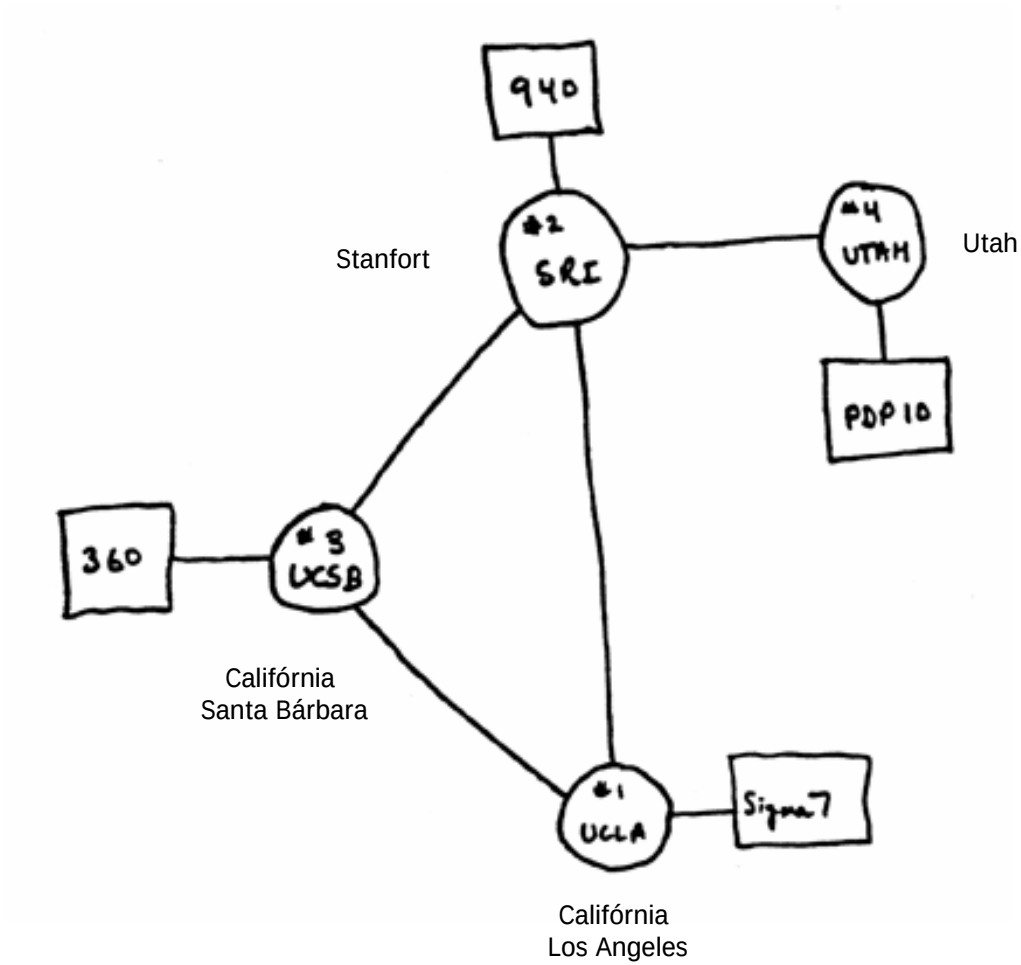
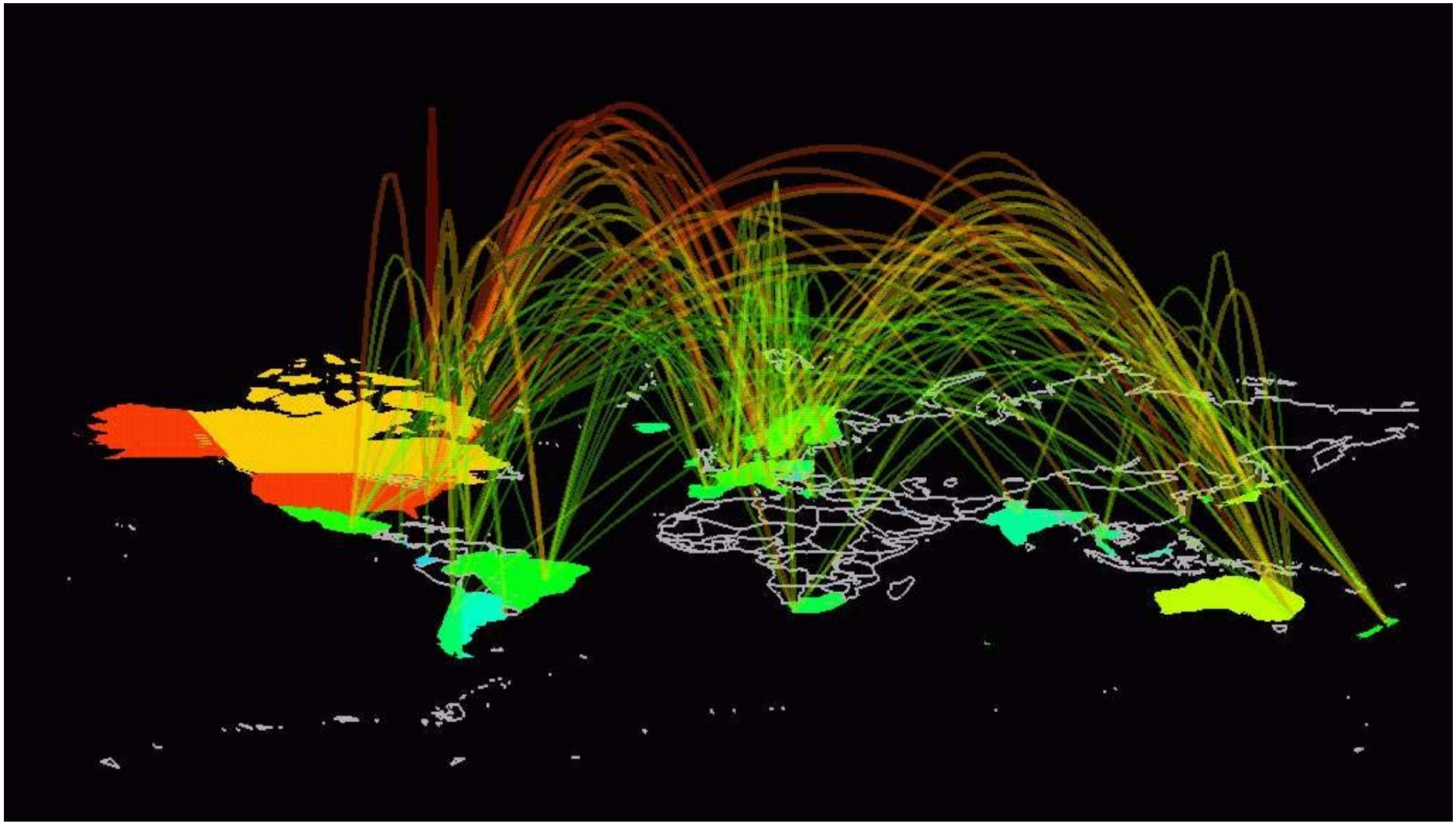
Fatos, equívocos e verdades que afetam a proteção dos negócios

» Autor
Marcos Sêmola
marcos@semola.com.br
Palestra Base 2005

Conectividade: 1967



Internet em 1992



Business

Metade das empresas investe incorretamente em segurança

Quinta-feira, 6 de Março de 2003 - 16h54

IDG Now!

