09

Sou cliente do Banco Itaú a mais de 12 anos, NUNCA tive um histórico de uso indevido em qualquer canal de atendimento do Itaú.
Entretanto tive alguns problemas com a Instituição que mostra alguns problemas de segurança que me deixou preocupado.
Tenho em meu relacionamento como Banco, 3 previdências privadas, investimentos em ações, investimento em fundos, investimentos em CDBs e Investimento em poupança só em investimentos.
O primeiro problema que ocorreu foi quando deixei de ser 1o. titular, solicitei que minha esposa fosse a 1a. titular e eu o segundo, neste momento tive problemas de acesso aos sistemas, nos primeiros dias eu tinha que conectar via Internet Banking com o meu usuário, porém com a senha de minha esposa e isto ocorreu também ao acessar o Itaú corretora.
O problema do acesso ao Internet Banking foi solucionado depois de 2 reclamações, porém a do acesso ao Itaú Corretora, foram diverdas reclamações até eles finalmente resolverem o problema. O pior de tudo foi escutar que provavelmente eu havia feito alguma ação indevida.
Recentemente tive problemas com uma compra indevida de um cartão de crédito do Itaú ligado a minha conta quando eu era 1o. titular, inclusive sendo considerando um DEVEDOR prestes a ser enviado para o SPC. E MESMO ASSIM O BANCO INSISTE EM DIZER QUE NÃO EXISTE PROBLEMAS DE SEGURANÇA.

Frequência de Incidentes

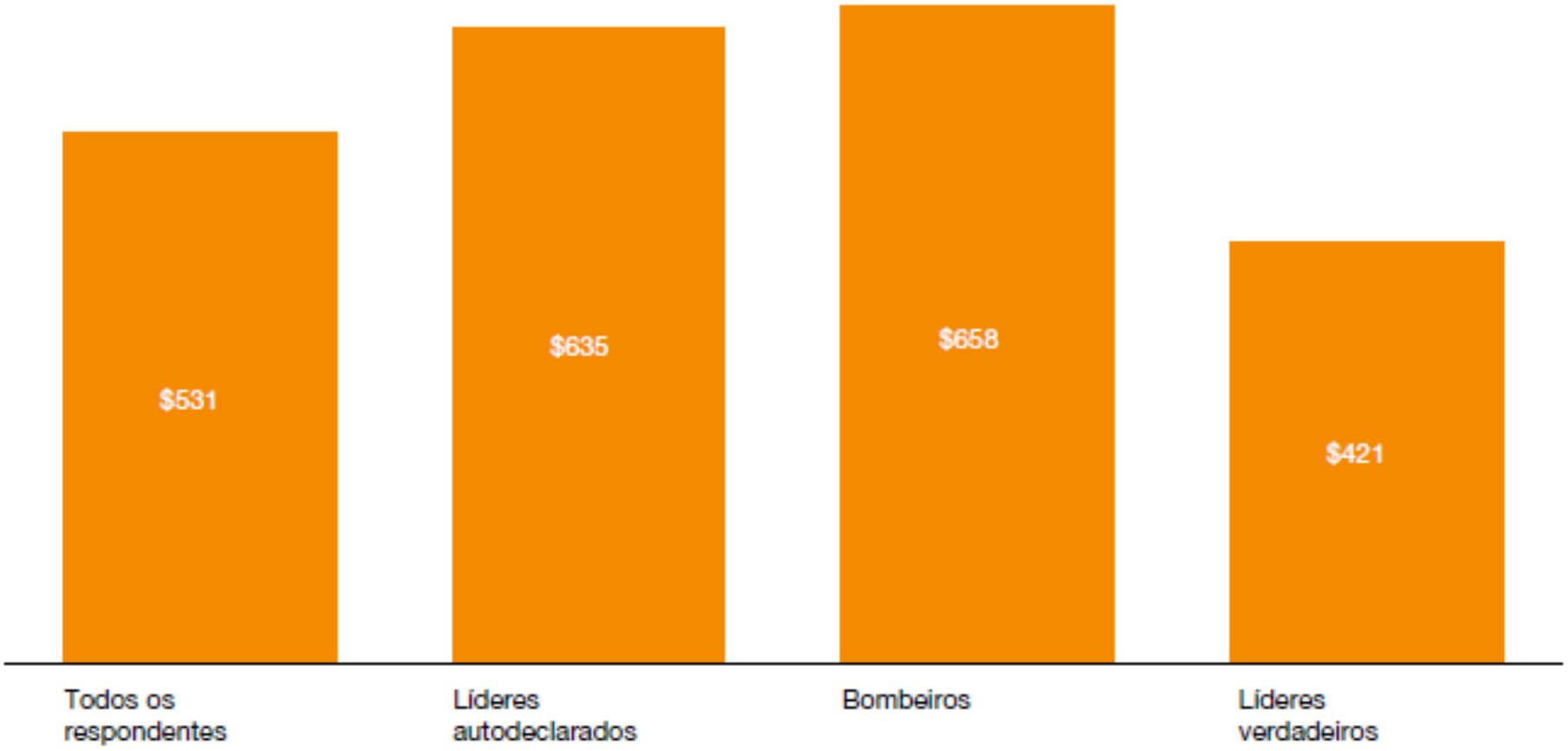
Figura 4: Número médio de incidentes de segurança nos últimos 12 meses



Fonte: Pesquisa PWC 2014

Custo tangível por Incidente

Figura 6: Custo médio por incidente de segurança



Fonte: Pesquisa PWC 2014

Caso de Sucesso: Siemens

Wagner Giovanini, diretor de Compliance da Siemens: "Numa concorrência acirrada, o cliente assina contrato conosco por conta da nossa postura ética"

As empresas sabem da importância de combater o problema, sobretudo num país como o Brasil, que passou, no ano passado, de 69º para 73º lugar, numa lista de 182 países, no Índice de Percepção da Corrupção Mundial, avaliado pela ONG Transparência Internacional. Para descolar-se dessa realidade, algumas companhias já contam com robustos departamentos focados na definição de regras de conduta conhecidas pelo termo *compliance* entre funcionários, fornecedores e clientes. Mesmo que, num primeiro momento, a transparência não traga ganhos financeiros, o rótulo de empresa ética pode vir a ser o fiel da balança para fechar negócios.

“Há casos em que, numa concorrência acirrada, o cliente assinou contrato conosco por conta da postura ética e responsável da nossa empresa”, disse à DINHEIRO Wagner Giovanini, diretor de *compliance* da Siemens para a América Latina. A multinacional alemã adotou uma política global rigorosa depois de ter sua reputação abalada por escândalos envolvendo CEOs em filiais de vários países, inclusive no Brasil. A área de *compliance*, criada em 2007, trabalha para prevenir e detectar casos de má conduta. Gastos com viagens, presentes a terceiros, patrocínios, doações e jantares passam pelo pente-fino da equipe especializada. Nos 190 países em que a empresa atua, são 600 funcionários envolvidos com o assunto. No Brasil, o departamento tem 30 pessoas, que checam se os 800 parceiros comerciais respeitam as regras estabelecidas nos contratos.

Fonte: Isto é – Dinheiro – Jan 2012

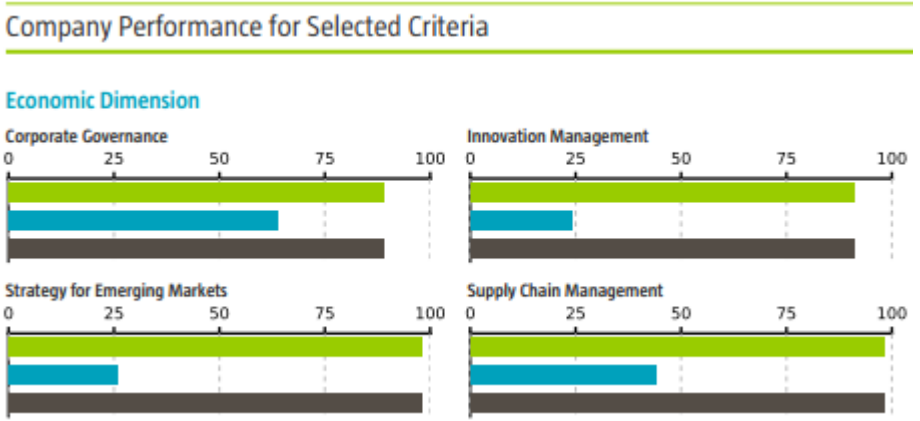
Caso de Sucesso: Siemens

Dow Jones Sustainability Indices (DJSI)

Assessment 2013 – Industry Group Leaders

as of September 2013

Volkswagen AG	Automobiles & Components	Germany
Australia & New Zealand Banking Group Ltd	Banks	Australia
Siemens AG	Capital Goods	Germany
Adecco SA	Commercial & Professional Services	Switzerland
Panasonic Corp	Consumer Durables & Apparel	Japan
Tabcorp Holdings Ltd	Consumer Services	Australia
Citigroup Inc	Diversified Financials	United States
BG Group PLC	Energy	United Kingdom
Woolworths Ltd	Food & Staples Retailing	Australia
Nestle SA	Food, Beverage & Tobacco	Switzerland
Abbott Laboratories	Health Care Equipment & Services	United States
Henkel AG & Co KGaA	Household & Personal Products	Germany



Fonte: Dow Jones Report 2013

Diagnóstico

- As empresas não investem em segurança de forma Top-down, e sim bottom-up
  - TI costuma ser responsável pela área de SegInfo
  - Práticas são adotadas com base em cartilhas
- Não há um processo de Gestão da SegInfo
- Não é estimulada a criação de cultura corporativa de SegInfo
- A Gestão da SegInfo não é compartilhada por todos

Solução

- Garantir que o processo se inicie na Direção da empresa
- Garantir que as ações de SegInfo sejam alinhadas com o negócio e a estratégia da organização
- Garantir que haja conscientização, treinamento e criação de cultura de SegInfo
- Garantir que a Gestão da SegInfo seja analisada pela Direção, demandando melhoria contínua

Fundamentos Teóricos

- 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).

Conceito de Risco

- 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 .

