

A importância da Gestão da Segurança da Informação



Marcos Sêmola

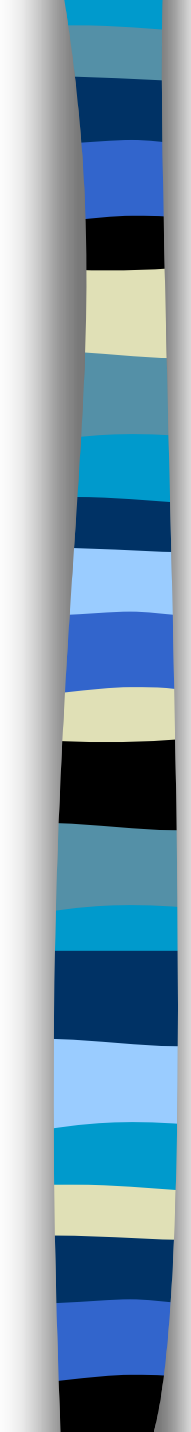
Consultor em Gestão de
Segurança da Informação

marcos@semola.com.br

Apresentação

- **Consultor em Gestão de Segurança da Informação**
12 anos de experiência em projetos de Tecnologia da Informação
05 anos de experiência como Consultor Sênior e Gerente Nacional de Serviços de Segurança da Informação (ex-Módulo)
- **Professor da Fundação Getúlio Vargas**
Gestão de Segurança da Informação para os cursos MBA
- **MBA em Tecnologia Aplicada/FGV**
Mestrando em Economia Empresarial
Pós Graduado em Marketing e Estratégia de Negócios
Pós Graduado em Redes Locais
Bacharel em Ciência da Computação
- **Autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed. Campus 2003**
Articulista em publicações do especializadas
Escritor da coluna Firewall da IDGNow
Palestrante em congressos no Brasil
Integrante da comissão de estudos CB-21/ISO17799

Agenda

- 
- Conceitos fundamentais
 - A importância da informação
 - Informação vs Segurança
 - Respondendo as perguntas:
 - QUE informações proteger
 - POR QUE proteger
 - QUANDO proteger
 - ONDE proteger
 - O QUE proteger
 - DO QUE proteger
 - COMO proteger
 - A importância da gestão
 - A norma BS7799/ISO17799

Por que falar de
Informação e
Segurança?

Informação

1 Ato ou efeito de informar. 2 Transmissão de notícias. 3 Instrução, ensinamento. 4 Transmissão de conhecimentos. 5 Opinião sobre o procedimento de alguém. 6 Investigação. 7 Inquérito.

Fonte: Dicionário Michaelis

Seguro (Segurança)

1 Livre de inquietações. 2 Sossegado. 3 Confiado. 4 Livre de perigo ou não exposto a ele. 5 Que oferece segurança contra ataques, acidentes, desastres ou danos de qualquer outra natureza...

Fonte: Dicionário Michaelis

Informação

Possuir Informação é ganhar agilidade, competitividade, previsibilidade, dinamismo. Informação é um diferencial!



atividade de
um indivíduo
comum

- aumento da gasolina
- aumento da inflação
- precipitação de chuvas
- promoção da passagem aérea
- limite salarial para um cargo
- queda da Bovespa
- planos do seu chefe para você
- abandono da sua empregada
- mudança no Código Civil
- ...

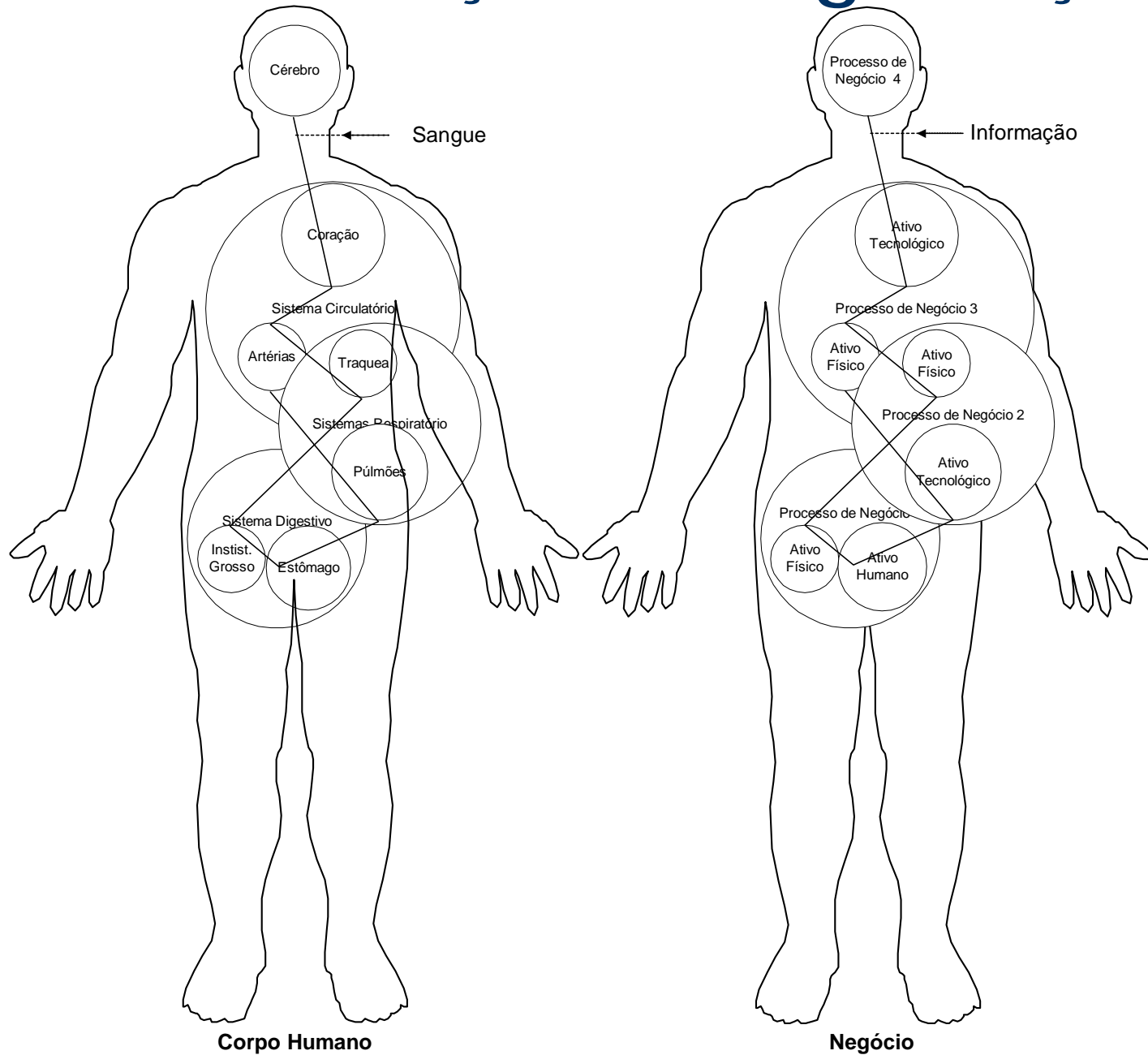


negócio de
uma empresa

- discurso do presidente Lula
- conflito no Oriente Médio
- valorização do Petróleo
- tendências tecnológicas
- planos do concorrente
- oscilação da taxa de juros
- plano de greve funcionários
- falência de uma parceira
- resultados do último exercício
- ...

Informações úteis que podem ser usadas a seu favor ou contra você e sua empresa.

Informação vs Segurança



Informação vs Segurança



CASE



atividade de
um indivíduo
comum

Informação vs Segurança

■ QUE informações precisam de segurança?

- Identidade
- CPF
- Endereço residencial
- Telefone celular
- Código da maleta
- Senha da agenda eletrônica
- Informações bancárias e senhas
- Senhas de acesso da empresa
- Número do Cartão de Crédito
- \$ espécie na carteira
- \$ patrimônio
- \$ saldo bancário
- \$ prêmio do seguro de vida e beneficiários
- Rotina e horários de trabalho



atividade de
um indivíduo
comum

INFORMAÇÕES

• **ONDE DEIXA A CHAVE RESERVA PARA A EMPREGADA!**

Informação vs Segurança

■ POR QUE proteger as informações?



atividade de
um indivíduo
comum

- Por seu valor
- Pelo impacto de sua ausência
- Pelo impacto resultante de seu uso por terceiros
- Pela importância de sua existência
- Pela relação de dependência com a sua atividade
- ...



Informação vs Segurança

■ QUANDO proteger as informações?

Durante seu ciclo de vida

- Manuseio
- Armazenamento
- Transporte
- Descarte



atividade de
um indivíduo
comum

Manuseio

Armazenamento

Transporte

Descarte

INFORMAÇÕES

Informação vs Segurança

■ ONDE proteger as informações?