Embora os departamentos de segurança da informação de corporações do mundo todo tenham recebido um aumento médio de 5% em seus orçamentos, um estudo do Giga Information Group revela que mais de 50% das empresas investiram em projetos de segurança incorretos e irrelevantes.

Como resultado, no início deste ano, a maioria das companhias americanas e européias, cortou 30% de seu orçamento de tecnologia destinado à segurança para se aproximar do total mais provável a ser investido neste setor em 2003.

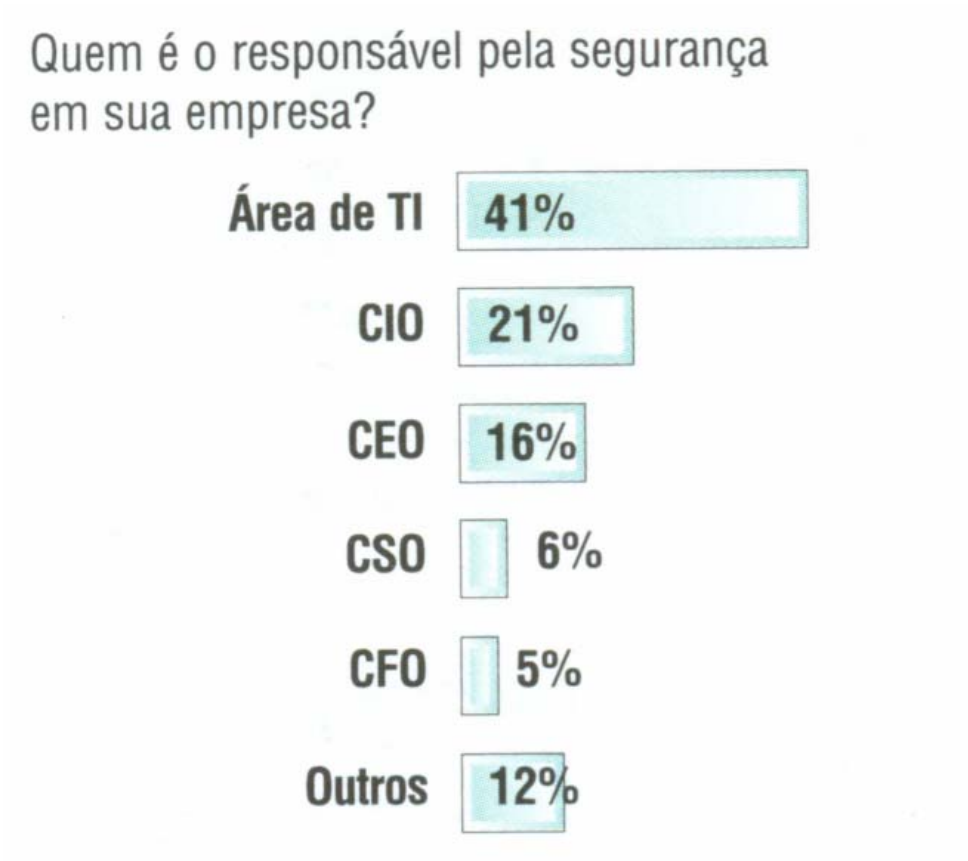
Entretanto, segundo Steve Hunt, analista da Giga Information Group, a maioria dos departamentos de segurança de TI estão economizando bastante sob o ponto de vista estratégico e administrativo. Por isso, cortes em curto prazo não poderão ultrapassar a marca dos 5%.

Para uma redução de custos de 10% a 15%, o analista acredita que seria necessário terceirizar tarefas táticas, como o gerenciamento remoto de firewalls.

A pesquisa ainda informa que, antes dos ataques terroristas de 11 de setembro de 2001, apenas 30% entre todas as empresas norte-americanas e européias tinham capacitado uma pessoa para mapear medidas de segurança.

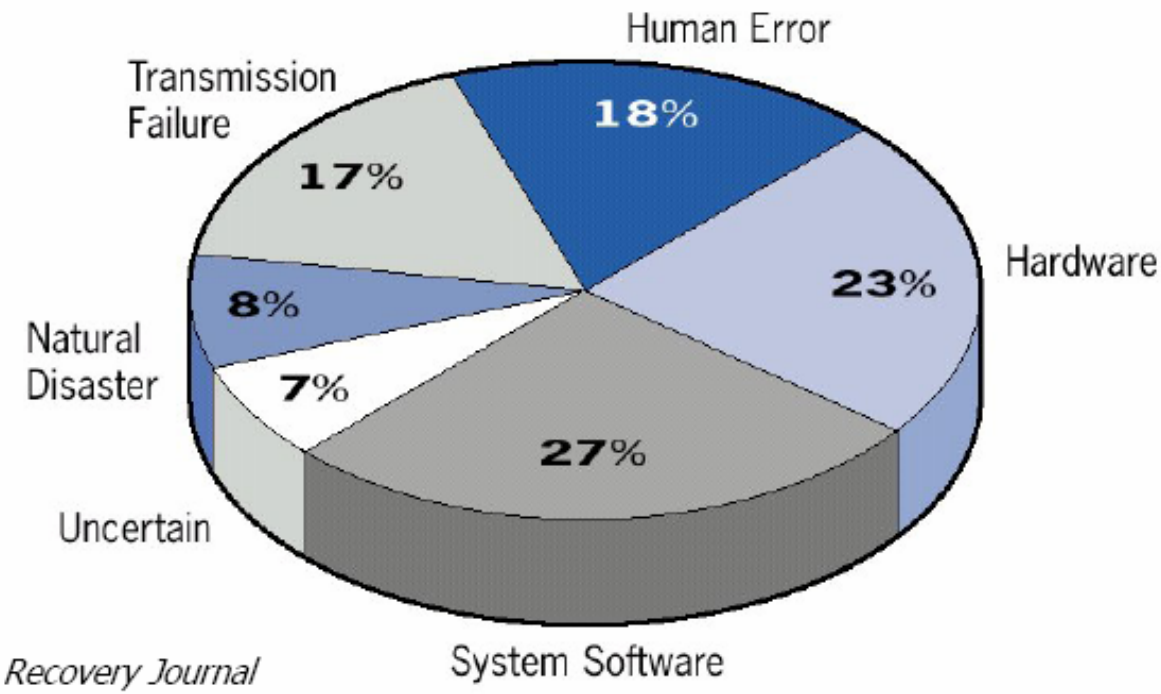
Este ano, o Giga prevê que mais de 90% de todas as organizações nomearão um indivíduo ou um departamento especial para essa tarefa.