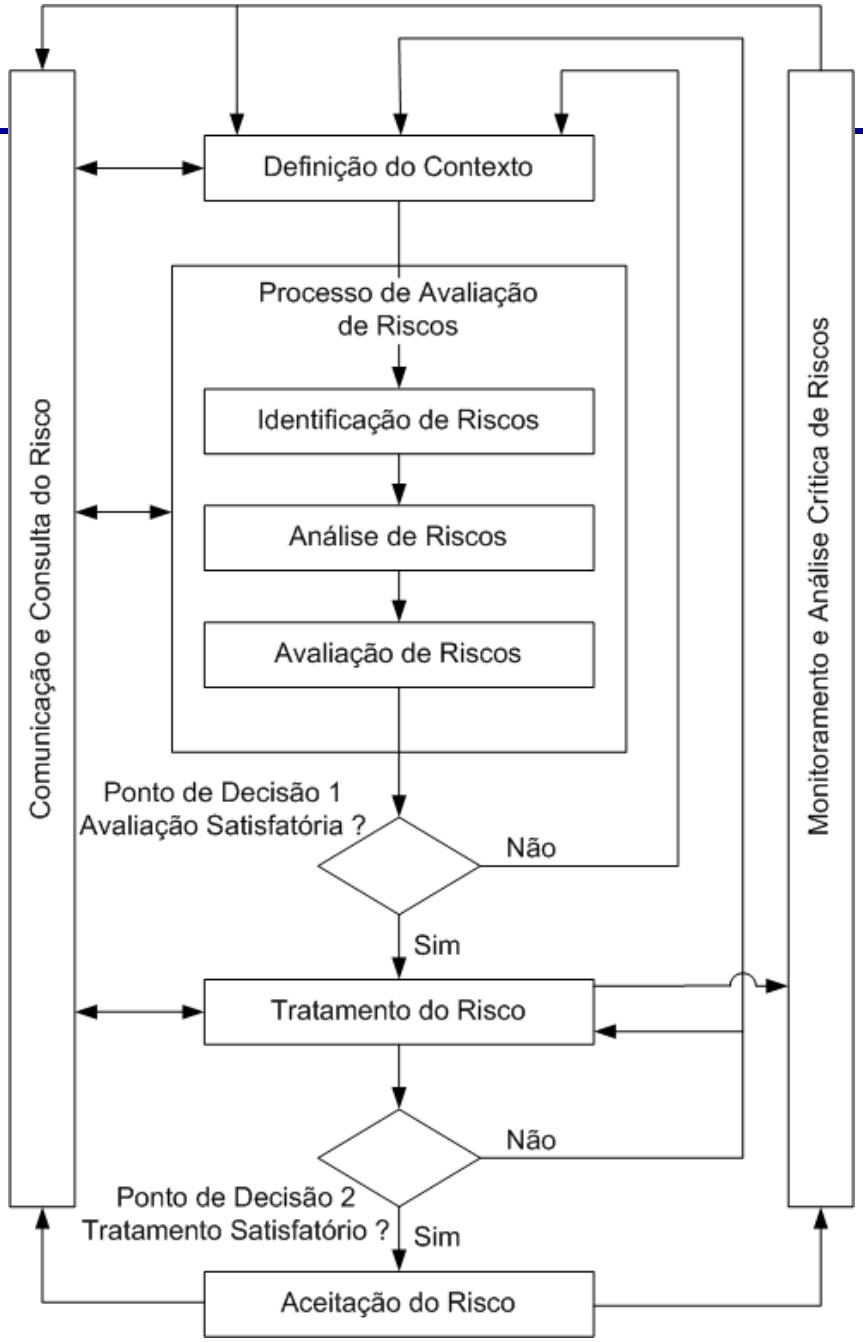
Anatomia do Risco

- 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

Critérios de Aceitação de 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.

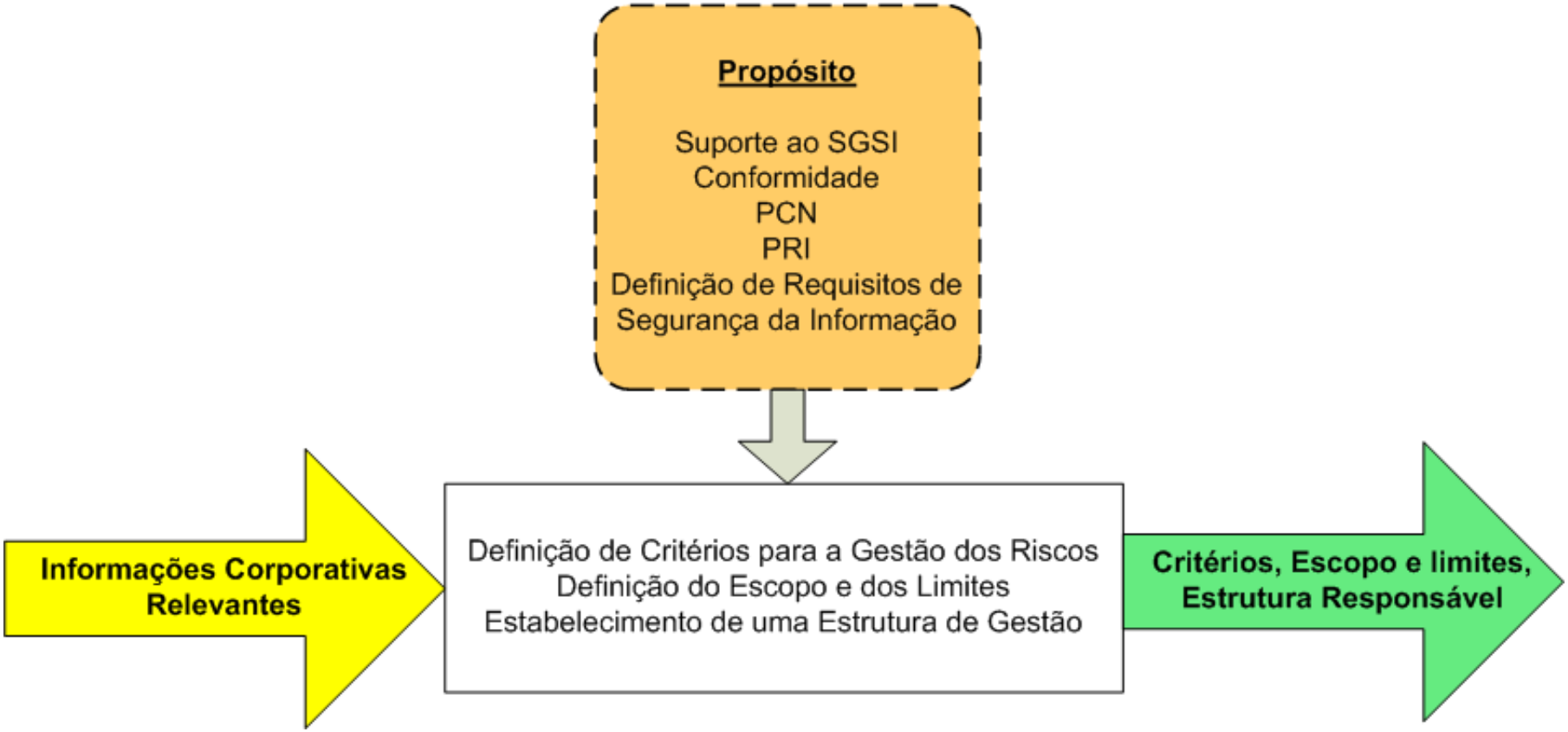


ISO 27005 Risk Management

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



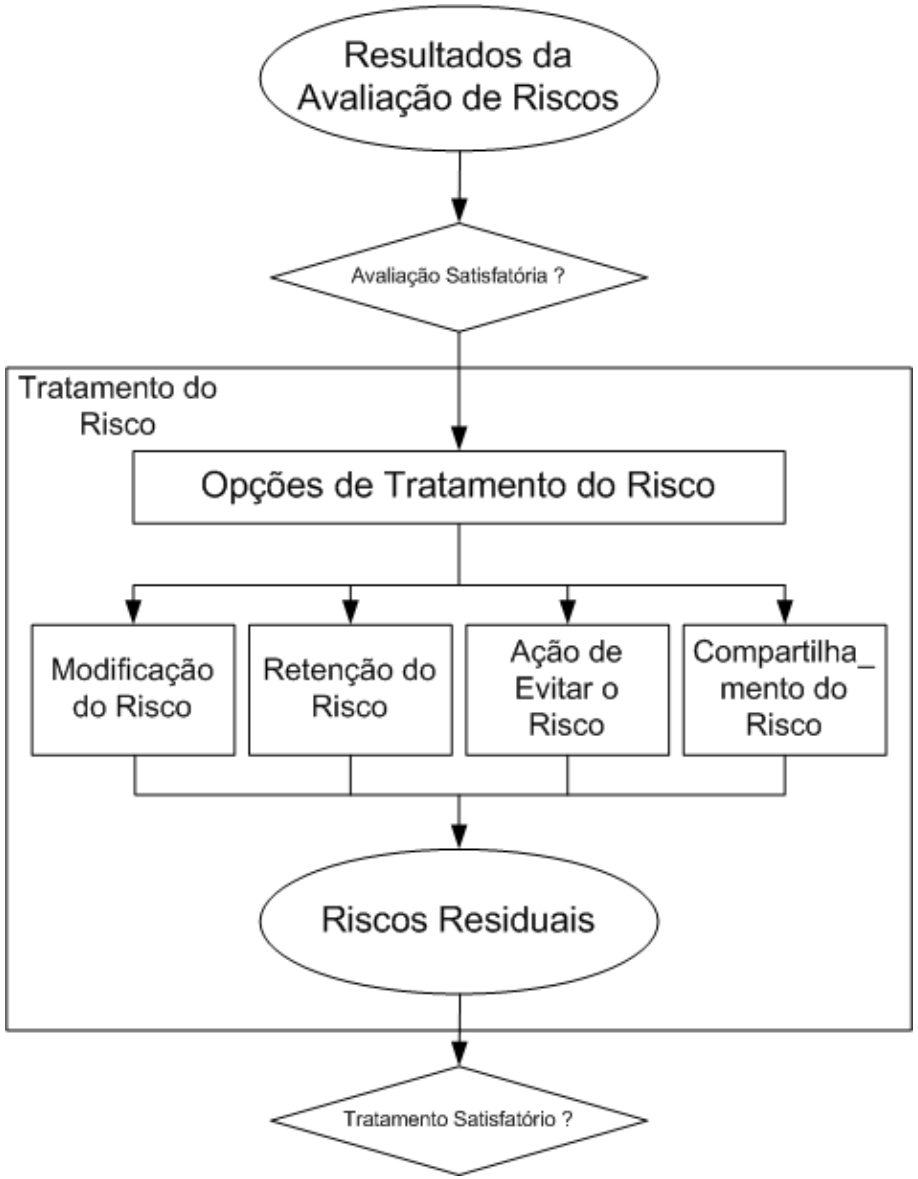
Avaliação de Riscos

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

Análise/Avaliação do Risco

- 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.

Tratamento dos Riscos



Modificar

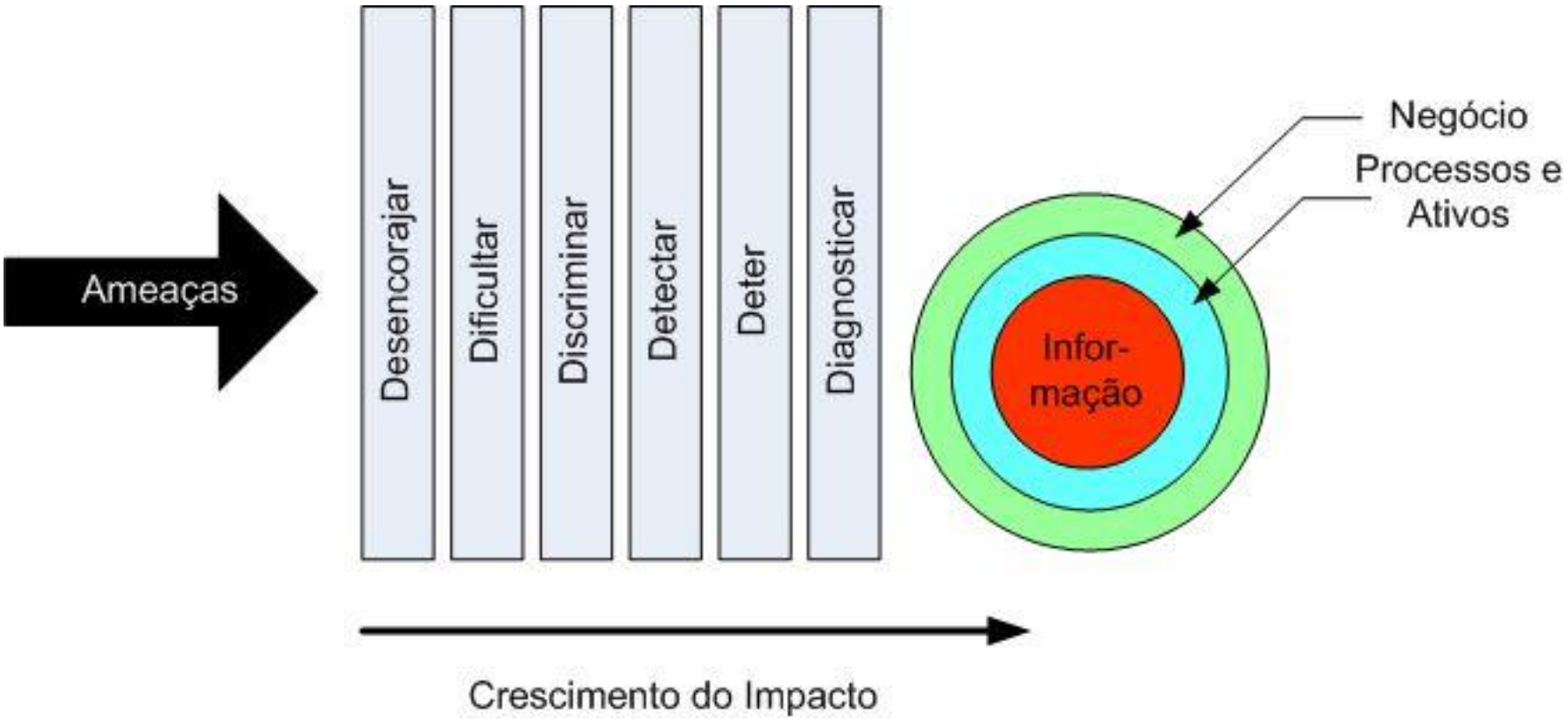
Reter

Evitar (Eliminar)