Nos ativos que as custodiam:

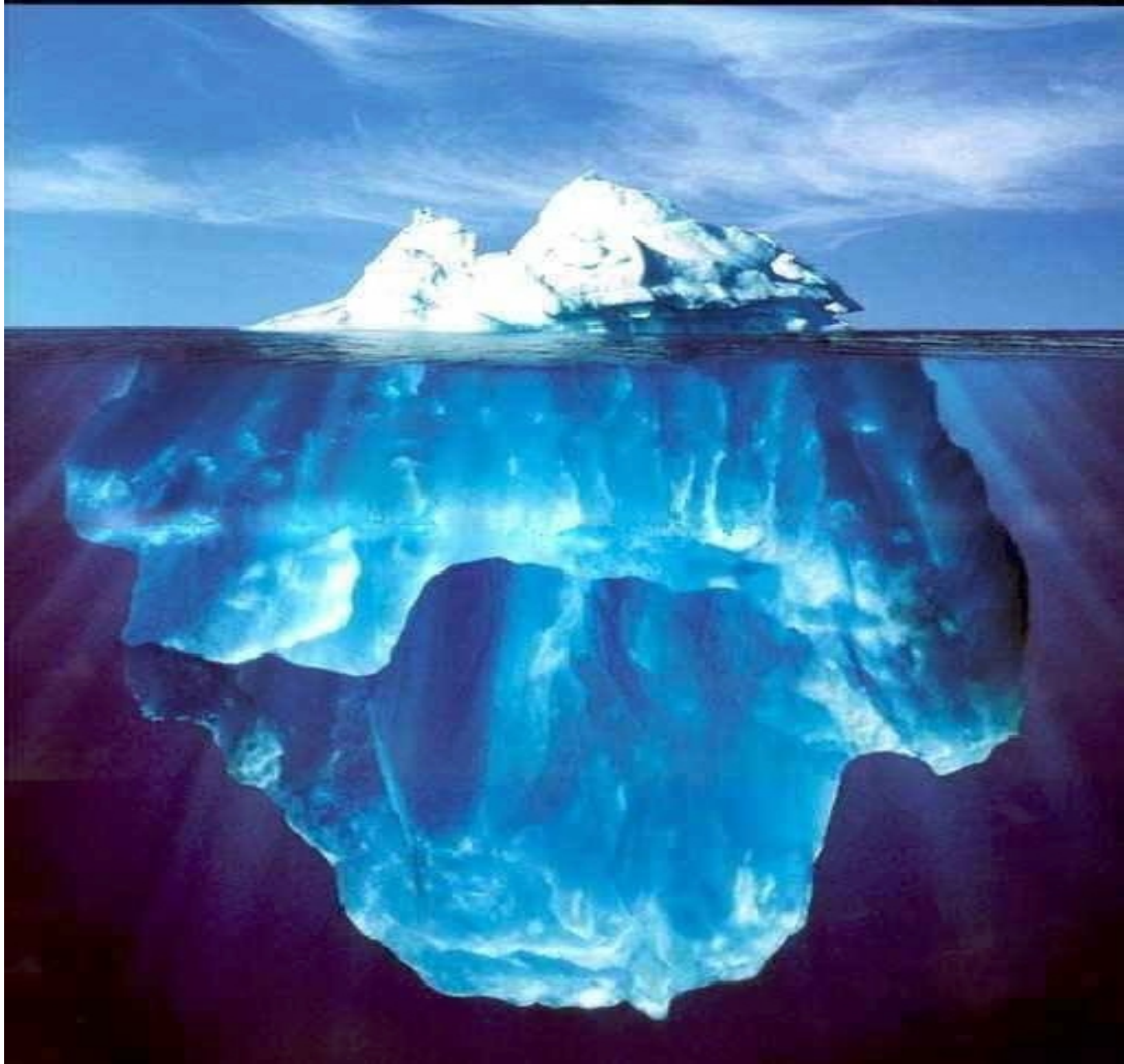
- Físicos
- Tecnológicos
- Humanos



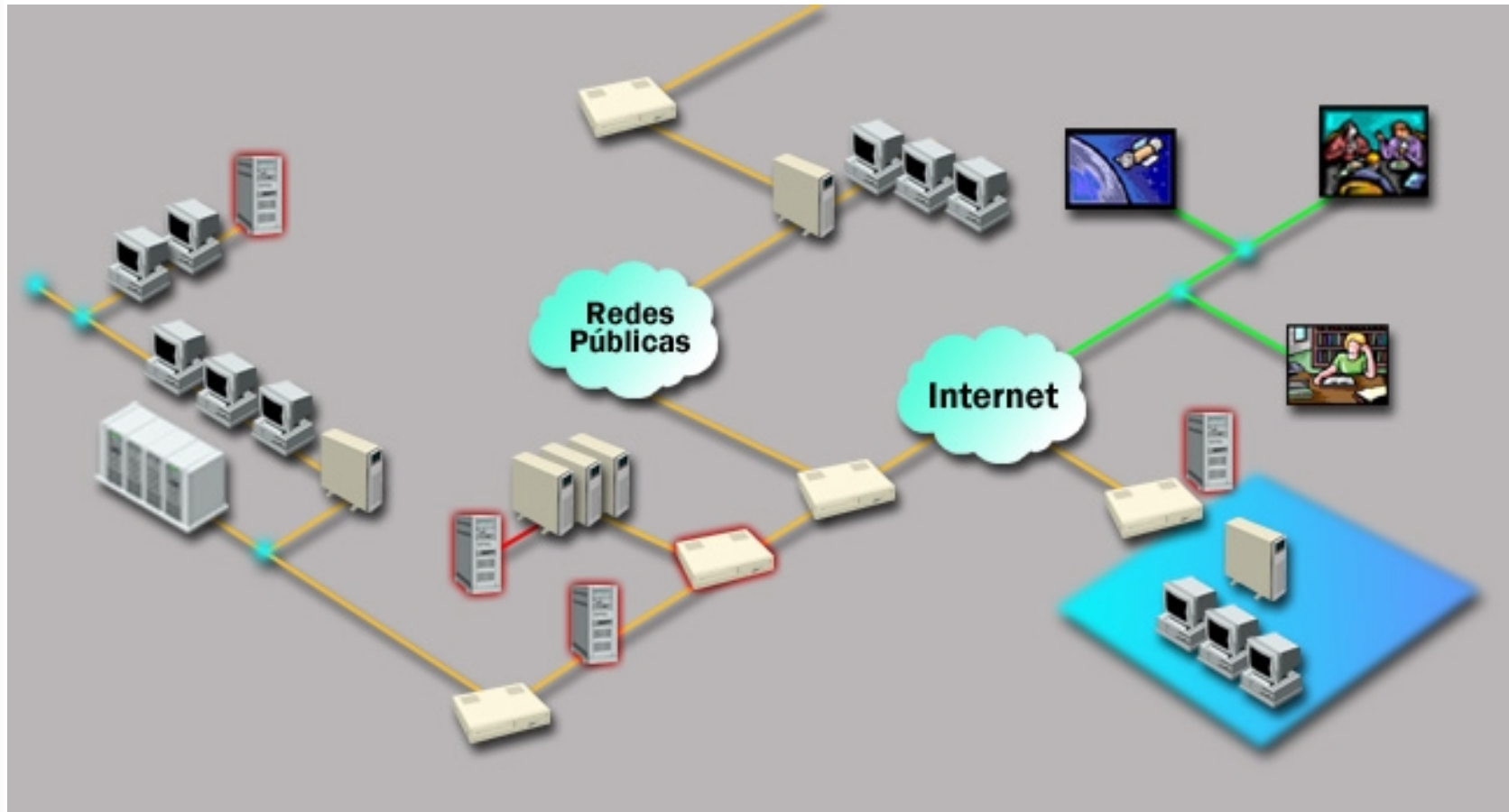
atividade de um indivíduo comum

ATIVOS	FÍSICOS	TECNOLÓGICAS	HUMANOS
	<ul style="list-style-type: none">• agenda• sala• arquivo• cofre	<ul style="list-style-type: none">• sistema• e-mail• servidor• notebook	<ul style="list-style-type: none">• funcionário• parceiro• secretária• porteiro

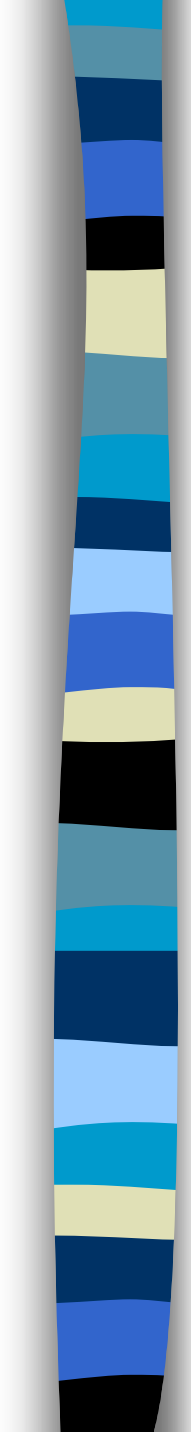
Miopia do Iceberg



Miopia do Iceberg



Miopia do Iceberg

- 
- Bug de software
 - Serviço crítico FTP habilitado
 - Desatualização do sistema operacional
 - Firewall sem configuração
 - ...
 - Alarme e tranca de porta frágil
 - Sistema de combate a incêndio inoperante
 - Cabeamento desestruturado
 - Ausência de controle de acesso físico
 - ...
 - Email enviado à pessoa errada
 - Relatório crítico descartado sem cuidado
 - Segredo de negócio falado no elevador
 - Arquivo eletrônico apagado distraidamente
 - ...

Informação vs Segurança

■ O QUE proteger nas informações?

Os conceitos principais:

- Confidencialidade
- Integridade
- Disponibilidade



atividade de
um indivíduo
comum

Os aspectos:

- Legalidade
- Autenticidade

Que podem ser atingidos pela exploração de uma falha ou vulnerabilidade presente em um ativo.

VULNERABILIDADES

Informação vs Segurança

■ DO QUE proteger as informações?

De ameaças:

- Físicas
- Tecnológicas
- Humanas



atividade de um indivíduo comum

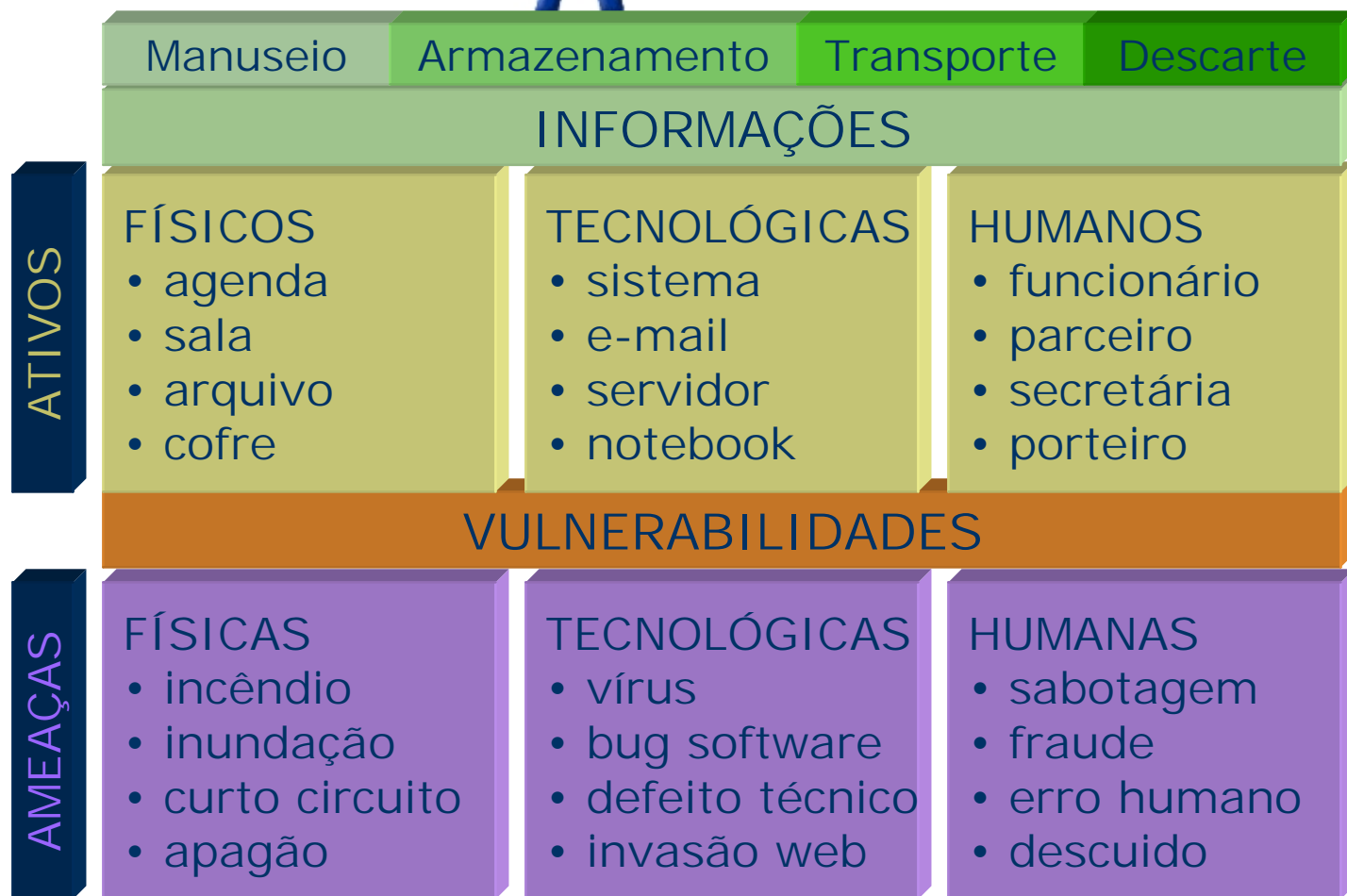
AMEAÇAS	FÍSICAS	TECNOLÓGICAS	HUMANAS
	<ul style="list-style-type: none">• incêndio• inundação• curto circuito• apagão	<ul style="list-style-type: none">• vírus• bug software• defeito técnico• invasão web	<ul style="list-style-type: none">• sabotagem• fraude• erro humano• descuido

Informação vs Segurança

■ Visão Geral



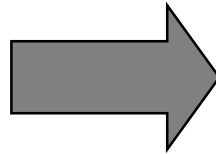
atividade de um indivíduo comum



Informação vs Segurança



atividade de
um indivíduo
comum



negócio de
uma empresa

- Heterogeneidade tecnológica
- Volume de informações disponibilizadas
- Volume de relacionamentos com terceiros
- Volume de ativos físicos, tecnológicos e humanos
- Altos índices de conectividade e compartilhamento
- Pressão por competitividade e lucratividade
- Manutenção da credibilidade da imagem
- ...

AMEAÇAS exploram

VULNERABILIDADES

presentes nos **ATIVOS** que

mantém informações, causando

IMPACTOS no Negócio

Cadernos

- :: 1º Caderno
- :: Empresas & Tecnologia
- :: Finanças
- :: Eu&
- :: Legislação & Tributos

Suplementos

- :: Guia Valor Veículos
- :: The Economist

Em tempos de recessão, a "inteligência competitiva" vale ouro (espionagem industrial é outra coisa).

Espionar, sim, mas no bom sentido

Foto: Pepe Casals



Há dois anos, quando os executivos da Texas Instruments começaram a suspeitar que uma empresa rival planejava adquirir a Telogy Networks, dispararam vários alarmes na empresa. Na época, a Telogy fornecia o *software* necessário para a telefonia de

**QUASE UM
SÉCULO
INVESTINDO
EM ENERGIA**

ESPIONAGEM

titulos e ações, até pesquisar em bancos de dados e fazer contatos pessoais com representantes de empresas rivais nos encontros e feiras do setor. E diferente da "espionagem" corporativa, ou seja, o roubo de segredos comerciais através de meios ilegais, como grampear telefones, oferecer subornos ou invadir computadores pela internet.

Mesmo assim, há aqueles que extrapolam os limites da ética. No ano passado, a Procter & Gamble contratou profissionais para espionar a rival Unilever, mas lhes deu um basta quando descobriu que um deles havia examinado as latas de lixo da rival. A Oracle admitiu que os detetives que contratou pagaram para o pessoal da limpeza pesquisar o lixo da Microsoft, em busca de provas para utilizar nos tribunais.

Colunistas

- :: Angela Bittencourt
- :: Eliana Cardoso
- :: Michael Reid
- :: Rosângela Bittar

Canais

- :: Valor 1000
- :: Valor Carreira


tin
"tr
ad
un
de
ho
pe
ve
de

From: Alguem que nao te esquece

Date: domingo, 11 de agosto de 2002 01:03

To: none

Subject: Velhos Tempos III

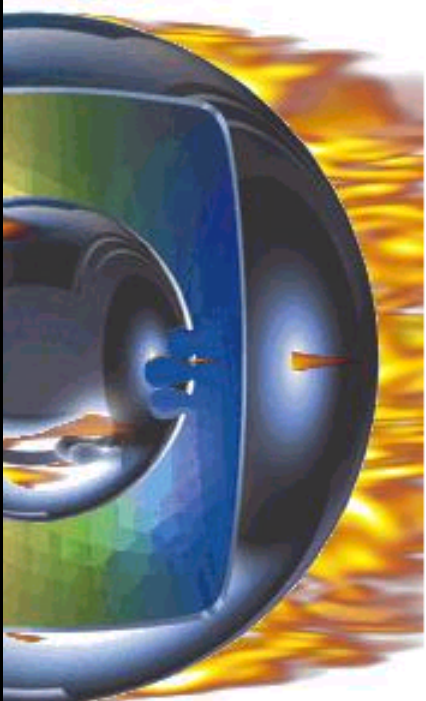
Attach:  QUEM.EXE (205 KB)

Lembra-te com quem voce estava ha exatamente 01 ano atraz ? mas eh assim mesmo, eu tambem nao consigo me lembrar de muita coisa, mas voce foi um marco em minha vida...pessoas como voce jamais sera esquecida, ja sabe quem sou eu ? conseguiu lembrar ? estive acompanhando alguns momentos de sua vida, os momentos tristes e alegres... sabe quem sou eu agora ?

Veja a Foto Compactada em Anexo:

Salve em seu disco O arquivo QUEM.EXE e saberas quem sou...

COMTAMINACÃO



INVASÃO

REDE GLOBO

Email falso:

Subject: Proposta conta corrente
BRADESCO BANKLINE NET BRASIL S/A

.....
SEJA VOÊ TAMBEM UM CLIENTE ON LINE BRADESCO . ABRA JA SUA CONTA SEM NENHUMA
COMPROVAÇÃO DE RENDA E SEM RESTRIÇÃO E GANHE UM LIMITE INICIAL DE R\$500,00
E MAIS UM CARTÃO BRADESCO FACIL. BASTA PREENCHER A PROPOSTA ABAIXO E ENVIAR
POR E-MAIL PARA: bradescobankmail@ig.com.br *OBS: (PARA SUA PROPOSTA SER
APROVADA É NECESSARIO QUE VOCE POSSUA CONTA EM OUTRO BANCO OU TENHA CARTÃO
DE CREDITO.(PARA FINS DE COMPROVAÇÃO DE CREDITO)

FRAUDE

CADASTRE SUA SENHA DE DESBLOQUEIO DO CARTÃO QUE VIRÁ PELO CORREIO.
VOCE PODE UTILIZAR A SENHA DO BANCO ATUAL. (NÃO OBRIGATORIO)

1ºSENHA:
2ºSENHA:

.....
OS DADOS SERÃO ANALIZADOS E DENTRO DE CINCO DIAS UTEIS VOCE RECEBERÁ UMA
CONFIRMAÇÃO VIA E-MAIL. OBS:(PREENCHA ATENTAMENTE OS CAMPOS DA PROPOSTA
TODAS AS INFORMAÇÕES CONTIDAS NESSE FORMULARIO SERÃO SIGILOSAS E A UNICA
PESSOA QUE TERÁ ACESSO A ELAS SERÁ VOCE.
OBRIGADO POR SE TORNAR UM CLIENTE BRADESCO.

.....
bradescobankmail@ig.com.br

CEP:
CIDADE:
ESTADO:
TELEFONE:
CPF:
RG:
NOME DO PAI:
NOME DA MÃE:
BANCO QUE POSSUE CO
AG:
CONTA:
CARTÃO DE CREDITO:
ADMINISTRADORA:
NUMERO DO CARTÃO:
/VALIDADE:

Alerta geral contra a espionagem

Políticos mudam hábitos em Brasília por causa da guerra de dossiês e de escutas telefônicas

Os casos comprovados de grampo telefônico e de vazamento de informações sigilosas provocaram uma curiosa situação em Brasília. Tanto na Esplanada dos Ministérios quanto no Congresso funcionários, autoridades e parlamentares mudaram seus hábitos por causa da preocupação em manter o segredo de suas conversas. Procuram falar por telefone apenas o essencial, pedem periodicamente varredura nas linhas e constantemente trocam os números de seus celulares para escapar da espionagem.

O ministro da Integração Nacional, Ney Suassuna, diz que foi dado um

"alô de alerta" aos Brasília por causa da atuação da divisão de segurança do

GRAMPO

Suassuna costuma pedir a varredura das linhas telefônicas do

ministério. Em sua residência, Suassuna também adota cautela. Ele

evita falar ao telefone sobre estratégias políticas. Isto porque o ministro

From: Modulo.com

Date: quinta-feira, 8 de novembro de 2001 19:57

To: colaboradores@modulo.com.br

Subject: Modulo e-Security News - No. 217

9 - CRACKER INVADE SISTEMA DE CONTROLE DE ESGOTO

IAfrica - 05 Nov 2001

O cracker Vitek Boden, 49 anos, pegou dois anos de cadeia por assumir o controle dos sistemas de uma estacao de tratamento de esgoto na Australia e despejar milhoes de litros de residuos nos rios da regioa de Maroochy Shire, na provincia de Queensland, nordeste do pais.