Causa x Efeito



Publicada em 04/02/04 no Valor Econômico

Principais agentes de indisponibilidade dos negócios



Fonte: Disaster Recovery Journal

VAZAMENTO

FRAUDE

ERRO

CONTAMINACÃO

SABOTAGEM

INDISPONIBILIDADE

Fato
Segurança faz parte da agenda

1

COMPUTERWORLD

Busca

IDG BRASIL

- Carreira
- Segurança
- Gestão
- Tecnologia
- Mercado

- Fale conosco
- As
- As

Edições Anteriores

Revista Impressa São Paulo, 8 fevereiro de 2005

ADS POWERED BY: PREDICTA MAESTRO

O que priorizar em 2005?

Segunda-feira, 31 janeiro de 2005 - 13:26

Luciana Coen

Apesar de ser um tema recorrente na área de TI, a segurança dos sistemas de informação sempre ficou relegada a segundo plano - quando não a terceiro -

O que priorizar em 2005?

Prévia da pesquisa anual Agenda CIO, do Gartner, revela que segurança e adequação de sistemas de TI às normas e leis internacionais estão no topo da lista de preocupação das empresas.

[31/01/2005 13:26]

dobre em relação ao ano passado, quando cerca de mil executivos participaram do levantamento que busca elencar os produtos e tecnologias que estarão na pauta de prioridades durante o ano. Ione observa que a pesquisa aponta que, se não fosse a obrigatoriedade de adequação à lei norte-americana que controla o mercado de capitais e as normas do acordo Basiléia 2 de disciplina financeira internacional, que estipula um teto de empréstimos das instituições, a prioridade de investimento estaria em ferramentas de business intelligence (BI), que ficou em segundo lugar no levantamento.

Equívoco
Motivações secundárias + importantes

1

- Para seguir uma tendência de mercado
- Para ser reconhecida como uma empresa visionária
- Para ganhar prêmios pela governança corporativa
- Para estar à frente da concorrência
- Para não ficar atrás da concorrência
- Para demonstrar solidez
- Para atrair investidores
- Para fortalecer a imagem de credibilidade da marca
- Para respeitar regulamentações setoriais ou leis

Alinhamento
Motivações legítimas para o negócio

1

Americanas.com representou 13.3% do total de vendas da rede, que hoje conta com 137 lojas espalhadas pelo País. "Há uma expectativa de crescimento forte para este ano", diz o diretor comercial da companhia, Ronney Pastro.

O número de fraudes bancárias e financeiras realizadas via internet no País cresceu 577% em 2004, revelou o balanço do Grupo de Resposta a Incidentes para a Internet Brasileira (NBSO), mantido pelo Comitê Gestor da Internet.

ameaças internas e externas, e da necessidade de adequação e muitas delas às novas normas e regulamentações nacionais e internacionais, como Sarbanes-Oxley, Basiléia 2 e Solvência, o assunto começou a ganhar destaque na agenda de prioridades dos CIOs. E a preocupação deve prosseguir neste ano. Isso pelo menos é o que indica a prévia da pesquisa anual Agenda CIO realizada pelo Gartner, a qual o COMPUTERWORLD teve acesso com exclusividade. "Por causa de leis como a Sarbanes-Oxley, segurança tornou-se o tema principal. Há até um pouco de paranóia", avalia a coordenadora do

Fato
Todo negócio possui risco

2

$$\text{Risco} = \frac{\text{Ameaças x Vulnerabilidades}}{\text{Contramedidas}} \times \text{Valor}$$

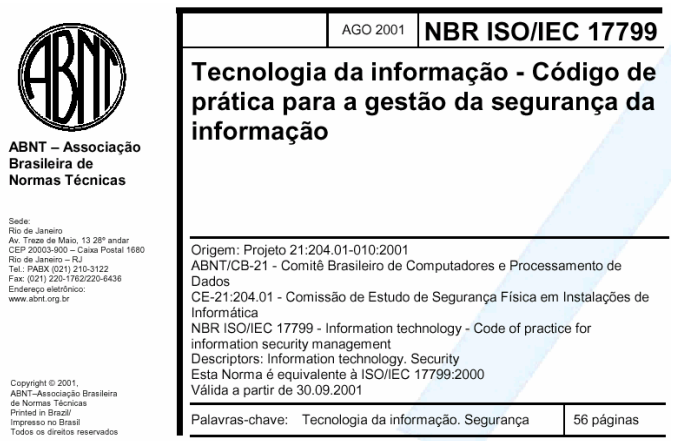
Risco inerente: não considera contramedidas existentes
Risco presente: considera contramedidas existentes
Risco residual: considera contramedidas existentes e recomendadas

Equívoco
Os recursos são ilimitados

2

- Escopo vertical x Escopo horizontal x Tempo

  - Política de Segurança da Informação
  - Segurança Organizacional
  - Classificação e controle dos ativos de informação
  - Segurança em pessoas
  - Segurança Física e Ambiental
  - Gerenciamento das operações e comunicações
  - Controle de Acesso
  - Desenvolvimento de Sistemas e Manutenção
  - Gestão da continuidade do negócio
  - Conformidade



ABNT – Associação Brasileira de Normas Técnicas

Sede:
Rio de Janeiro
Av. Treze de Maio, 13 28º andar
CEP 20003-900 – Caixa Postal 1680
Rio de Janeiro – RJ
Tel.: PABX (021) 210-3122
Fax: (021) 220-1762/220-6436
Endereço eletrônico:
www.abnt.org.br