Compartilhar

Tratamento dos Riscos

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

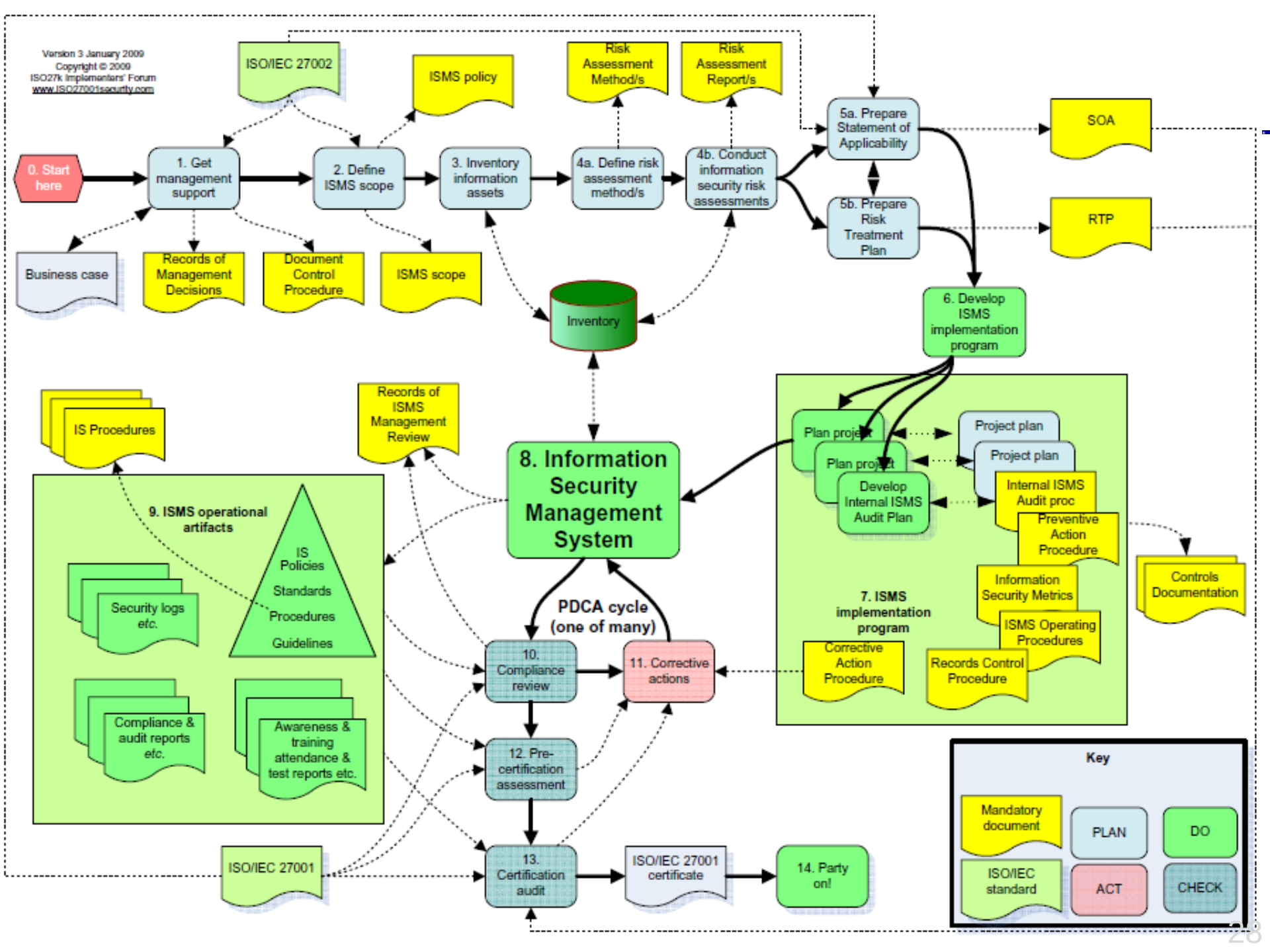


Tratamento dos Riscos

- 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.

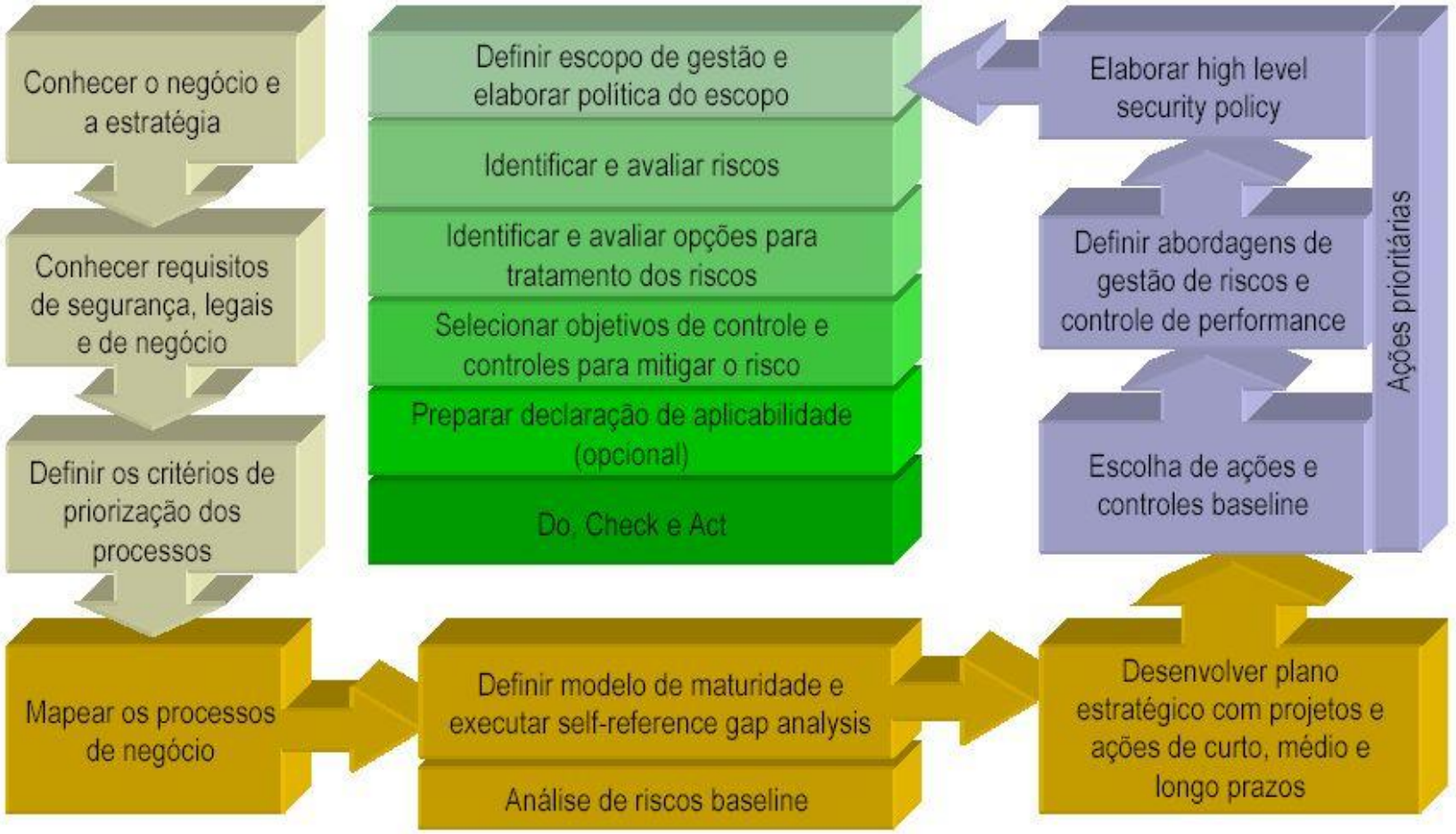
ISO 27001:2013

- 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.


Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com
ISO/IEC 27002
ISMS policy
Risk Assessment Method/s
Risk Assessment Report/s
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4a. Define risk assessment method/s
4b. Conduct information security risk assessments
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
SOA
RTP
Business case
Records of Management Decisions
Document Control Procedure
ISMS scope
Inventory
6. Develop ISMS implementation program
IS Procedures
Records of ISMS Management Review
8. Information Security Management System
9. ISMS operational artifacts
IS Policies
Standards
Procedures
Guidelines
Security logs etc.
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
PDCA cycle (one of many)
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
ISO/IEC 27001
ISO/IEC 27001 certificate
14. Party on!
Plan project
Plan project
Develop Internal ISMS Audit Plan
Project plan
Project plan
Internal ISMS Audit proc
Preventive Action Procedure
Information Security Metrics
ISMS Operating Procedures
Records Control Procedure
Corrective Action Procedure
7. ISMS implementation program
Controls Documentation
Key
Mandatory document
ISO/IEC standard
PLAN
DO
ACT
CHECK

Proposta de Trabalho

Visão funcional
Planejamento Estratégico



Detalhes a observar na proposta

- 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.