Boden atacou os computadores 45 vezes ate conseguir assumir o controle da estacao, que eh totalmente informatizada. No julgamento, a promotoria provou que o cracker - que era funcionario da empresa que instalou o software que controlava o tratamento de esgoto na estacao - poluiu a area deliberadamente. O invasor teria se candidatado a uma

DANO

Oficiais da NASA estão investigando o roubo de diversas informações confidenciais sobre desenvolvimento de novos projetos de construções de veículos espaciais. A notícia foi divulgada pelo site *Computerworld.com*, que teria recebido os arquivos de um cracker.

Teriam sido roubados do sistema da agência espacial, via FTP, cerca de 40 MB de arquivos confidenciais, incluindo 15 páginas de apresentações em PowerPoint sobre uma nova linha de design, detalhes do projeto Cobra e do Boeing T44 Advanced Checkout, Control & Maintenance System.

VAZZAMENTO

Ex-funcionário processado por danificar sistemas de sua antiga empresa

DATA - 20 Dez 2002

FONTE - CNET News.com

O americano Roger Duronio, de 60 anos e ex-administrador de sistemas da UBS PaineWebber, foi processado nesta semana por sabotar os sistemas de sua antiga empresa. Segundo as investigações, a ação de Duronio causou um prejuízo em torno de três milhões de dólares.

Antes de sair da empresa, o ex-funcionário teria instalado programas maliciosos, conhecidos como bombas lógicas, no sistema de rede que foram ativados em dia e horário programados. Assim, cerca de mil computadores e arquivos foram danificados pela ação do cracker.

Duronio está sendo processado por fraude e será enquadrado na lei "Computer Fraud and Abuse Act". Uma vez condenado, poderá ter que cumprir 20 anos de prisão e a pagar multas acima de 1,25 milhão de dólares.

"O crime virtual contra as empresas do sistema financeiro é um preocupante aviso. Embora o dano neste caso tenha sido contido, o potencial para danos catastróficos em outros casos serão constantes", diz o procurador-geral de Nova Jersey, Christopher J. Christie.

A ação do cracker foi motivada por vingança, pois antes de sair da UBS, Duronio exigia aumento de seu salário e das bonificações. No Brasil, 64% dos profissionais entrevistados para 8ª Pesquisa Nacional de Segurança da Informação, realizada entre os meses de março e setembro deste ano pela Módulo, apontavam os funcionários insatisfeitos como uma das principais ameaças à segurança da informação de suas empresas. ■

SABOTAGEM



INDISPONIBILIDADE



Questão chave: Risco

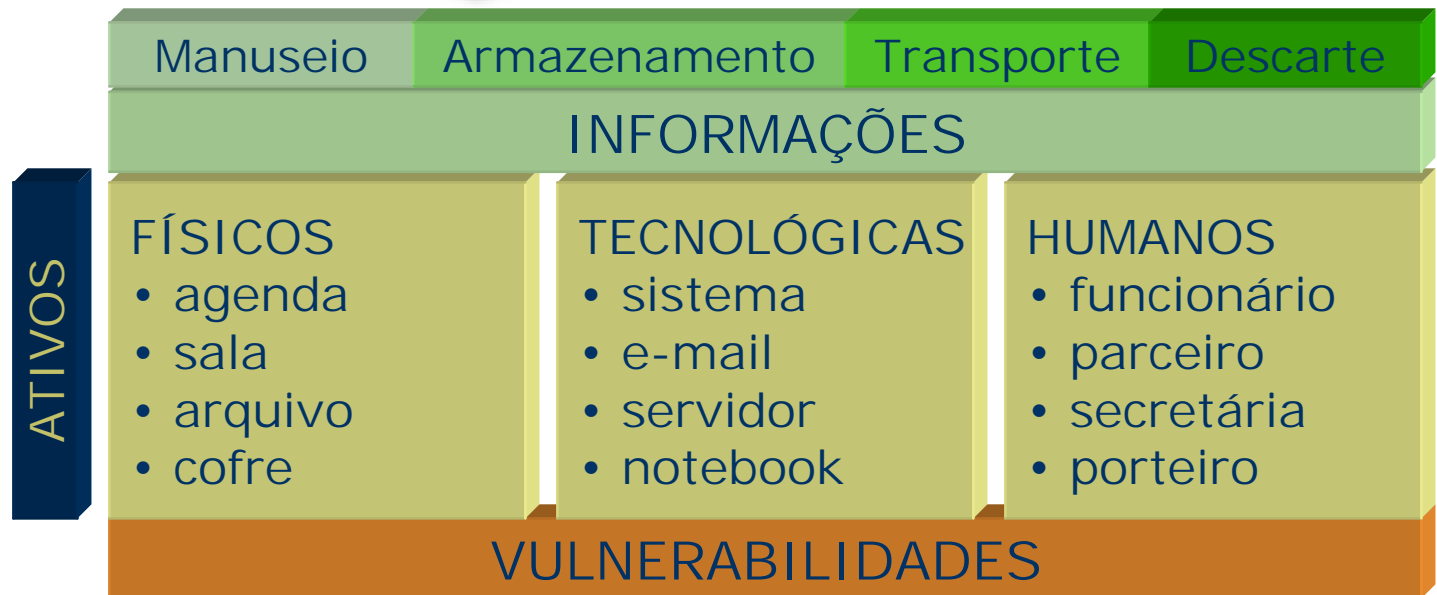
$$R_{\text{risco}} = \frac{\text{Ameaças} \times \text{Vulnerab.} \times \text{Impactos}}{\text{Medidas de Segurança}}$$

Segurança da Informação é adotar controles físicos, tecnológicos e humanos personalizados, que viabilizem a redução e administração dos riscos, levando a empresa a atingir o nível de segurança adequado ao seu negócio.

Informação vs Segurança



negócio de
uma empresa



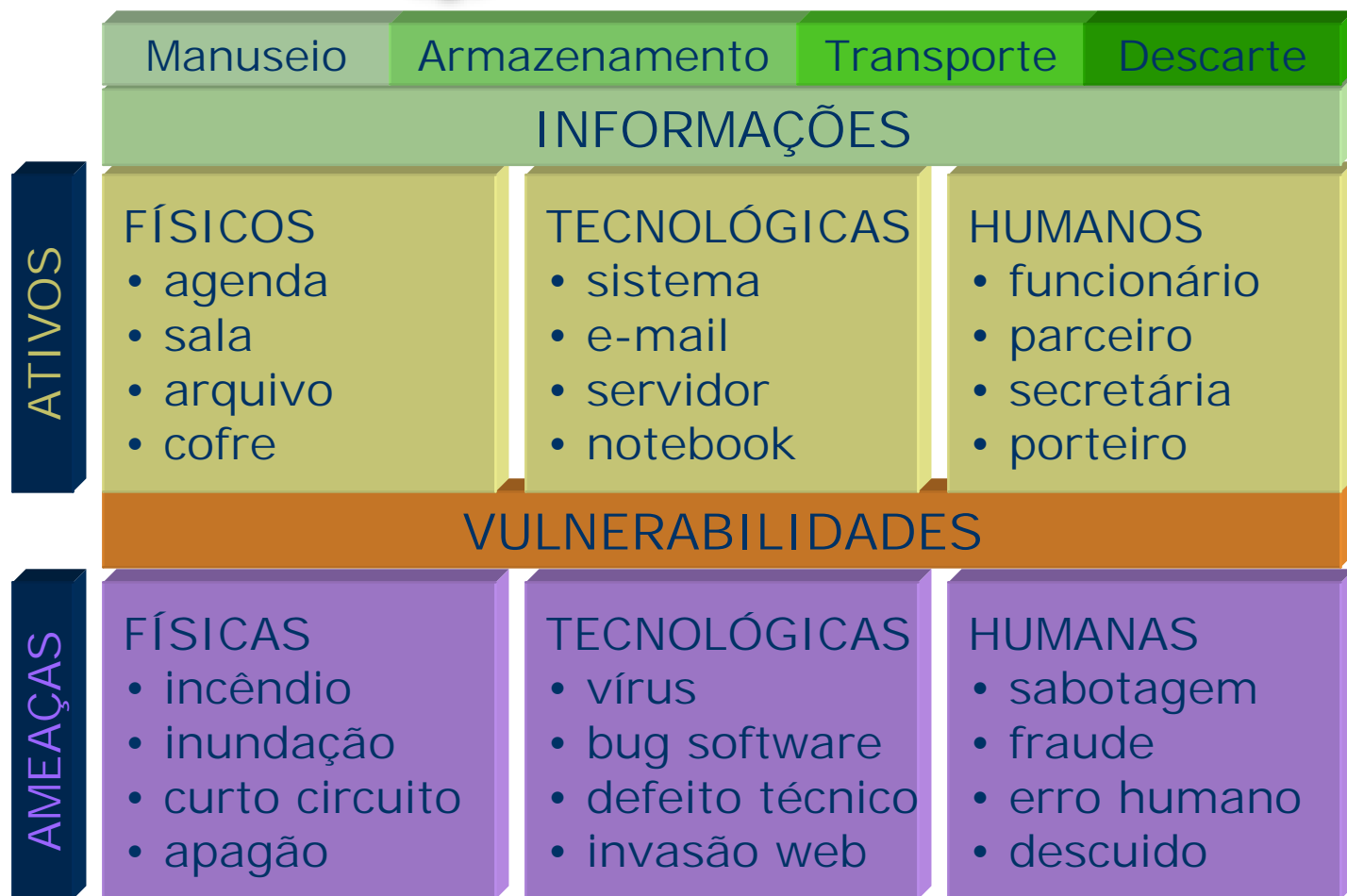
Existe RISCO nesta situação?