AGO 2001 **NBR ISO/IEC 17799**

Tecnologia da informação - Código de prática para a gestão da segurança da informação

Origem: Projeto 21:204.01-010:2001
ABNT/CB-21 - Comitê Brasileiro de Computadores e Processamento de Dados
CE-21:204.01 - Comissão de Estudo de Segurança Física em Instalações de Informática
NBR ISO/IEC 17799 - Information technology - Code of practice for information security management
Descriptors: Information technology. Security
Esta Norma é equivalente à ISO/IEC 17799:2000
Válida a partir de 30.09.2001

Palavras-chave: Tecnologia da informação. Segurança | 56 páginas

127
Controles

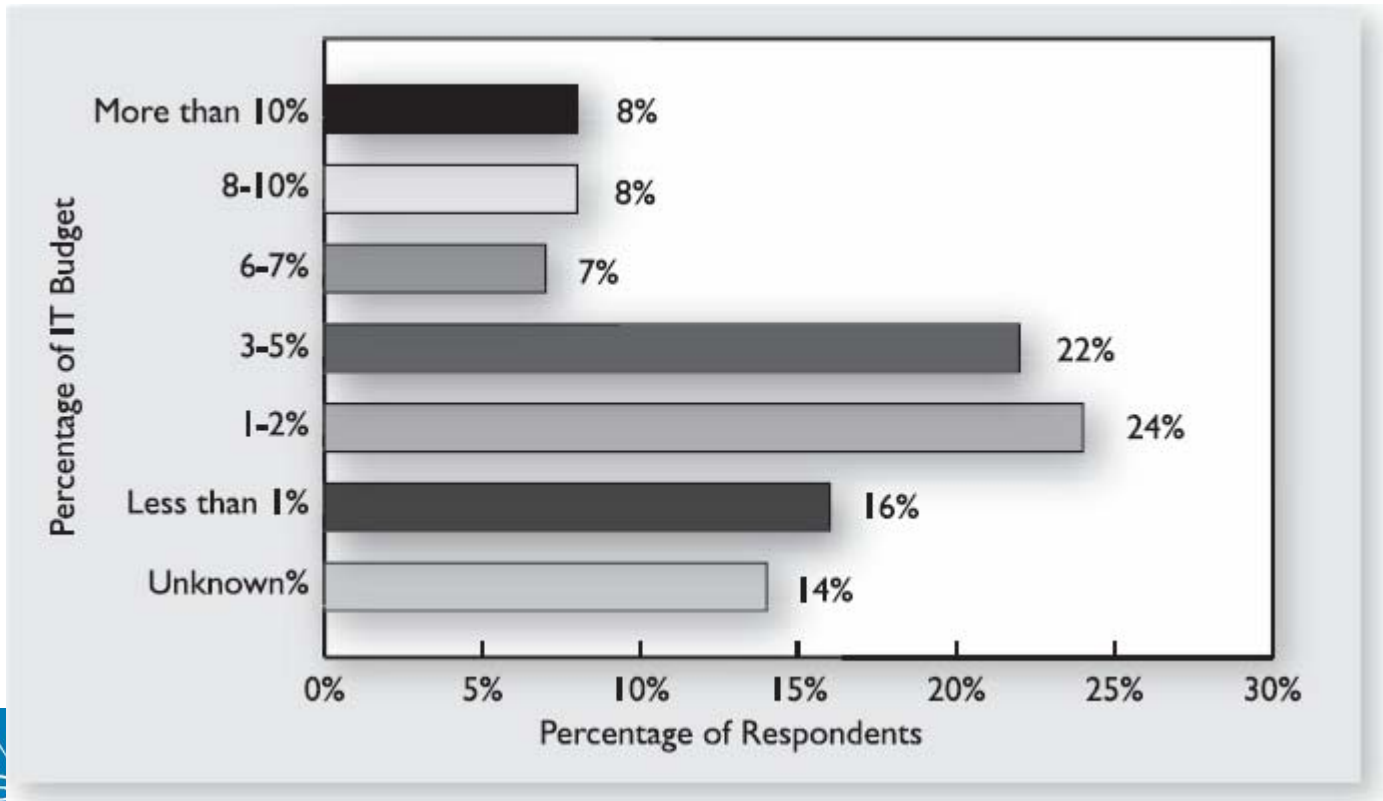
Alinhamento
É vital priorizar os investimentos

2

Fato
A tecnologia é uma fonte de riscos

3

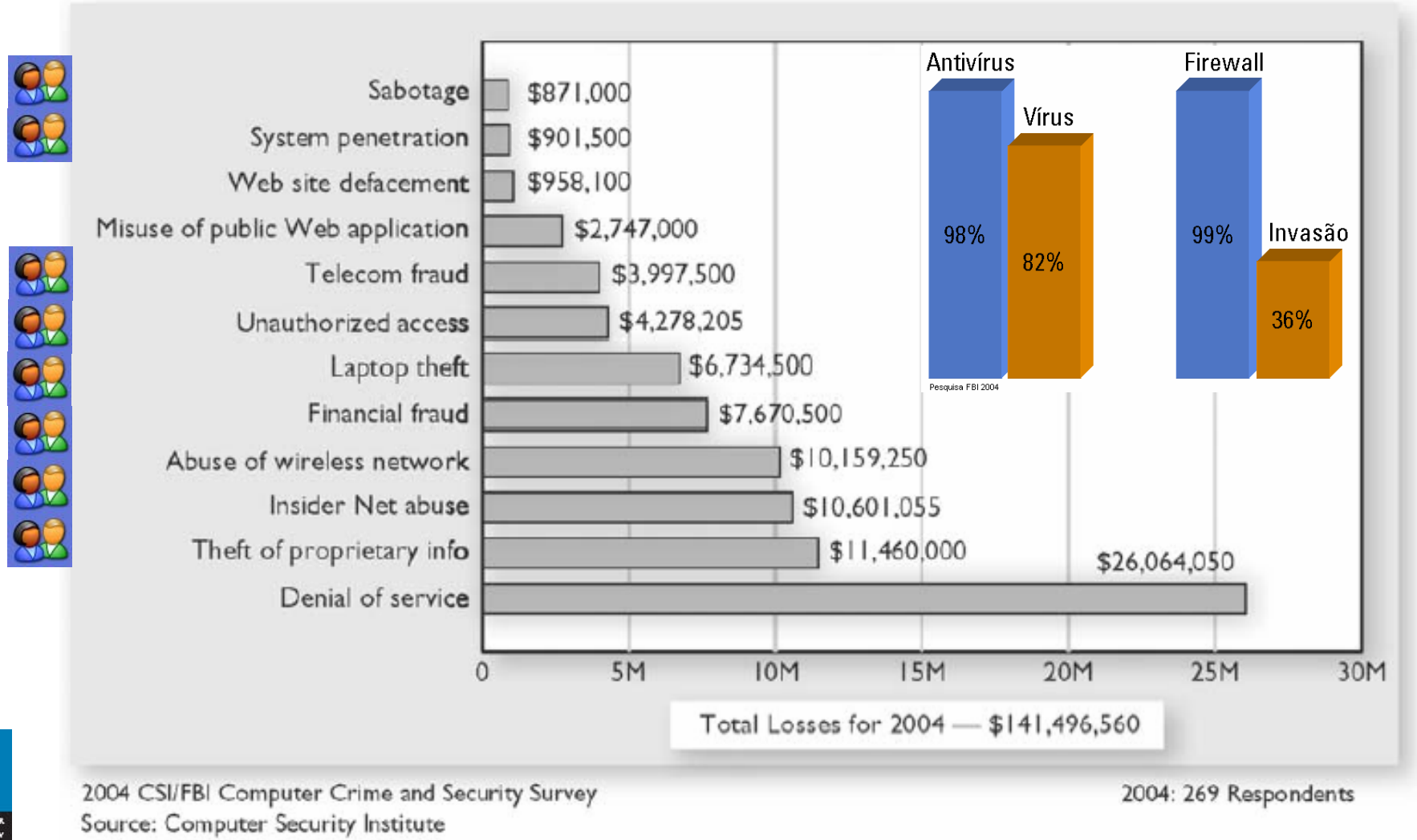
Tipos de ataques ou abusos nos últimos 12 meses.