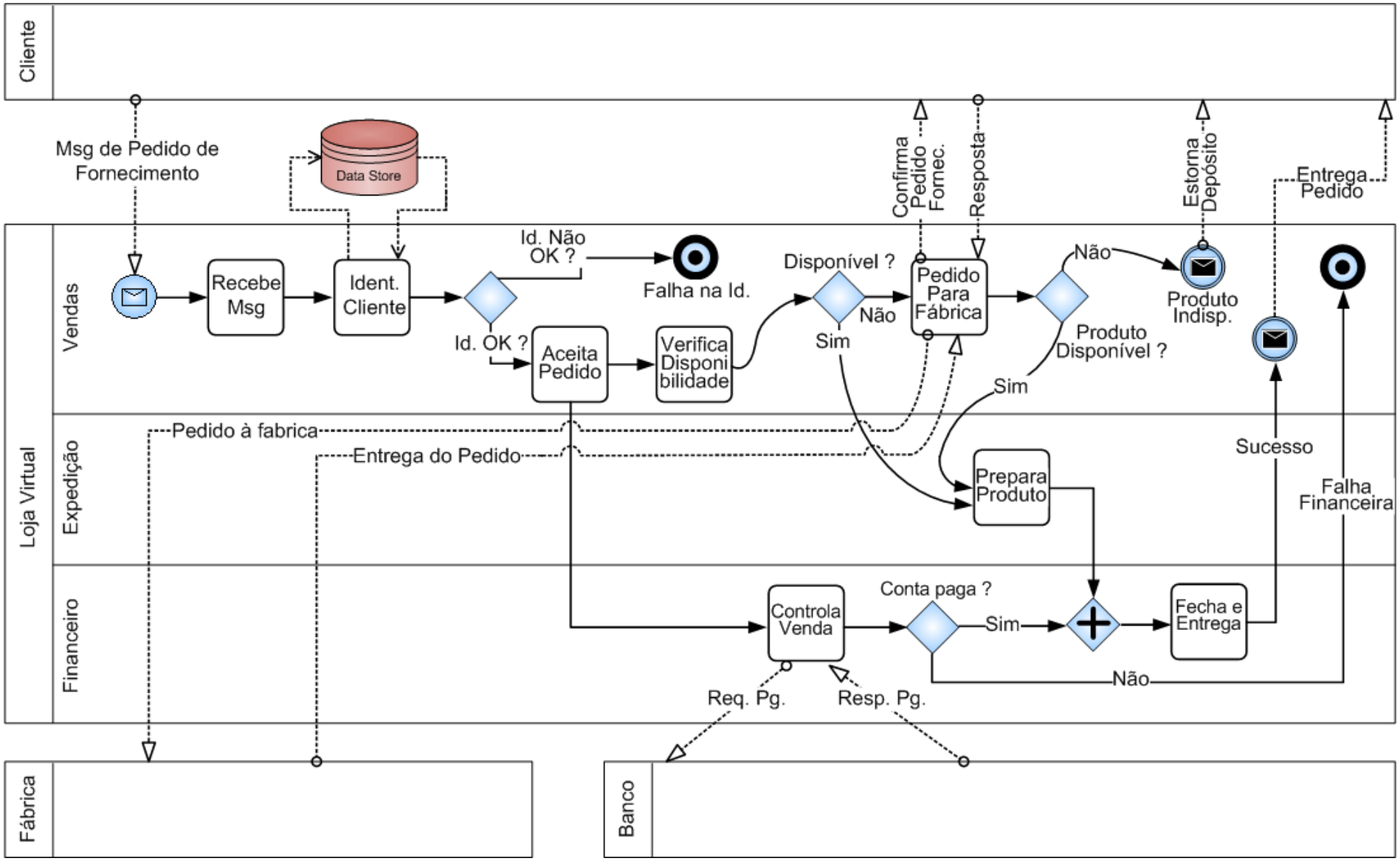
Mapeamento do Negócio

- 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").

Objetivo do Mapeamento do Processo

- 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.

Exemplo de processo mapeado em BPMN



Inventário de Ativos

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

Visão holística dos processos

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

Objetivo desta atividade

- 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.

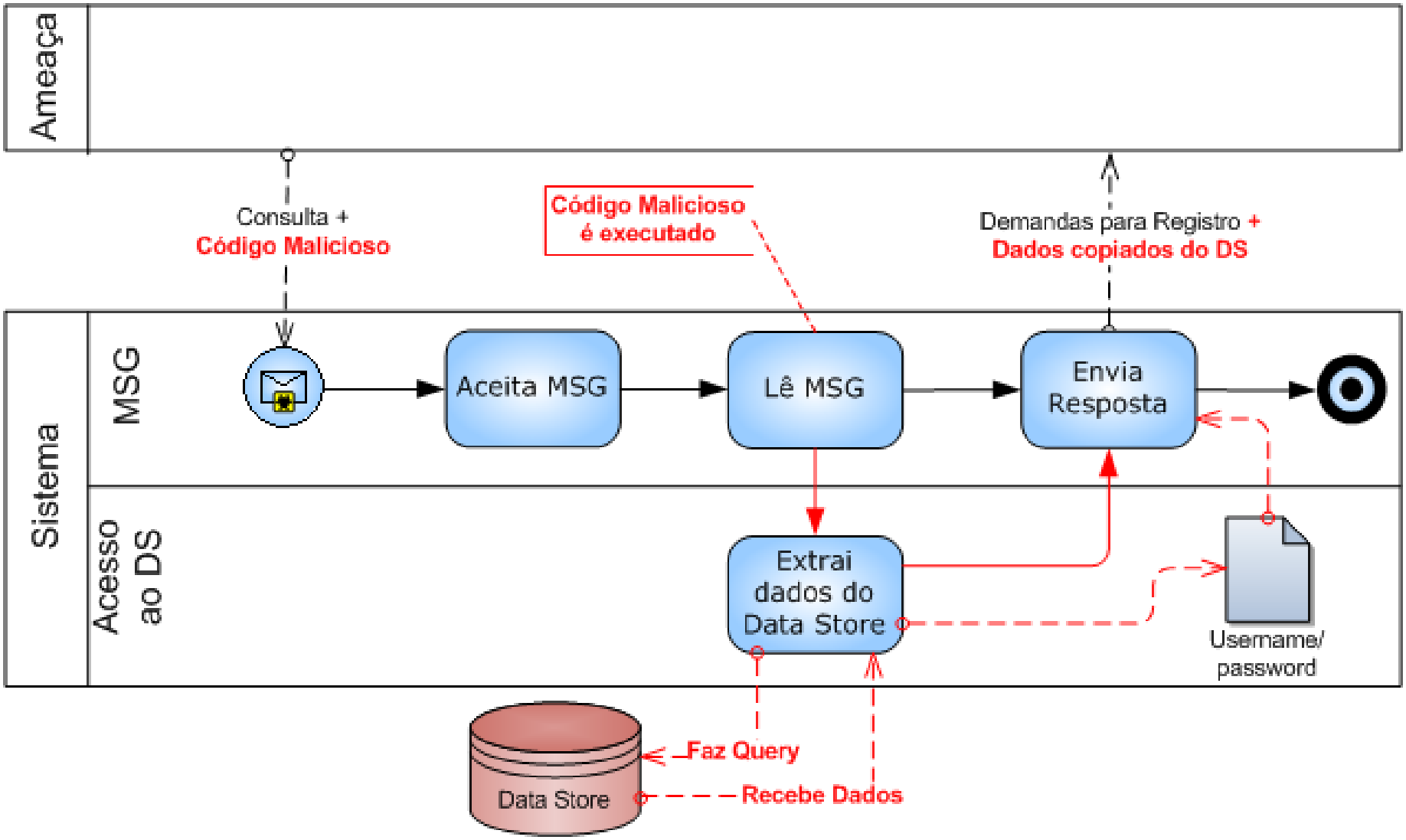
Análise de Riscos Baseline

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

Análise de Riscos Baseline

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

Exemplo de um possível incidente



Análise CIDAL

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

Avaliação da Sensibilidade

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

Objetivos da Análise CIDAL

- Possibilitar a identificação de sensibilidade nem sempre óbvia
- Permitir soluções compatíveis com a natureza do risco
- Priorizar processos de acordo com suas sensibilidades ao risco.

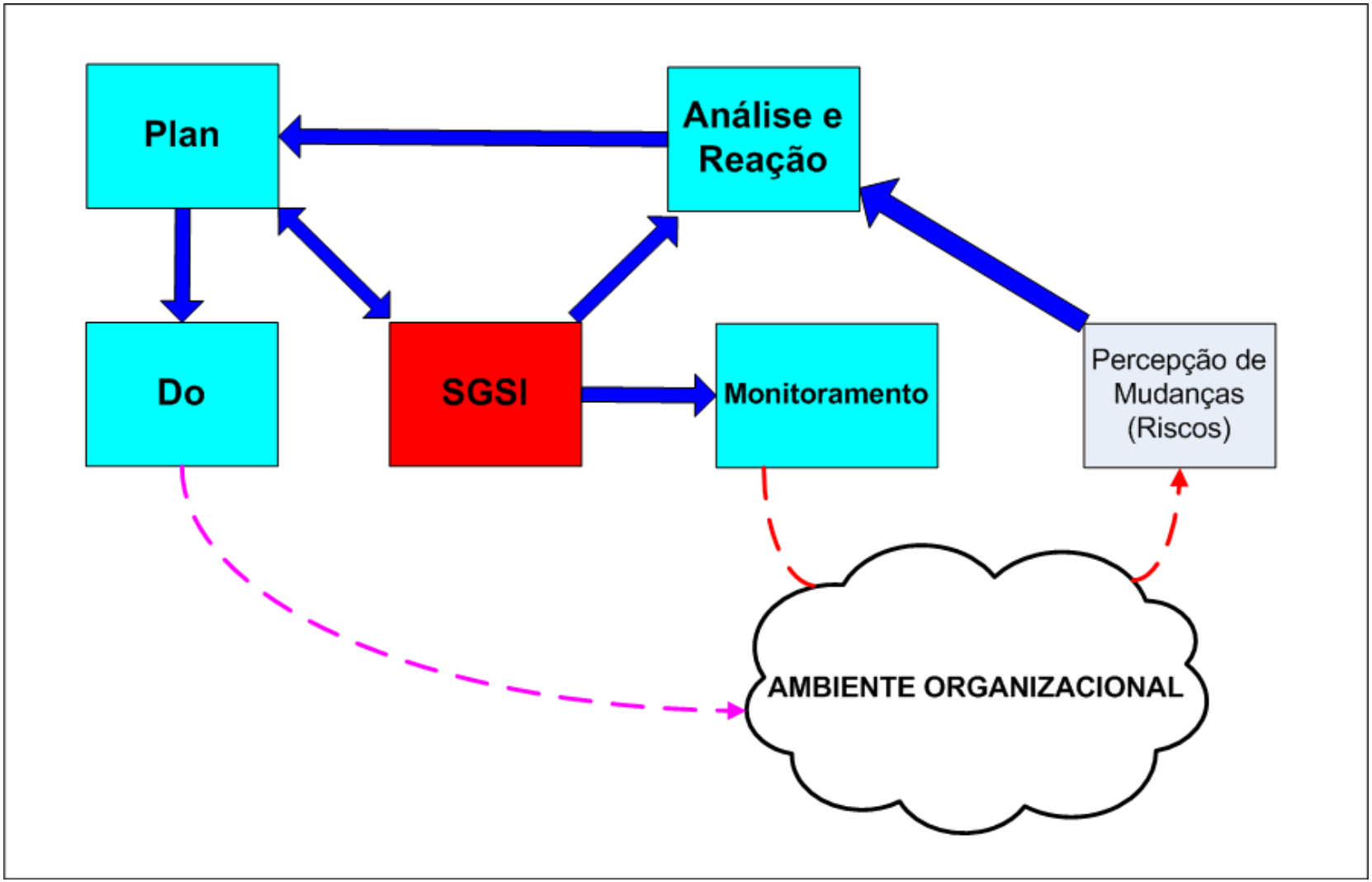
Exemplo de Métricas

Nível	Enquadramento
Controlado	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
Relevante	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
Importante	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.
Crítico	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.
Vital	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 *ad-hoc* 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.

A estrutura de gestão do risco

- Garantido o comprometimento da direção e a alocação de recursos, uma estrutura deve suportar o processo de gestão da SegInfo
- Características do CGSI
  - É importante ser *top-down* ?
  - É importante ser abrangente e democrático ?
  - É importante haver um *Security Officer* ?