Informação vs Segurança

■ Visão Geral



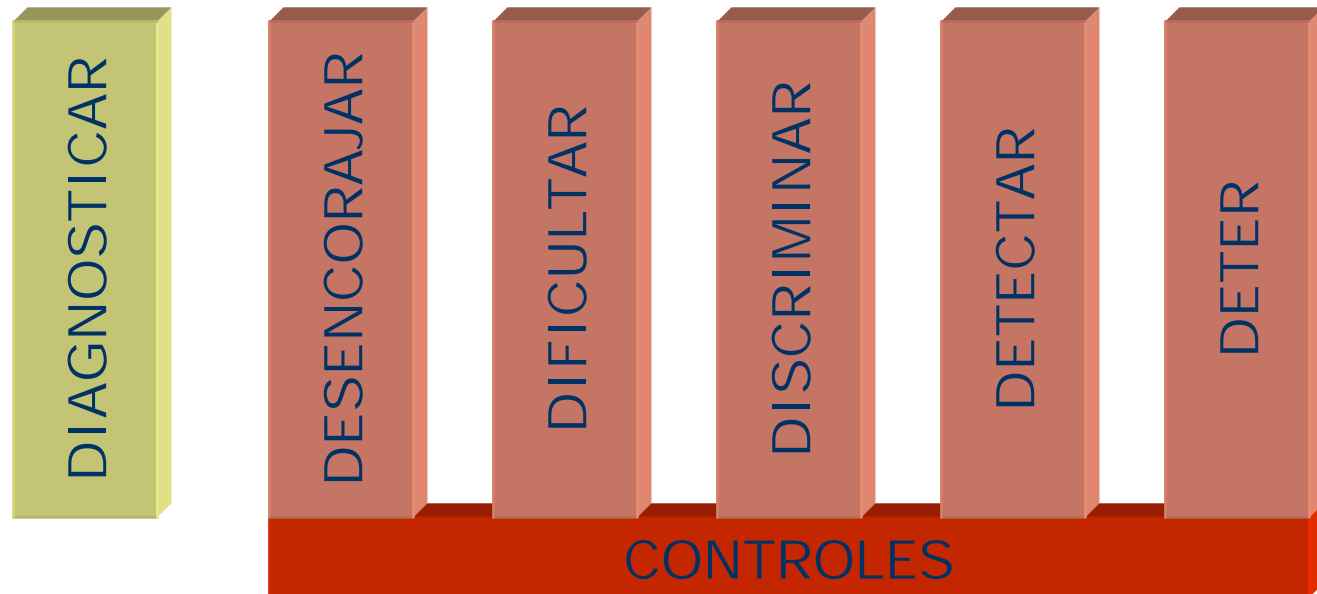
negócio de
uma empresa



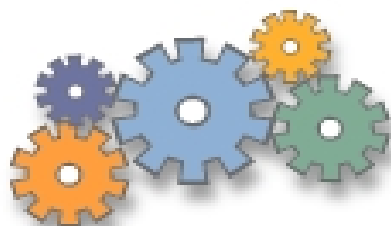
Informação vs Segurança

■ COMO proteger as informações?

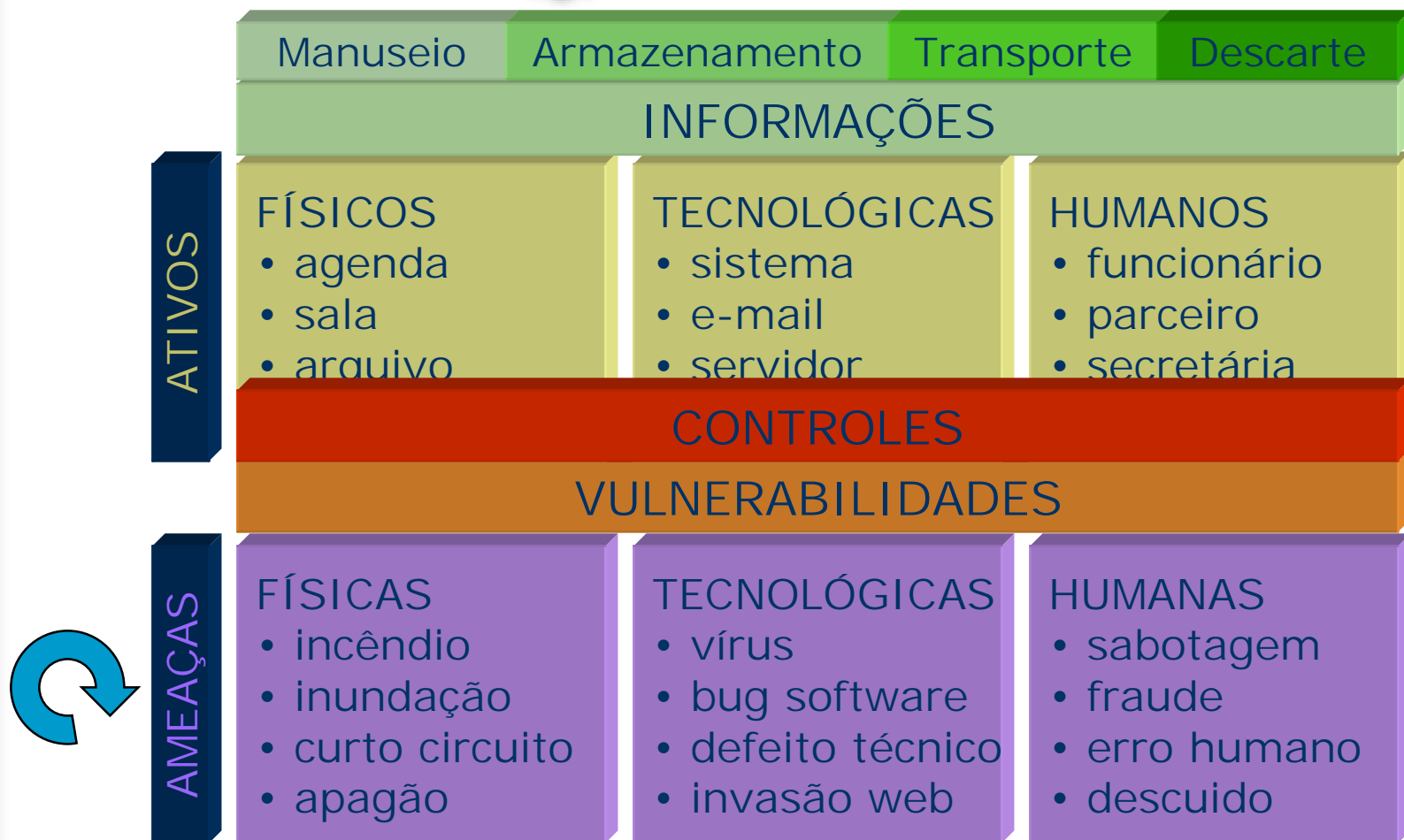
- Aplicando controles que eliminem e administrem as vulnerabilidades, reduzindo assim os riscos
- Segmentando-as pela importância (relevância)
- Definindo níveis de segurança compatíveis
- Avaliando o valor da informação e o custo da proteção