Jornal Valor Econômico 2004

Equívoco
A tecnologia é a única fonte de riscos

3

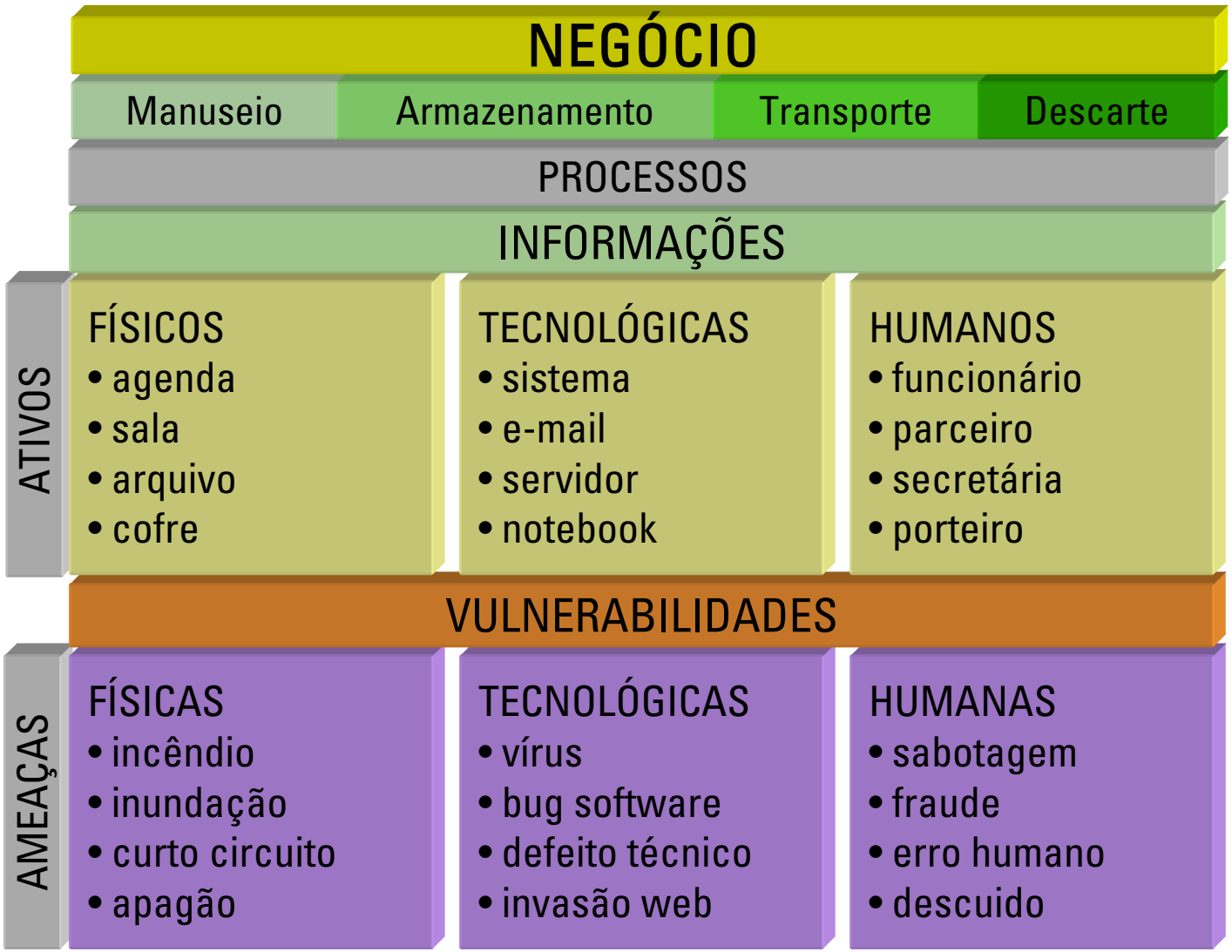


2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

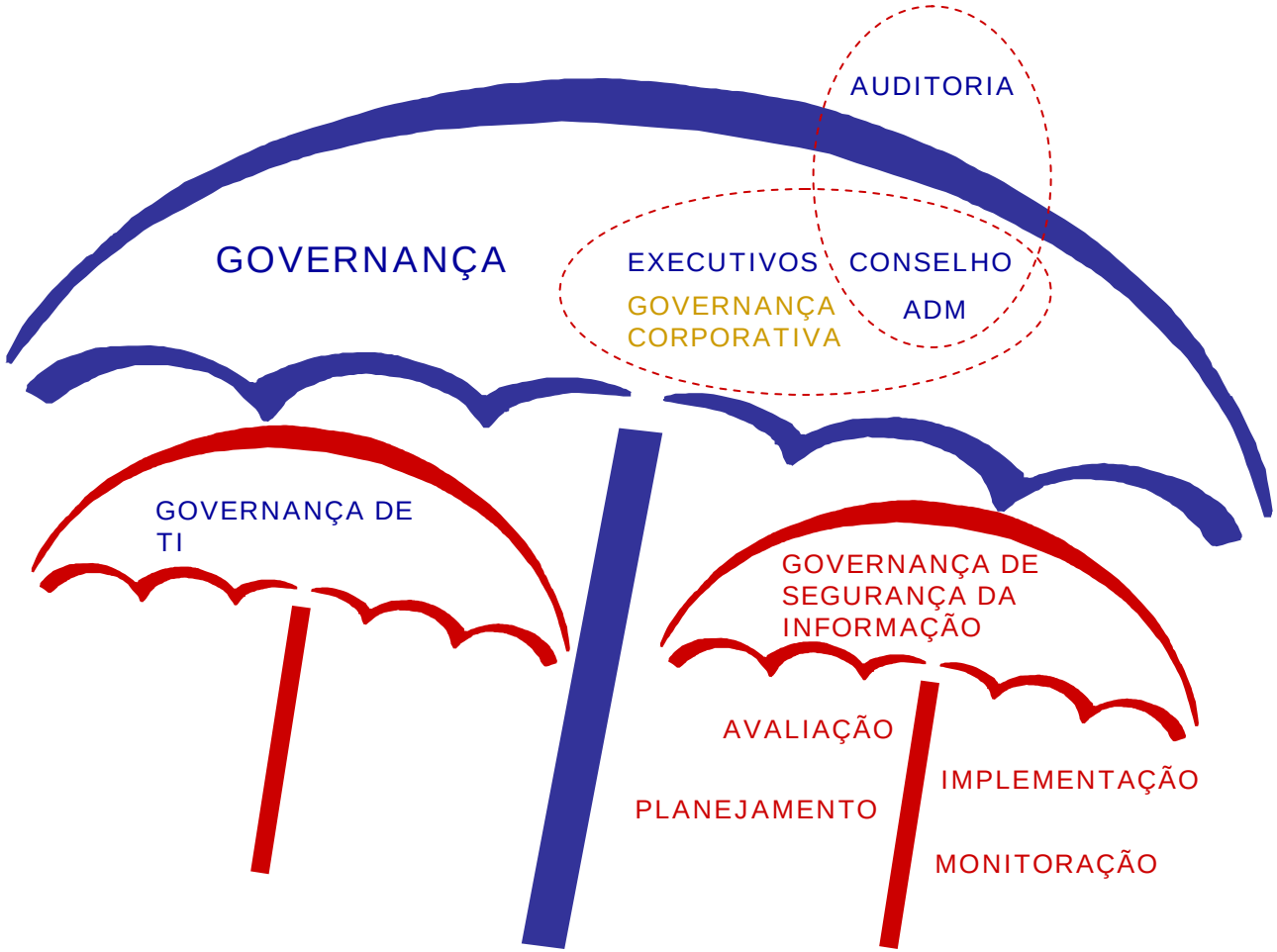
Alinhamento
Multiplos ativos suportam o negócio