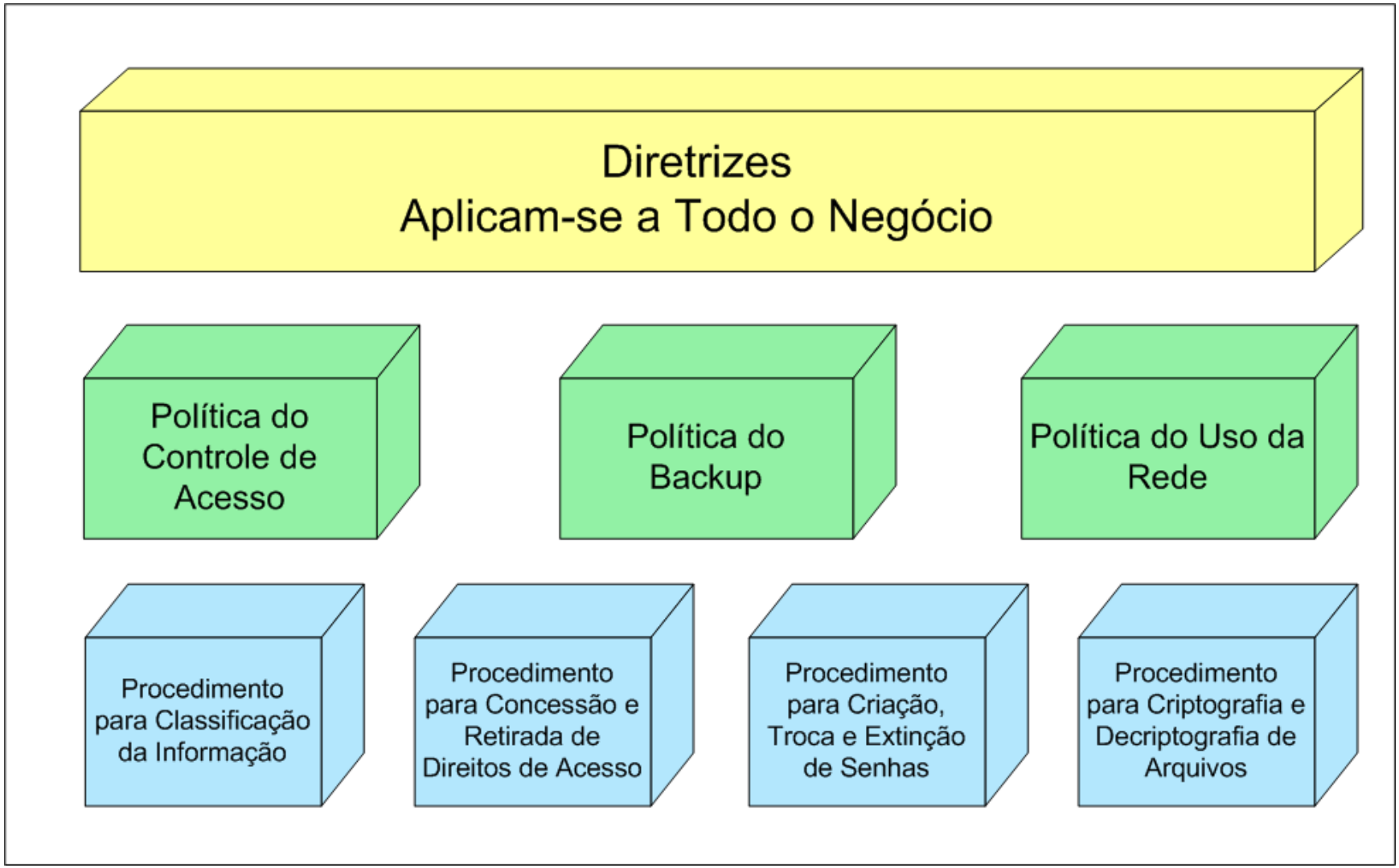
PDCA Modificado



Política de Segurança

- É o dia-a-dia do controle do nível de risco
- Depende de conscientização, treinamento e envolvimento *top-down*
- Definida através de Diretrizes, Normas e Procedimentos
  - Dependendo do tamanho e do nível de risco da corporação, várias políticas podem ser criadas
- Deve focar objetivamente nos riscos evidenciados durante o processo de gestão
- O Monitoramento contínuo demandará novas ações.

Política de Segurança



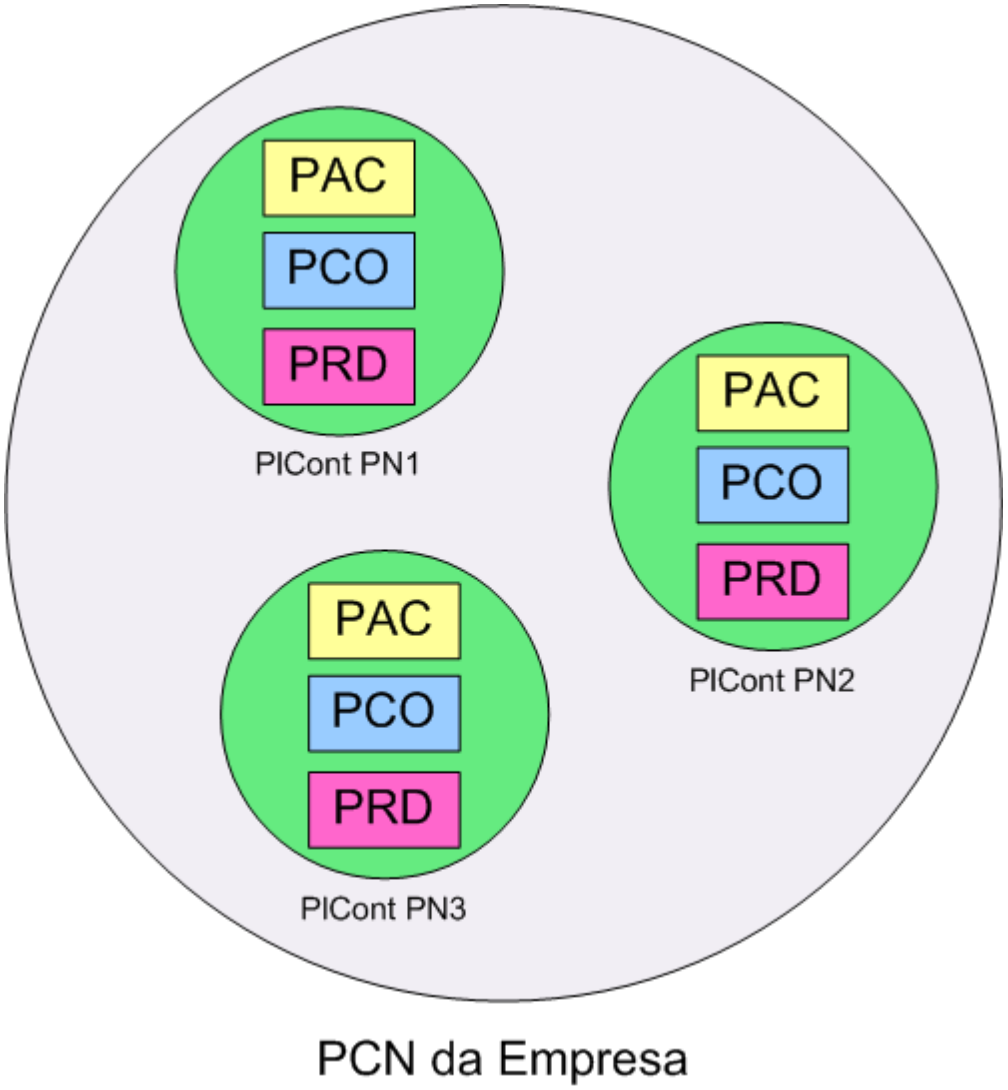
Objetivos da PolSeg

- 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 comprometimento com a Política
- Uma estratégia de capacitação deve garantir sua eficácia com eficiência.

Continuidade dos Negócios

- Plano de Continuidade dos Negócios
  - Contém uma forma alternativa de operação para os processos de alta criticidade
  - Devem ser criados para os processos, 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)



Estrutura dos PlCont

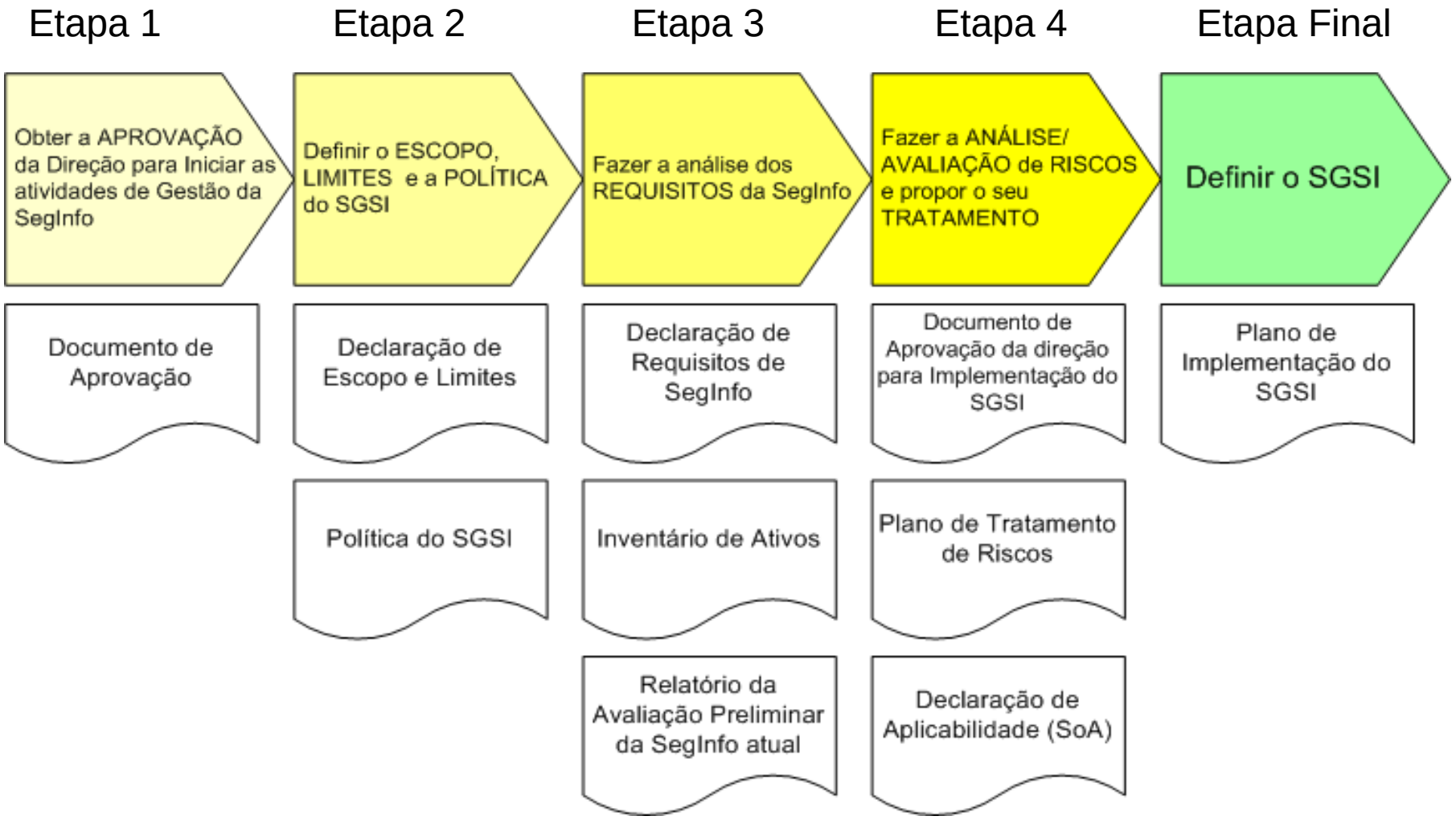
- Plano de Administração de Crise
  - Comunicação com Stakeholders
  - Define recursos e atores para a contingência
- Plano de Continuidade Operacional
  - Focado na continuidade do processo
- Plano de Recuperação de Desastre
  - Além do retorno à operação normal...
  - Lições aprendidas !