Informação vs Segurança



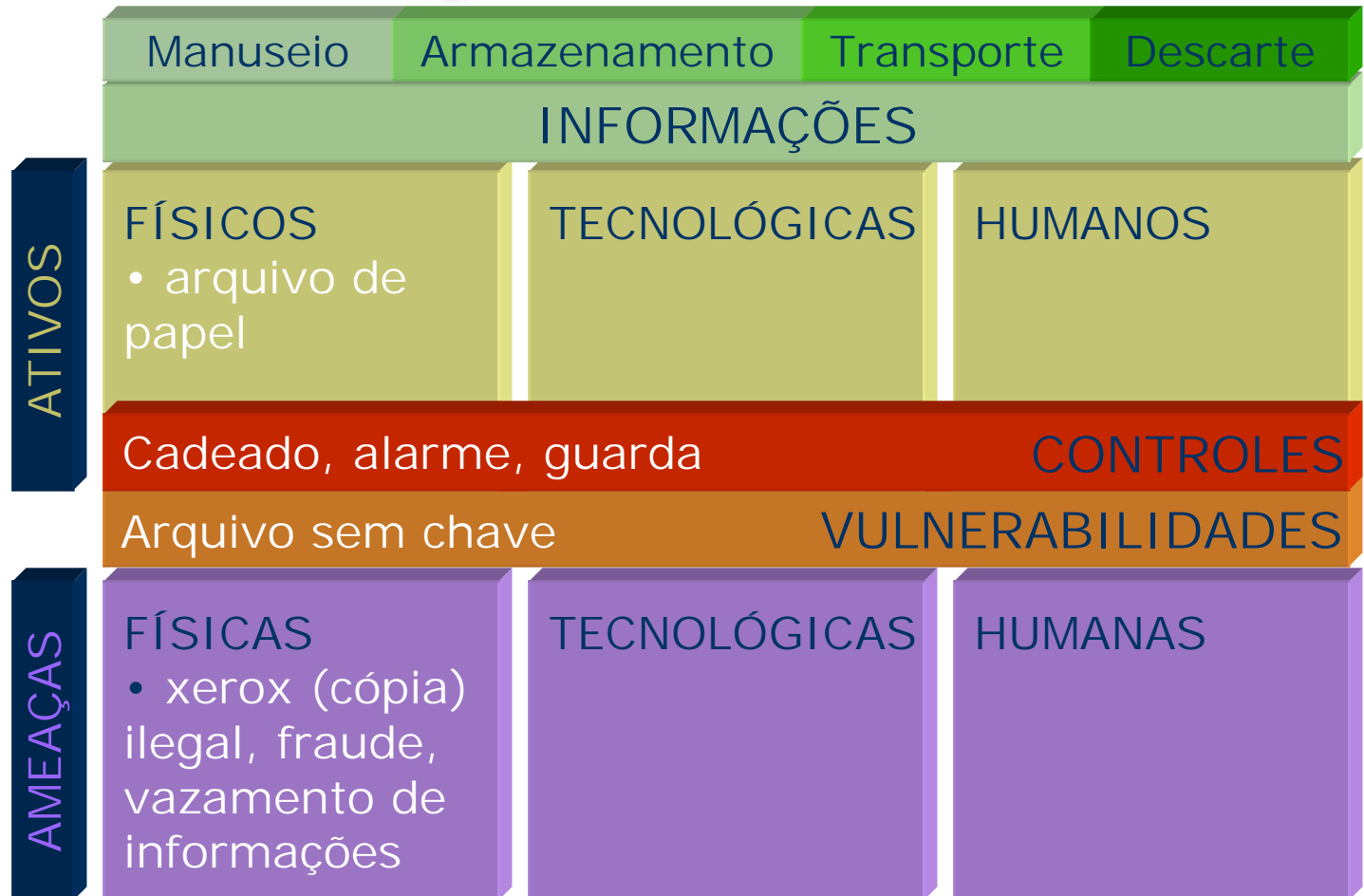
negócio de
uma empresa



Velocidade das Mudanças



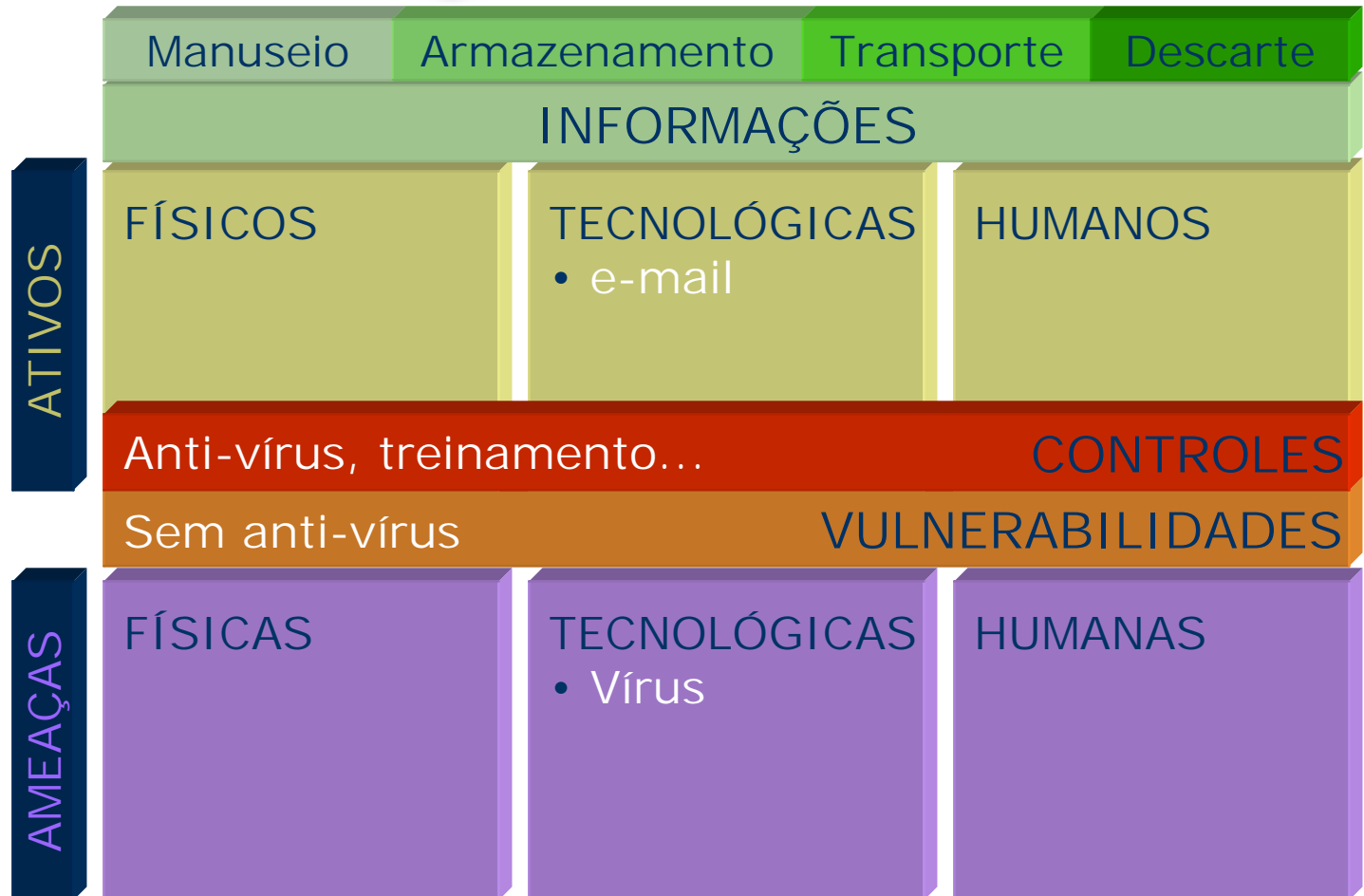
negócio de
uma empresa



Velocidade das Mudanças



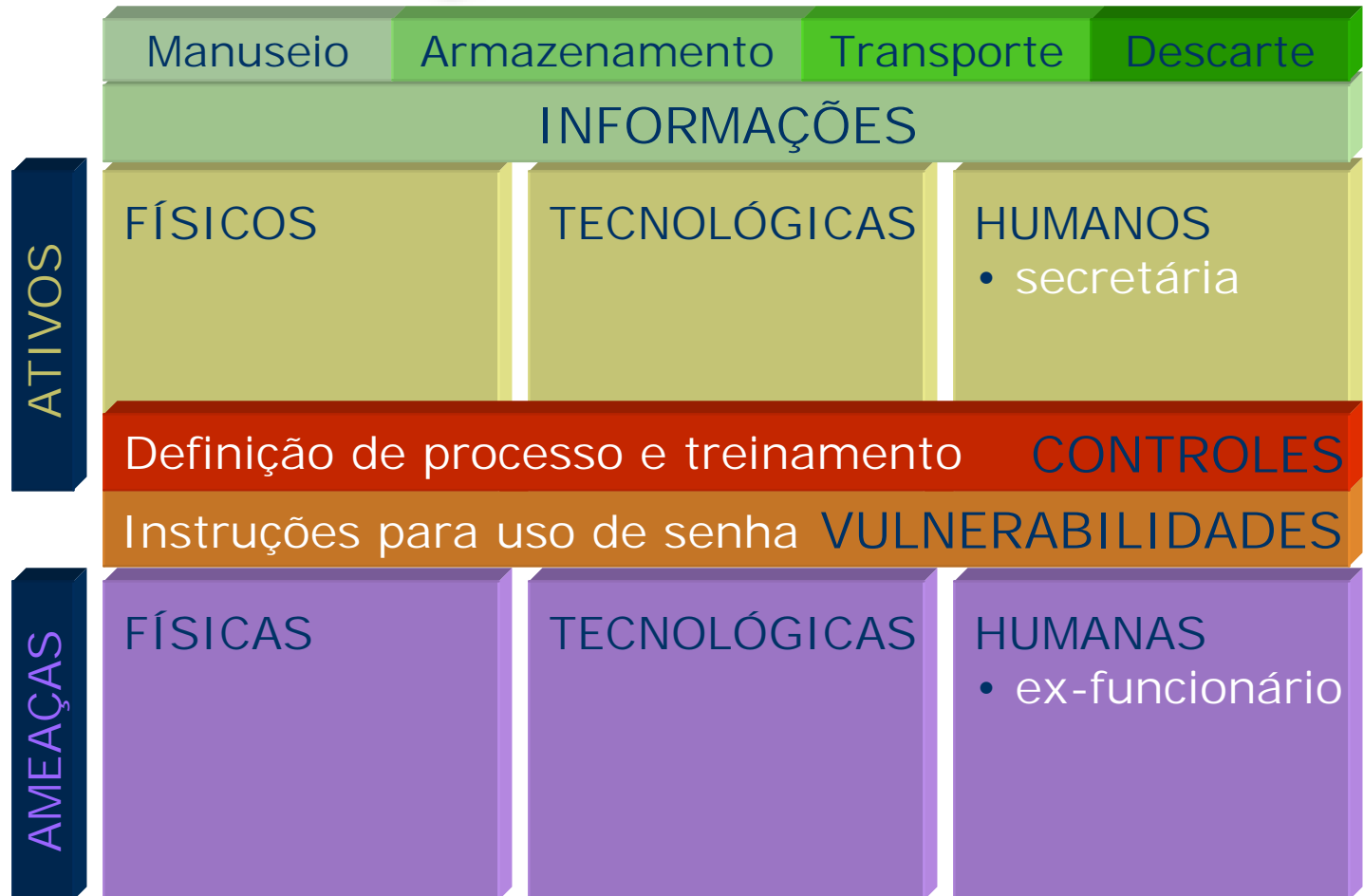
negócio de
uma empresa



Velocidade das Mudanças



negócio de
uma empresa



1.300 updates - 9 meses!

Correções de vulnerabilidades sobrecarregam gerentes de TI

[Computerworld/EUA](#)

O número de patches de segurança e atualizações para programas de proteção disponibilizados nos últimos 12 meses têm sobrecarregado os gerentes de TI (Tecnologia da Informação) de tal forma que a questão está se tornando um risco para grande parte das empresas. É o que mostra um estudo desenvolvido pela empresa britânica Activis.

Segundo o levantamento, uma empresa com oito firewalls e nove servidores, por exemplo, teria que realizar 1,3 mil updates nos últimos nove meses — mais de quatro atualizações por dia. O número se refere ao total de programas para atualização disponibilizados no período, por alguns dos maiores fabricantes de software.

Além disso, administradores de redes em companhias com esse tamanho teriam que gerenciar mais de 500 mil registros nos arquivos de log por dia. Cada firewall gera 200 mil a 300 mil entradas de log e 20 alertas por dia, de acordo com a pesquisa.

Segundo John Cheney, diretor da Activis, o estudo avaliou as configurações mais utilizadas, incluindo servidores da Microsoft, como SQL Server e Exchange, firewalls da Checkpoint Software e programas antivírus. O especialista recomenda que as empresas estabeleçam prioridades para a atualização de sistemas, colocando em primeiro lugar os servidores Web, que estão mais expostos.

Hoje xx:xxh



From: gnome3@superereva.it
Date: segunda-feira, 1 de outubro de 2001 13:12
To: gnome3@bol.com.br
Subject: Curso de Hackerismo por R\$ 42,00

Este curso demonstra quais são as principais vulnerabilidades do Windows e do Linux que permitem que hackers ataquem máquinas conectadas à Internet ou à uma rede local.