3



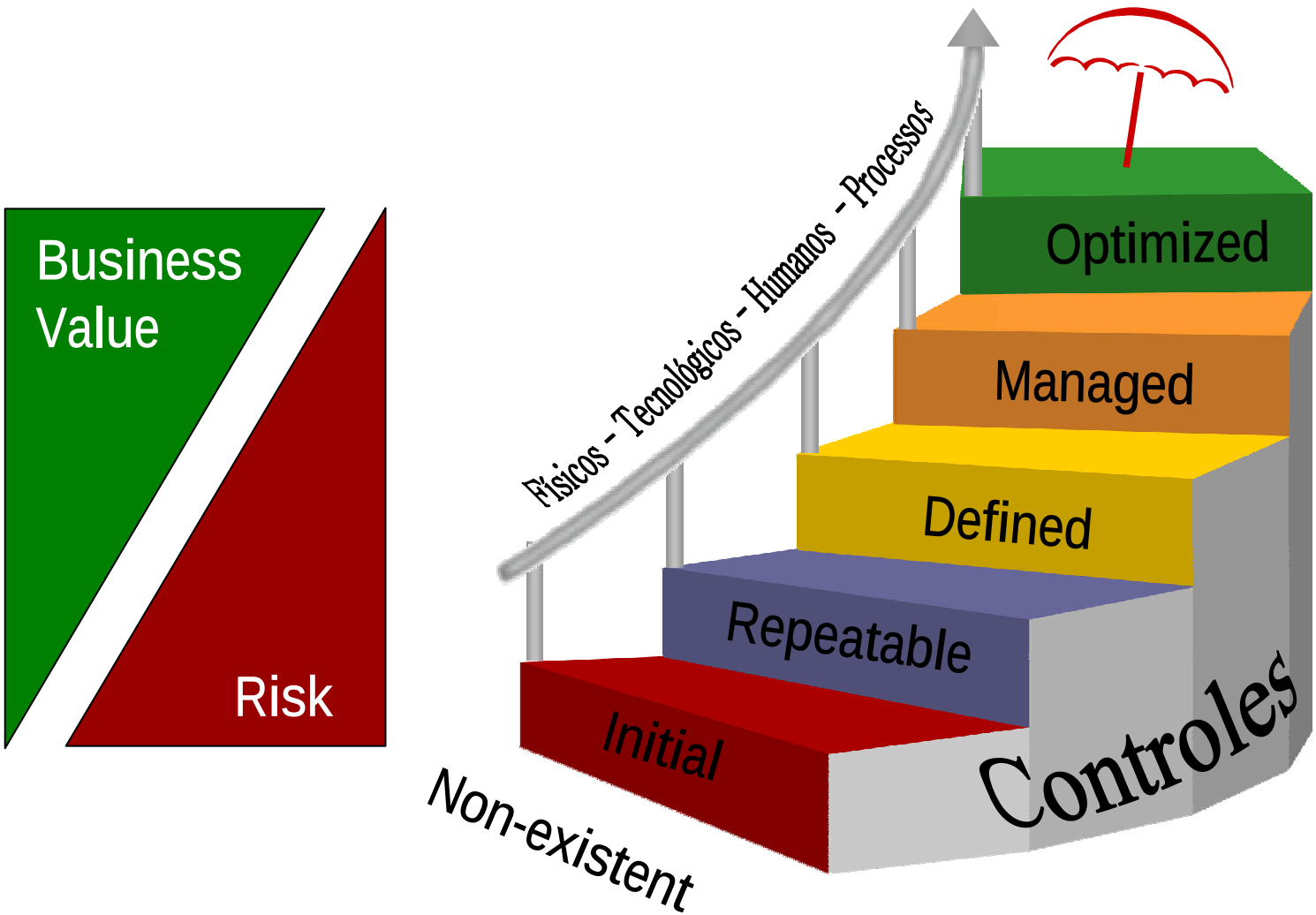
Governança Corporativa

Modelo de Gestão



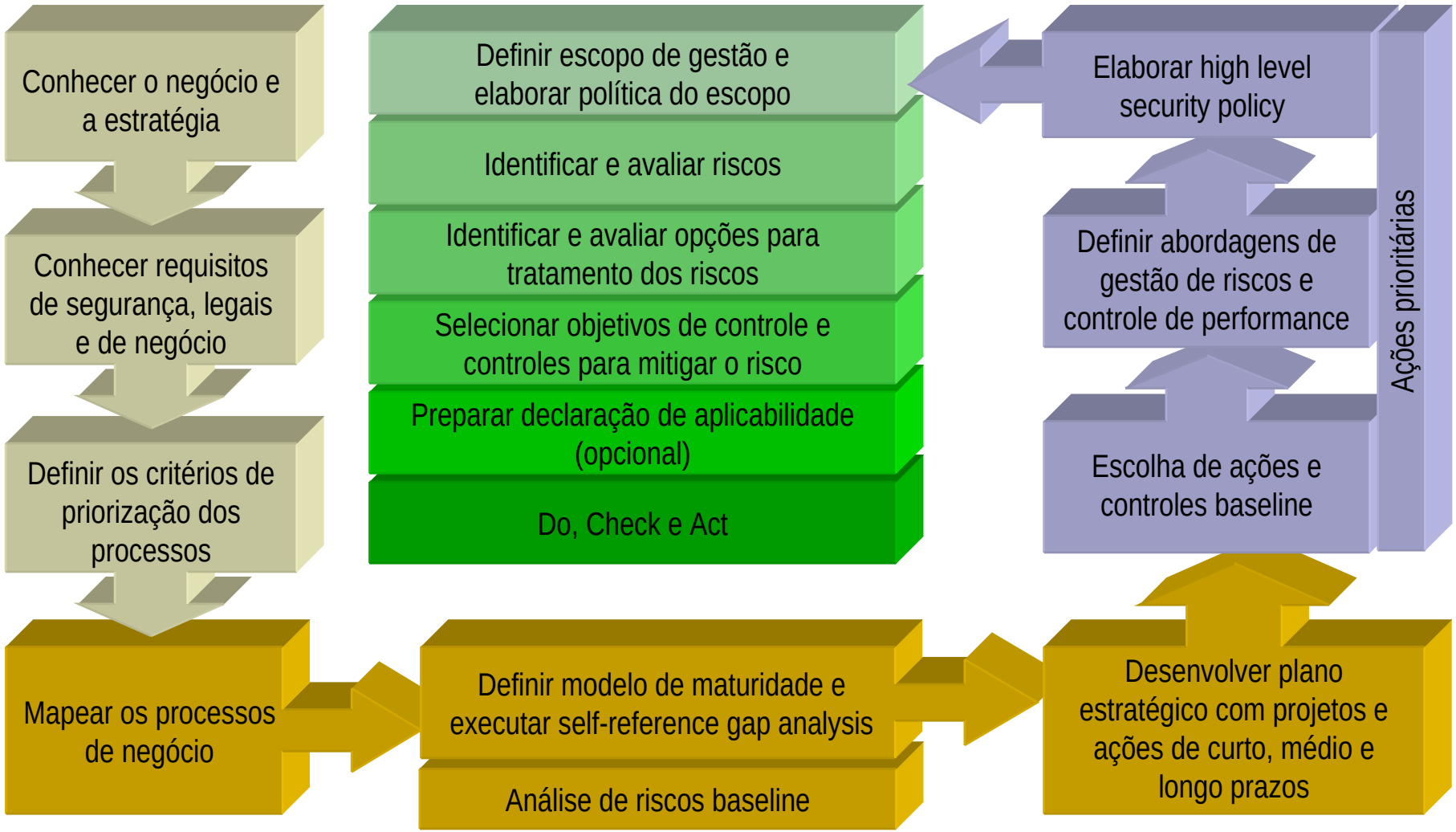
Evolução da Segurança Organizacional

Análise da Maturidade de Segurança

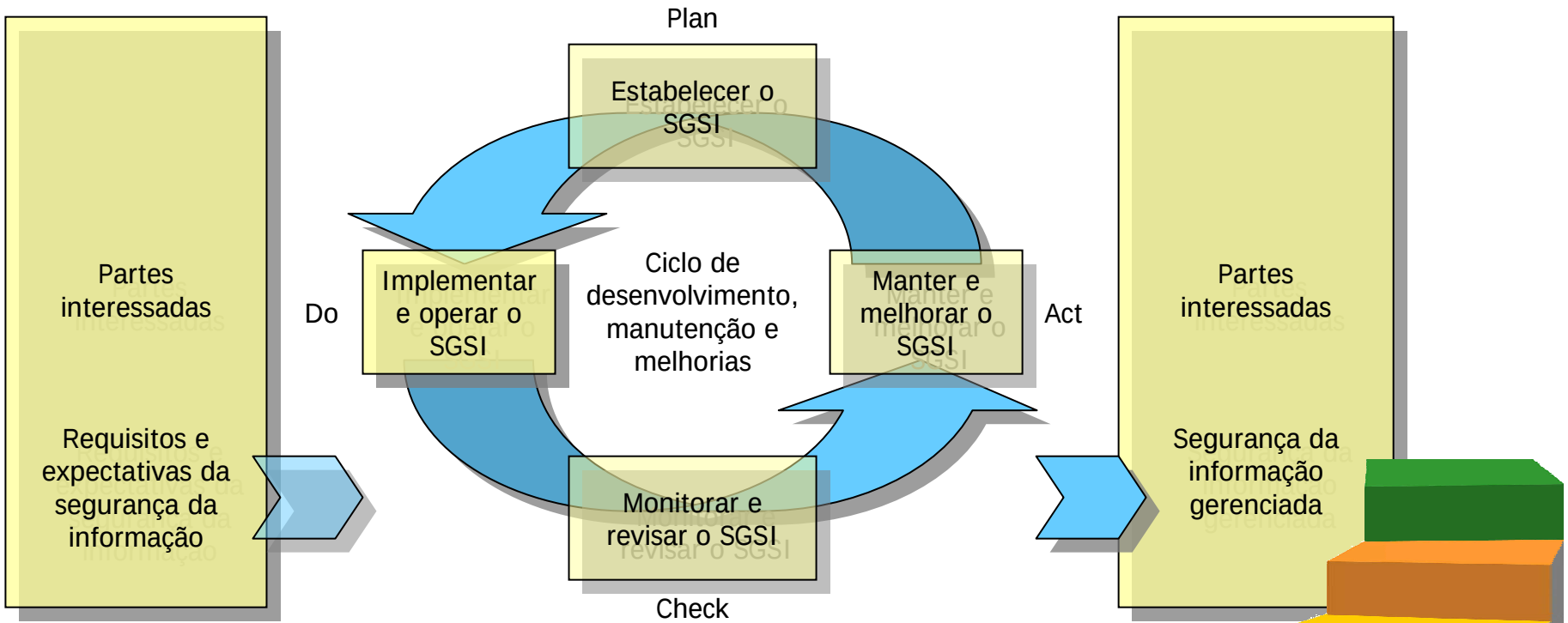


Fonte: Atos Origin

Visão funcional
Planejamento Estratégico



Visão gerencial
Framework de governança de segurança



PDCA model applied to ISMS process
Fonte: BS 7799-2:2002 (tradução livre)

Modelo de Maturidade COBIT

0 Non-existent
Management processes are not applied at all

1 Initial
Processes are ad hoc and disorganized

2 Repeatable
Processes follow a regular pattern

3 Defined
Processes are documented and communicated

4 Managed
Processes are monitored and measured

5 Optimized
Best practices are followed and automated

Fonte: ISACA/COBIT

Fator motivacional

O elemento chave é MOTIVAÇÃO

O Investidor se motiva pela... VALORIZAÇÃO DO INVESTIMENTO

O CEO se motiva pelo... RESULTADO DO NEGÓCIO