Fatores Críticos do Sucesso

- PolSeg, Objetivos e ações alinhadas com o NEGÓCIO
- Abordagem alinhada com a CULTURA organizacional
- Comprometimento visível de todos os níveis gerenciais
- Total entendimento dos REQUISITOS
- Conscientização, treinamento e educação
- Um efetivo Plano de Respostas a Incidentes
- Um efetivo Plano de Continuidade dos Negócios
- Melhoria contínua do SGSI

Processo de Criação

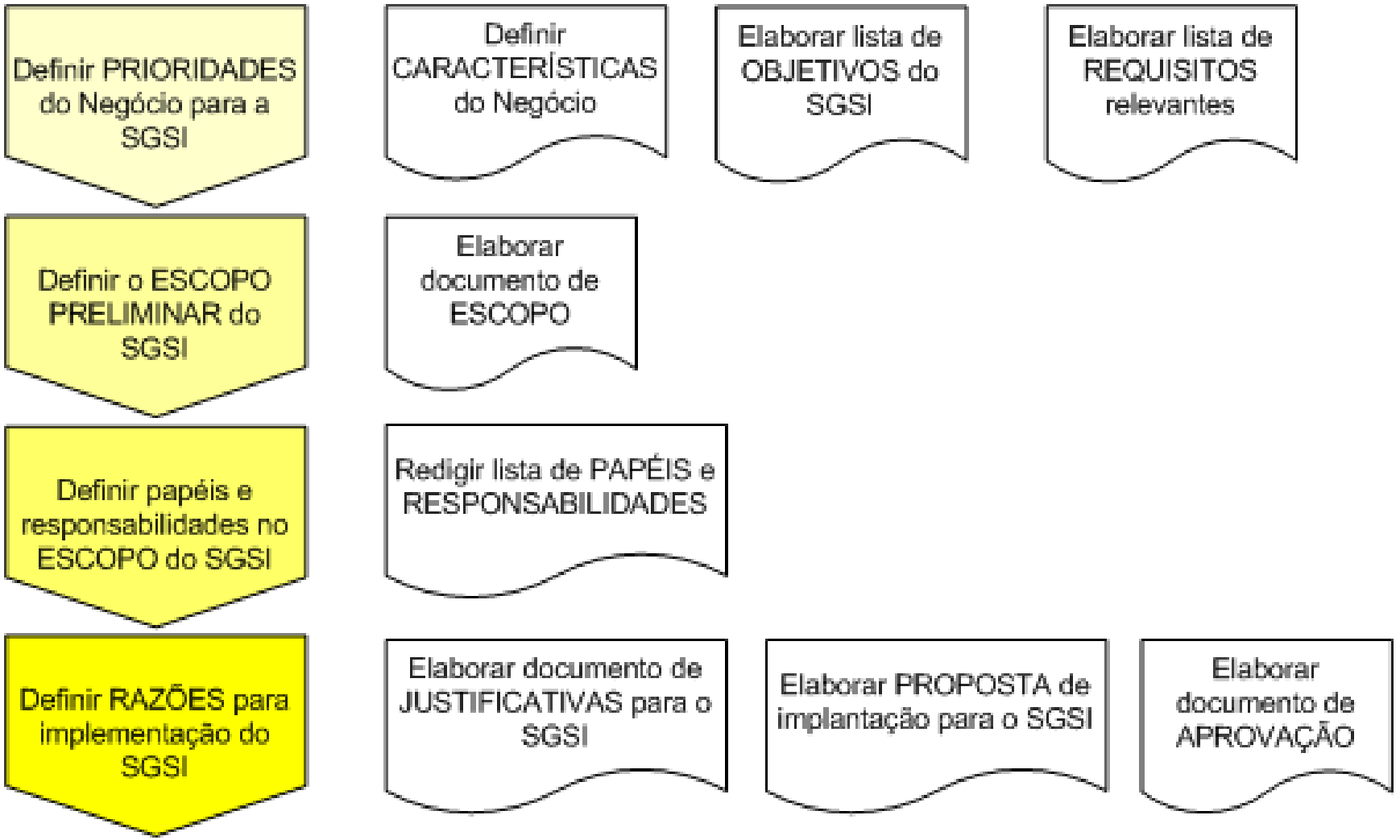
- Base na ISO 27003:2011



1 – Aprovação da Direção

- Para obter eficácia, convém que a Direção entenda claramente os motivos que justificam a existência do SGSI
  - Motivos que demandam a sua criação
  - Papéis e responsabilidades em relação à SegInfo
  - Ônus e Bônus para o negócio
- Além do entendimento, recursos devem ser alocados para suportar o SGSI

Fases e Documentos da Aprovação



Características do Negócio

- Entradas:
  - Levantar os OBJETIVOS ESTRATÉGICOS
  - Identificar os SISTEMAS DE GESTÃO existentes
  - Listar os REQUISITOS contratuais, regulatórios e legais
- Processo:
  - Identificar como a Gestão da SI pode contribuir para preservar os ativos e alavancar o negócio
- Saídas:
  - Documento com OBJETIVOS, PRIORIDADES e REQUISITOS da SegInfo

Definição de Requisitos e Objetivos

- Requisitos típicos:
  - Proteção de Informações e ativos críticos
  - Leis, regulamentos e *compliance*
  - SLA com clientes
  - Direcionadores de competitividade
- Objetivos comuns:
  - Manutenção da continuidade de processos críticos
  - Alcance de metas
  - Não ultrapassar limites específicos de risco

Definição do Escopo Preliminar

- Com as prioridades da fase anterior, define-se o escopo preliminar do SGSI contendo:
  - Necessidades internas e externas para alcançar os resultados importantes para o negócio
  - Requisitos dos *stakeholders* e os requisitos legais e regulamentares
  - Interfaces e dependências entre a organização e o exterior

Papéis e Responsabilidades

- Convém que seja identificado o responsável pela Gestão do SGSI (CISO)
- A responsabilidade final pelas atividades de gestão da SegInfo pertence ao nível GERENCIAL
- Cada colaborador é responsável pela observação da SegInfo na sua atividade cotidiana
  - Importante o entendimento da responsabilidade como “proprietário” da informação – definição da “necessidade de conhecer” para cada informação sensível

Exemplos

Papel	Responsabilidades
Diretor Executivo de SegInfo (CISO)	Responsabilidade e Governança da SegInfo em toda a corporação
Membro do CGSI	Participar da Análise/Avaliação de Riscos.
Gestores Setoriais	Comprometimento com as políticas. Orientar, educar, indicar demandas de treinamento, apontar situações de risco.
Administrador de Sistemas	Testes e monitoramento de vulnerabilidades dos sistemas
Gestor de Risco	Conduzir a Análise/Avaliação de Risco e submeter os resultados à Direção. Propor tratamento para os riscos.
Auditor de SegInfo	Auditar os processos da empresa, à luz dos requisitos estabelecidos pelo negócio
Colaborador	Cumprir as políticas. Comunicar eventos e incidentes de segurança

Justificativas e Aprovação do SGSI

- Metas, objetivos e benefícios para o negócio
- Escopo preliminar e os processos afetados
- Proposta de implantação:
  - Definição de marcos temporais e objetivos a alcançar em cada etapa
  - Definição de investimentos necessários
  - Estratégia de mensuração da eficácia do SGSI
- Documento de aprovação da direção para a implementação do SGSI

2 – Escopo e Política do SGSI

- Envolve duas atividades, a definição do escopo detalhado e a definição da Política do SGSI
- Definição do Escopo detalhado:
  - Definição das fronteiras da aplicação do SGSI
  - Mapeamento das funções e processos do escopo
  - Inventário preliminar de ativos
  - Identificação das demandas preliminares para atendimento dos objetivos e requisitos (Físicas, Tecnológicas e Humanas)

Política do SGSI

- Não é a Política de Segurança da empresa, e sim apenas do SGSI
- O primeiro passo é a definição dos critérios de aceitação do risco pelo negócio
- O principal objetivo da Política do SGSI é descrever os seus objetivos, responsabilidades, estrutura, escopo e limites
- Após a aprovação da direção, se inicia o levantamento das reais necessidades

3 – Análise dos Requisitos

- Envolve a identificação das necessidades básicas para a proteção dos ativos
- Com base no inventário dos ativos e processos:
  - Classificar os ativos e os processos quanto à sensibilidade, de acordo com os critérios e requisitos já disponíveis
  - Elaborar uma análise de *status quo*
    - Uma boa fonte de referência é a ISO 27002:2013
- Deve gerar uma documentação com a indicação de sensibilidade de processos à luz do negócio

4 – Análise/Avaliação de Riscos

- Etapa importante por definir objetivamente as ações a serem adotadas
- Envolve a identificação do risco e mensuração dos impactos para viabilizar uma proposição racional de soluções
- Deve sempre ser orientada pelos critérios de aceitação de risco pelo negócio
- A ISO 27002:2013 fornece uma boa lista de controles considerados boas práticas para o tratamento do risco

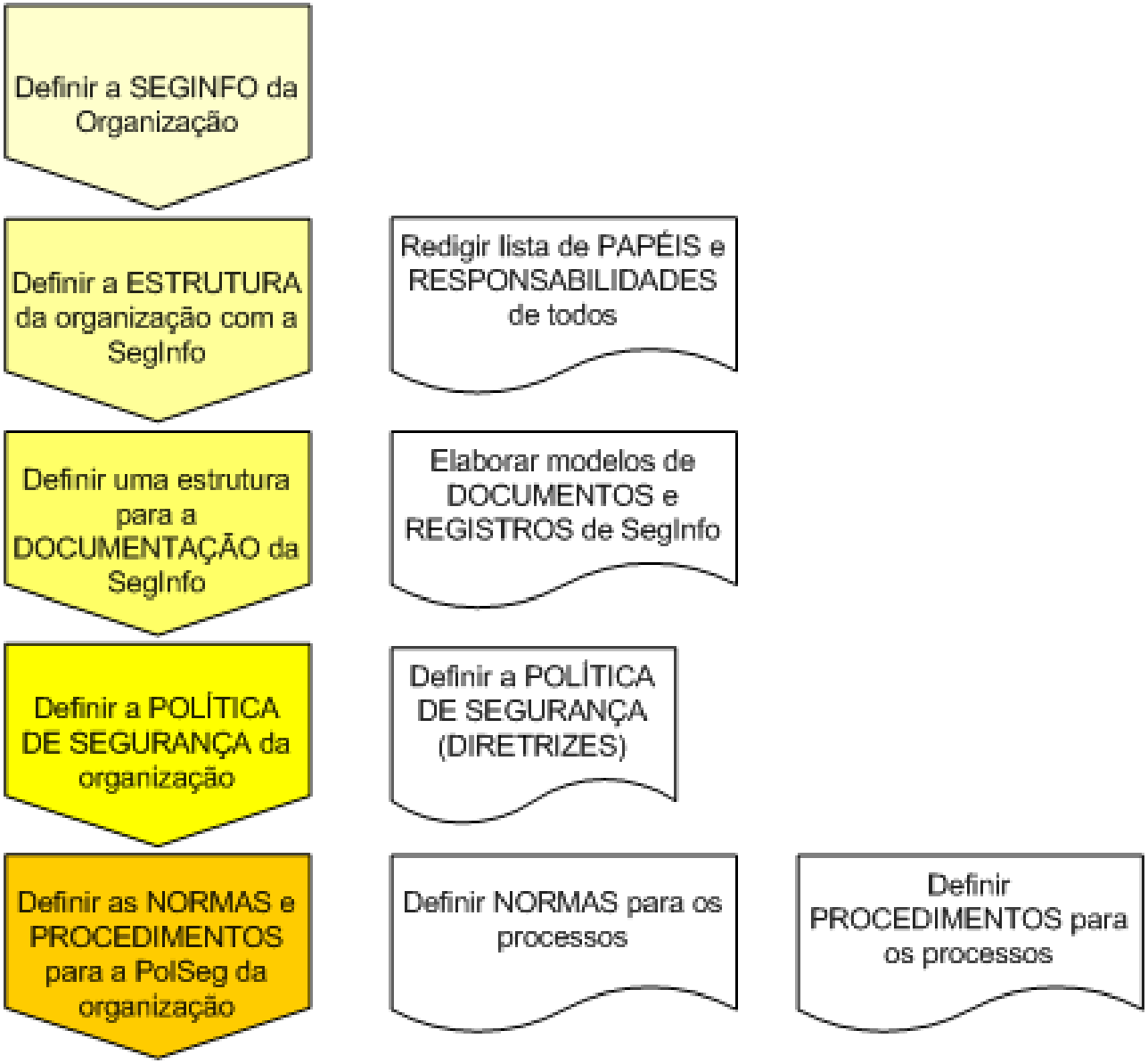
Tratamento dos Riscos

- Riscos indesejados devem ser tratados
- Riscos cujos impactos estejam acima do limite de aceitação do risco devem ter uma solução de contingenciamento
- Riscos residuais devem ser aceitos pela direção
- Ao final, a Declaração de Aplicabilidade deve indicar os controles adotados