CURSO DE HACKERISMO EM 21 AULAS

- Aula 01-Instalando o Nessus (uma excelente ferramenta Hacker)
- Aula 02-Vulnerabilidades de máquinas com Windows 95
- Aula 03-Vulnerabilidades de máquinas com Windows 95SR2
- Aula 04-Vulnerabilidades de máquinas com Windows 98
- Aula 05-Vulnerabilidades de máquinas com Windows 98SE
- Aula 06-Vulnerabilidades de máquinas com Windows ME
- Aula 07-Vulnerabilidades de máquinas com Windows NT4
- Aula 08-Vulnerabilidades de máquinas com Windows 2000
- Aula 09-Vulnerabilidades de Servidores Linux com Connectiva 5.0
- Aula 10-Vulnerabilidades de Servidores Linux com Connectiva 6.0
- Aula 11-Vulnerabilidades de Servidores Linux com Connectiva 7.0
- Aula 12-Vulnerabilidades de Servidores Linux com RedHat 5.2
- Aula 13-Vulnerabilidades de Servidores Linux com RedHat 6.0
- Aula 14-Vulnerabilidades de Servidores Linux com RedHat 7.0
- Aula 15-Vulnerabilidades de Servidores Linux com Mandrake 6.0
- Aula 16-Vulnerabilidades de Servidores Linux com Mandrake 7.0
- Aula 17-Vulnerabilidades de Servidores Linux com Mandrake 8.0
- Aula 18-Como os hackers ganham acesso root local por ataques ao LILO
- Aula 19-Defendendo-se contra ataques ao LILO

Já falamos de Informação e Segurança.
Por que falar de Gestão?

Gestão (Administração)

1 Ato de administrar. 2 Governar, reger. 3 Exercer (cargo, emprego, ofício).

Gerir

1 Ter gerência sobre; administrar, dirigir, gerenciar.

Fonte: Dicionário Michaelis

Gestão de Riscos

■ POR QUE um processo de gestão de riscos?

- Velocidade das mudanças

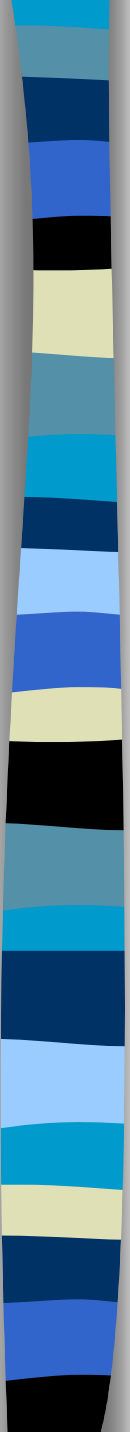
- Físicas
- Tecnológicas
- Humanas

Provocam o surgimento de novas vulnerabilidades

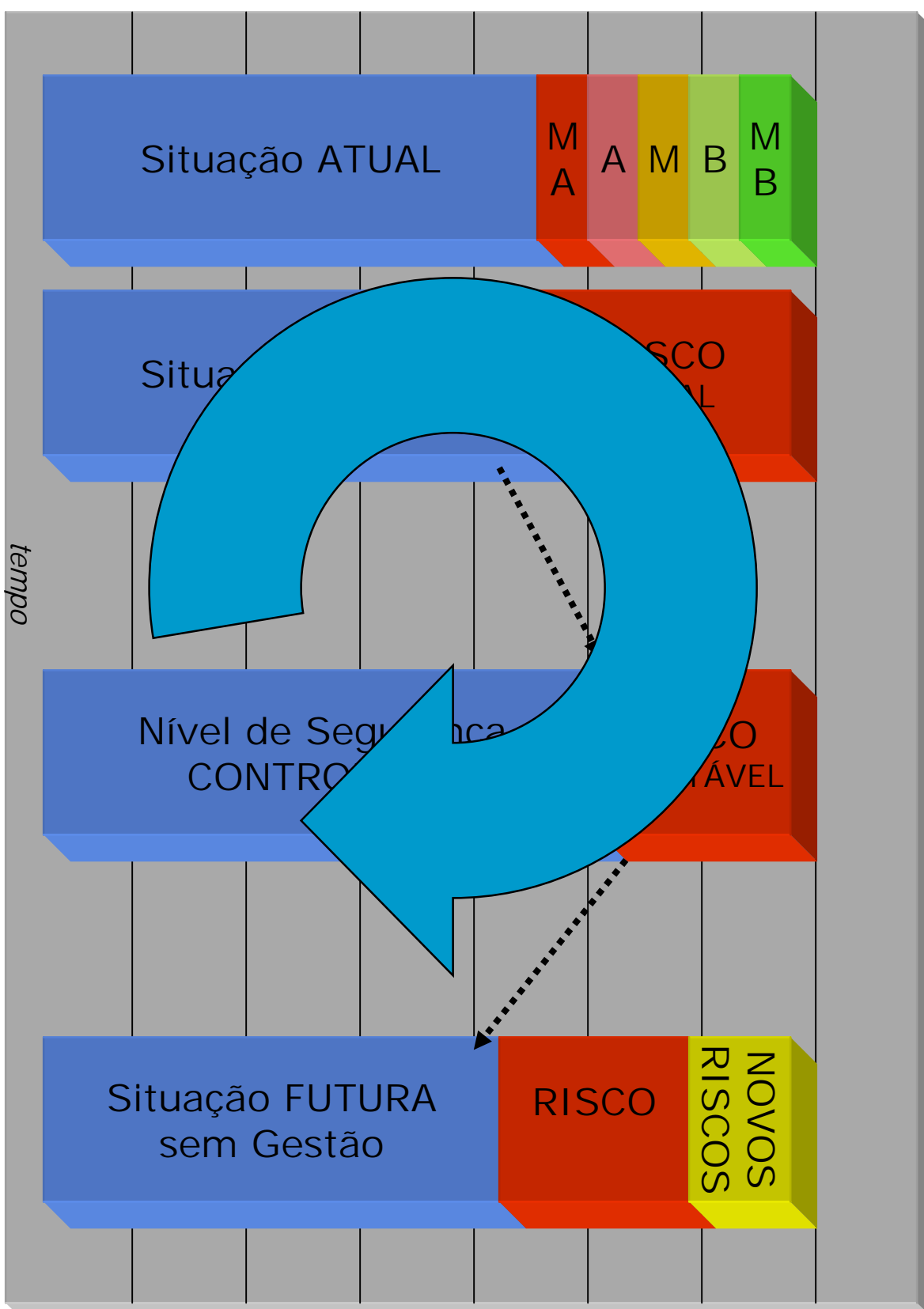
- Velocidade de criação de novas ameaças que estarão aptas a explorar as também novas vulnerabilidades.

Não existe segurança
100%

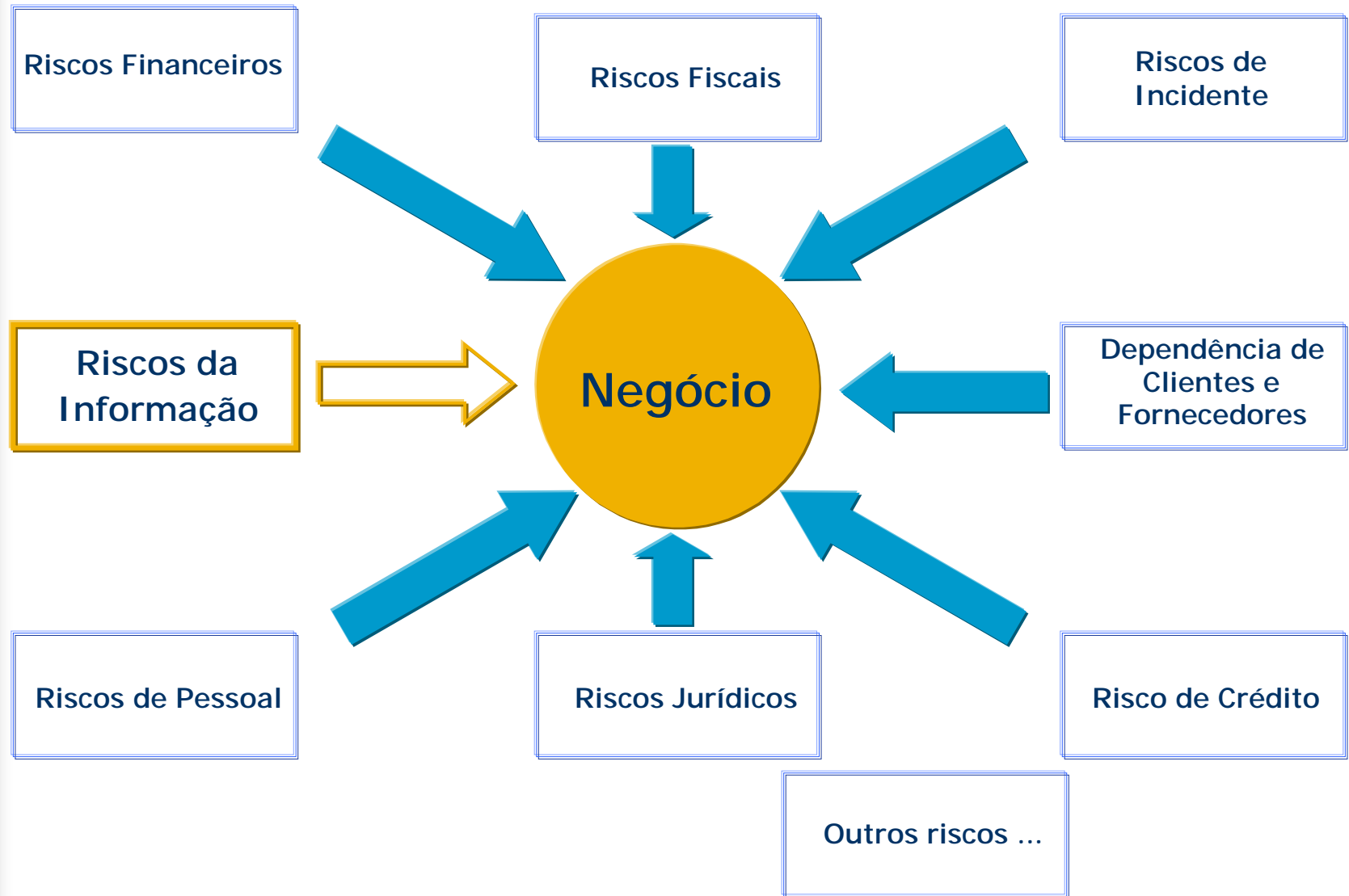
Segurança é risco
tendendo a zero.