O CFO se motiva pela... CREDIBILIDADE DAS INFORMAÇÕES

O CIO se motiva pela... EFICIÊNCIA DOS SERVIÇOS

O CSO se motiva pela... EFICÁCIA DA ADMINISTRAÇÃO DOS RISCOS

O Diretor se motiva pela... PRODUTIVIDADE DOS PROCESSOS

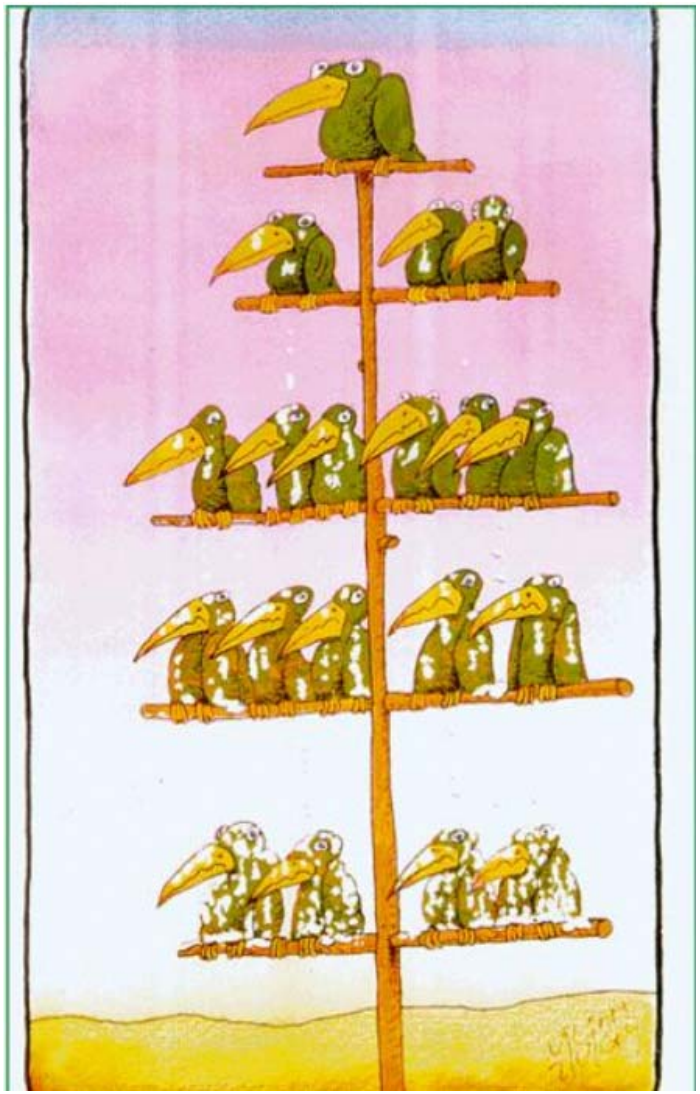
O Gerente se motiva pela... PRODUTIVIDADE DOS FUNCIONÁRIOS

O Usuário se motiva... POR QUE?

Em toda a cadeia corporativa de segurança, deve existir motivação específica para comprometer espontaneamente todos os níveis em todos os momentos de risco.

Fator motivacional

Investidor
CEO
CFO
CIO
CSO
Diretor
Gerente
Usuário



Na falta de qualquer elo motivacional a cadeia corporativa de segurança se desestrutura.

E quanto mais alto estiver o elo defeituoso, piores serão os efeitos gerados em cascata.

Os desafios de segurança são abrangentes, transcendem TI e devem assumir o perímetro corporativo…

...quando isso não ocorre, ações isoladas geram uma falsa sensação de segurança e não protegem o negócio.

Muitos riscos são assumidos sem uma avaliação de impacto que tenha apoiado esta decisão...

...e é fato que se existirem duas maneiras de executar uma tarefa, alguém escolherá a maneira mais arriscada.

Os recursos são limitados, por isso, é preciso priorizar as ações considerando as ameaças mais relevantes...

...e mesmo que muitas delas sejam de TI e requeiram investimentos em soluções tecnológicas de ponta...

...será preciso cuidar especialmente do ativo humano, por ser o ponto mais fraco do sistema.

É igualmente importante considerar os agentes naturais e as situações de risco impensadas, pois elas ocorrerão...

...e quando ocorrer, você deverá estar preparado de posse de um plano de continuidade de negócios.

E como se não bastasse, a equação de risco é dinâmica e há todo instante nasce uma nova e revolucionária ameaça.

Obrigado.

Marcos Sêmola, CISM
marcos@semola.com.br