Etapa Final – Definindo o SGSI

- Uma vez obtidos:
  - Comprometimento da Direção; e
  - Plano de Tratamento dos Riscos
- Cabe agora realizar a grande mudança !
  - Integrar a segurança no negócio
    - Física, Tecnológica e Humana
  - Planejar processos da Gestão da SegInfo
    - Monitoramento contínuo;
    - Aferição do SGSI;
    - Auditorias;
    - Treinamento e conscientização;
    - Gestão dos Incidentes; e
    - Melhoria contínua

Definindo o SGSI



Exemplos de Documentos

- Política de Segurança (Diretrizes, Normas e Procedimentos)
- Relatórios de análise/avaliação de riscos
- Plano de tratamento de riscos
- Plano para aferição da eficácia do SGSI
- Declaração de Aplicabilidade

Exemplos de Registros

- Livros de visitantes
- Formulários de autorização de acesso
- Formulários de movimentação de ativos
- Relatórios de treinamentos

Política de Segurança

- Com os resultados da análise/avaliação de risco, controles da ISO 27002:2013 devem ser adotados
- As regras devem implicar em mudanças processuais e comportamentais
- Pode ser uma única política ou várias especializadas
- O detalhamento em normas e diretrizes é importante para direcionar as demandas de acordo com os papéis e responsabilidades

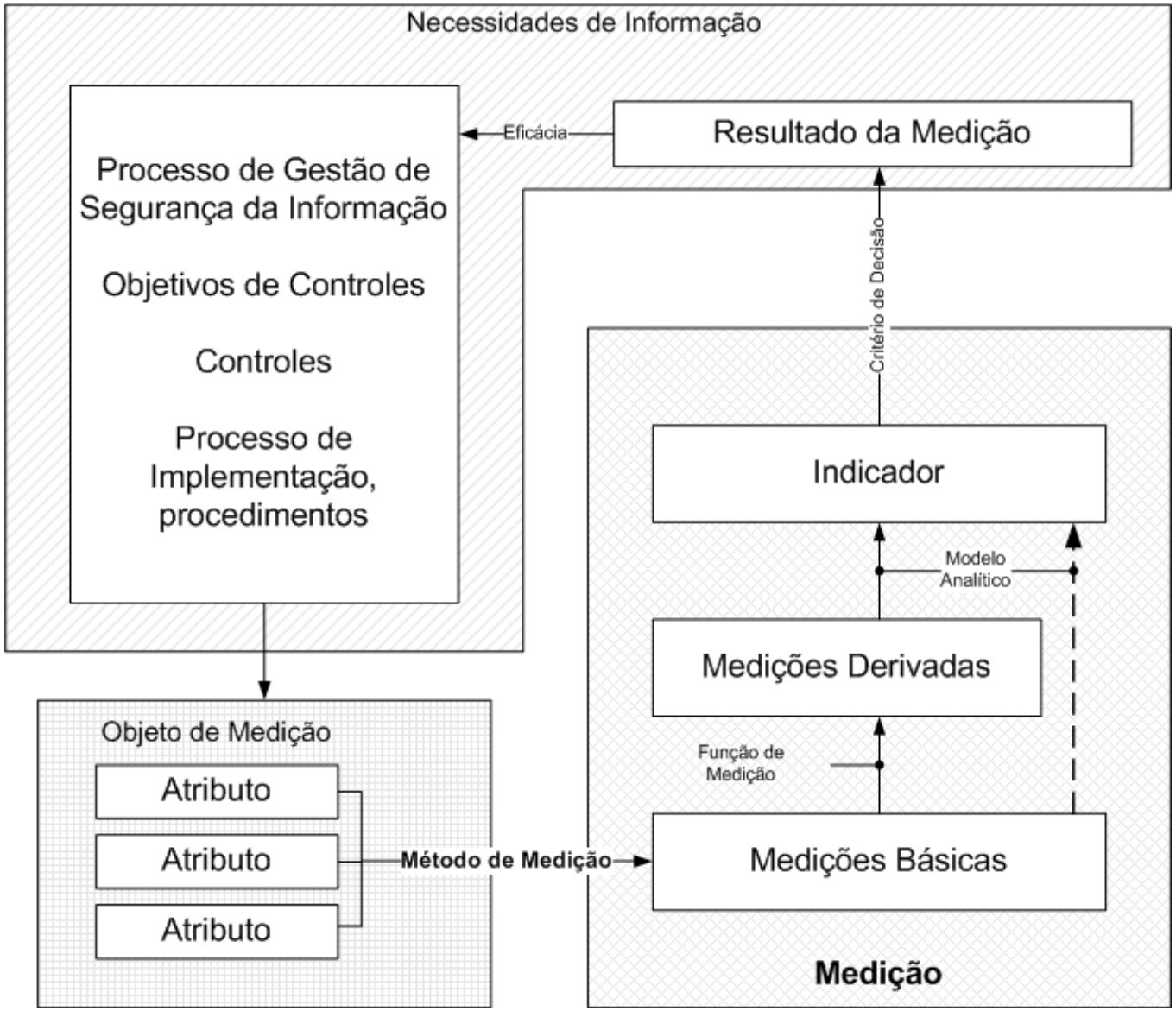
Normas e Procedimentos

- As normas detalham as diretrizes para um processo específico
- Os procedimentos dão o *how-to* de como cumprir a norma
- Exemplo:
  - A **diretriz** diz que a salvaguarda de informações sigilosas é uma obrigação de todos
  - Uma **norma** para o setor de RH define que informações classificadas como sensíveis devam ser criptografadas
  - Um **procedimento** explica como criptografar a informação

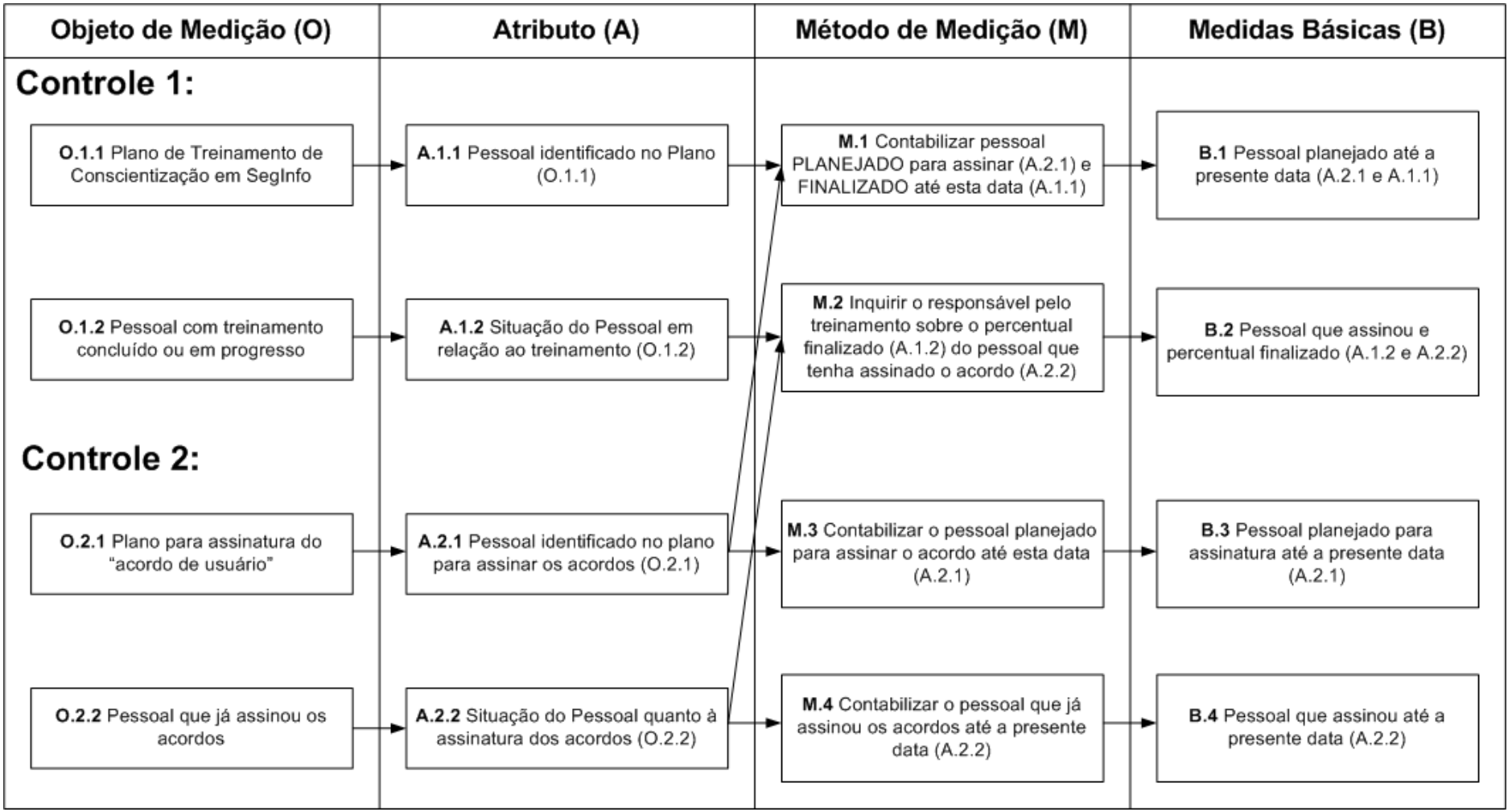
Análise Crítica do SGSI

- Uma vez adotada a SegInfo nos processos, uma forma de avaliar os resultados deve ser adotada para permitir a melhoria contínua
- A análise crítica é responsabilidade exclusiva da direção
- Deve se basear em medições desenvolvidas para o SGSI em análise – ISO 27004:2010

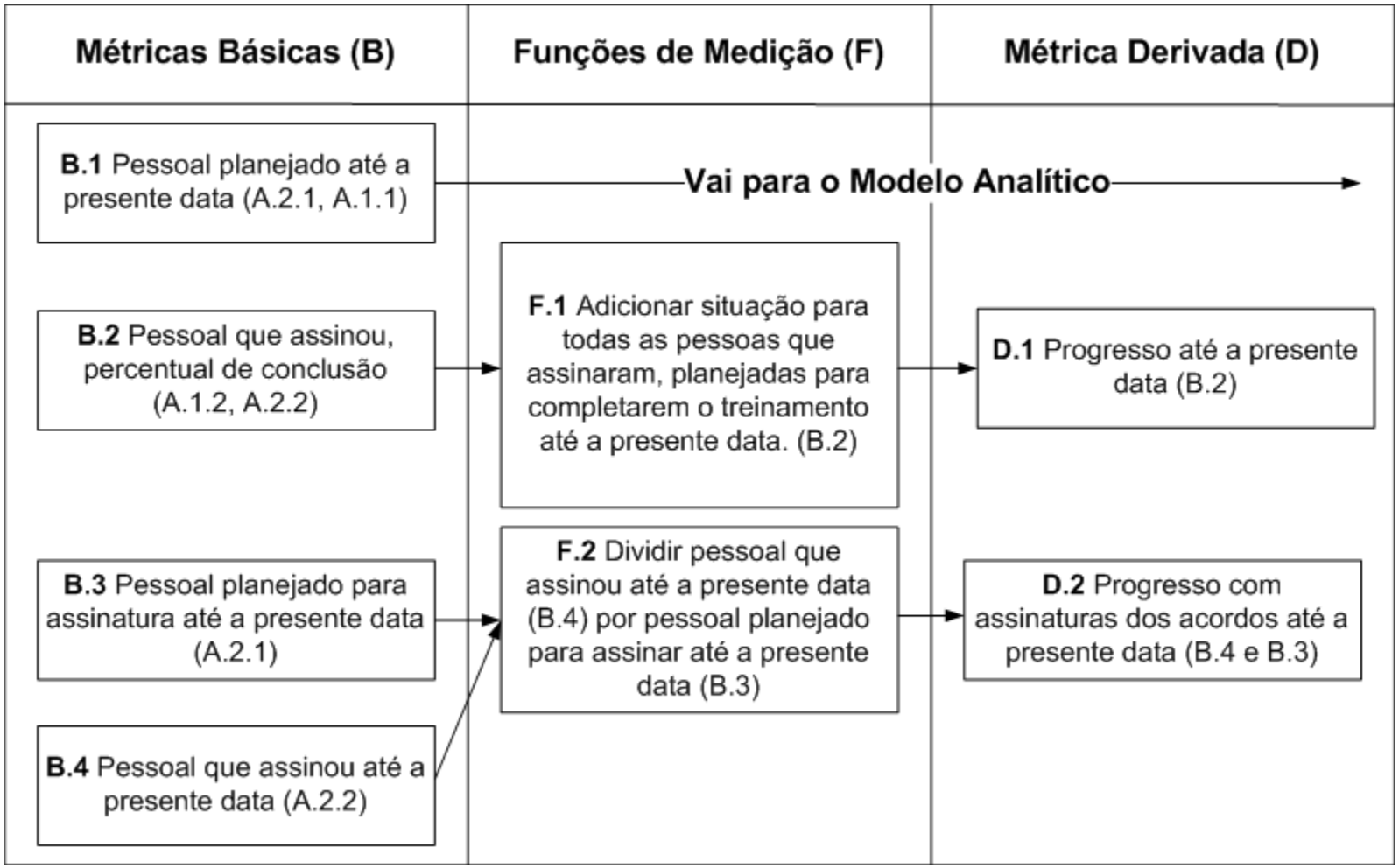
Processo de Medição



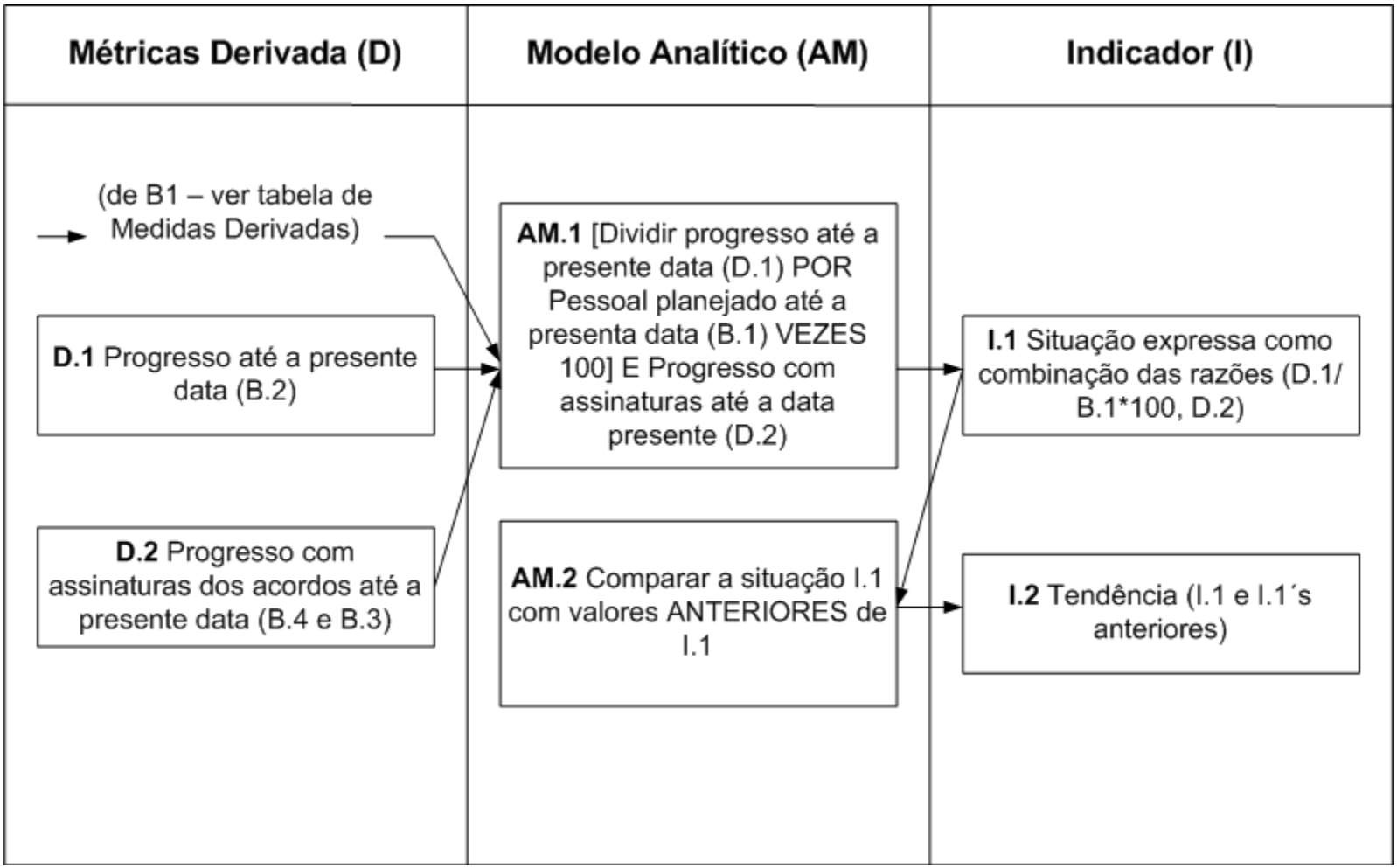
Medida Básica



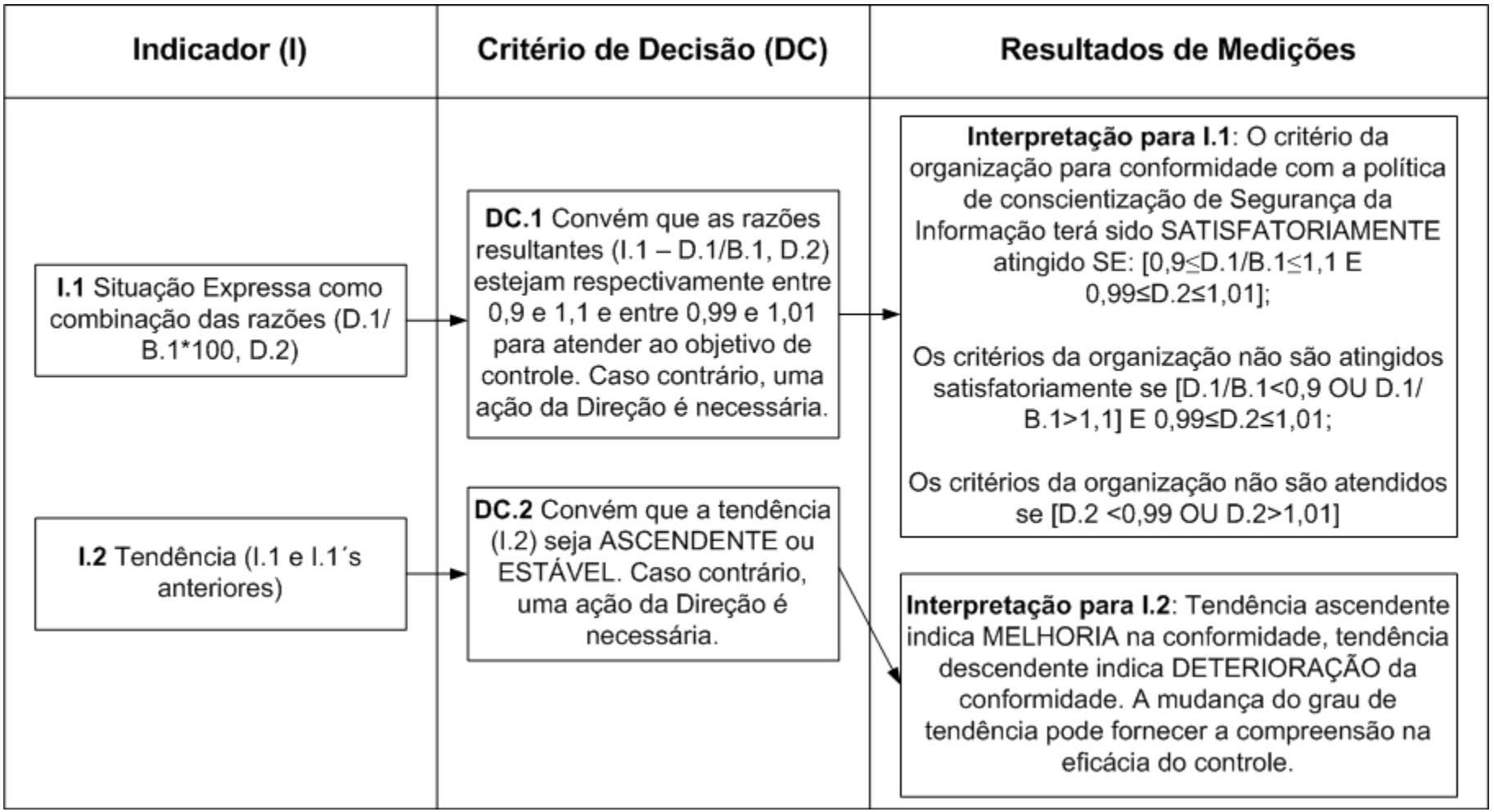
Medida Derivada



Modelo Analítico



Medição Final



Plano de Capacitação

- Deve conter as seguintes competências:
  - Identificação dos riscos, como motivador
  - Descrição clara dos termos técnicos necessários
  - Identificação dos canais de comunicação, para:
    - Esclarecer dúvidas
    - Comunicar ocorrências
    - Propor melhorias e sugestões
  - Desenvolver material de treinamento claro, objetivo e de fácil obtenção
  - Incluir avaliação da assistência

Conclusão

- A Segurança da Informação deve ser encarada como uma demanda do negócio
- Tem custos, mas pode agregar valor à marca e evitar prejuízos
- A segurança não pode “engessar” o negócio
- Entendendo que se trata de um processo lento e gradual, porém progressivo, é importante que se inicie o quanto antes possível.