Processo de Gestão



Riscos do Negócio





**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

Copyright © 2001,
ABNT–Associação Brasileira
de Normas Técnicas
Printed in Brazil/
Impresso no Brasil
Todos os direitos reservados

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

Norma ISO/BS7799

BS17799 (ISO17799)

- Parte 1: Código de Prática
10 domínios reunindo 127 controles
- Parte 2: Framework ISMS
ou SGSI – Sistema de Gestão de
Segurança da Informação

Posicionamento das empresas:

- Busca da certificação (definição de escopo)
- Orientação para a gestão de segurança
- Primeiro passo: diagnosticar

Análise de Riscos

ISO17799:1 - Objetivo

- Fornecer recomendações para a gestão da segurança da informação orientando os responsáveis pela introdução, implementação e manutenção da segurança em suas organizações
- Prover uma base comum para o desenvolvimento de normas de segurança e das práticas efetivas de gestão
- Prover confiança nos relacionamentos entre as organizações

ISO17799:1 - Estruturação

ISO17799:1

Código de Prática (parte 1 da BS7799)
Gestão de Segurança da Informação

Domínios

Dez domínios gerais, desmembrados em 36 grupos de controles de segurança



10

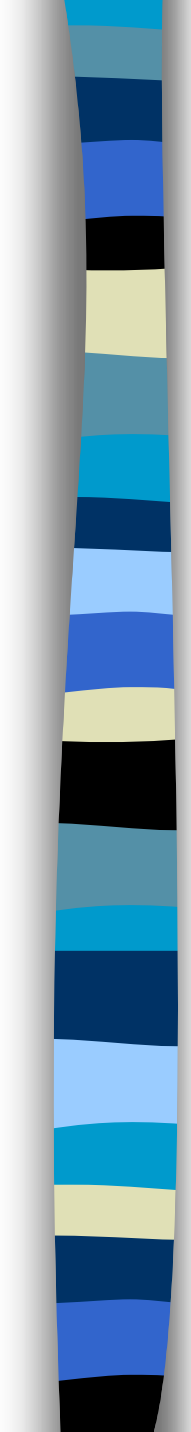
Controles e Objetivos de Controle

127 controles no total
Objetivos que se aplicam a cada domínio



127

Código de Prática

- 
- A norma estruturou os controles e os agrupou em 10 domínios:
 - 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

BS7799:2 - Passos sugeridos

Define a Organização da Segurança da Informação

1º Passo

Define Política de Segurança da Informação

2º Passo

Define o Escopo do ISMS

3º Passo

Ameaças, Vulnerabilidades, Impactos

Realiza a Avaliação de Risco

4º Passo

Abordagem do Gerenciamento de Risco - Grau de confiança requerido

Gerencia o Risco

5º Passo

Clausula 4 da BS7799-2:1999, Objetivos de controle e controles, Controles adicionais não contidos na BS7799.

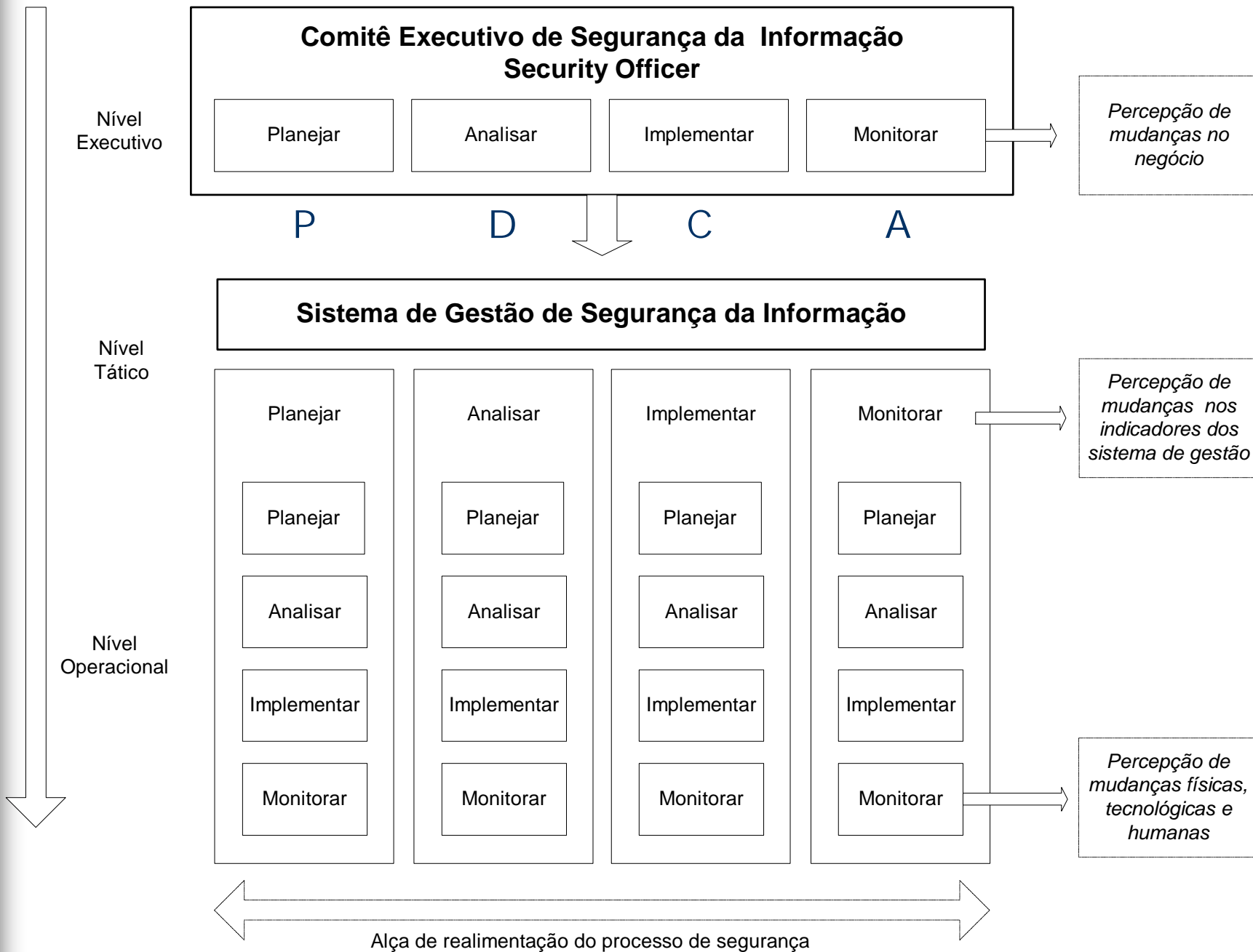
Seleciona os objetivos de controle e os controles a serem implementados

6º Passo

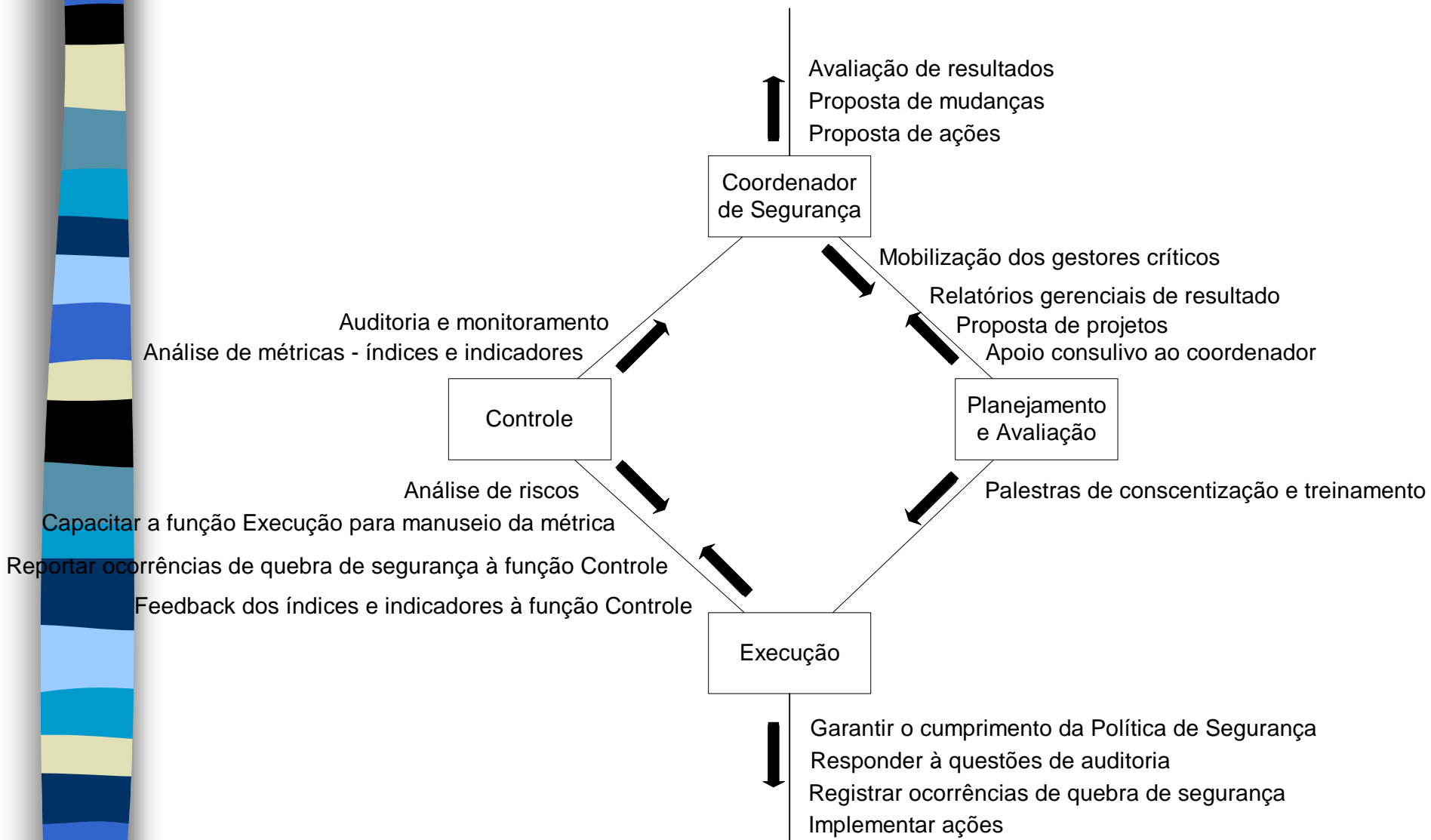
Prepara a Declaração de Aplicabilidade

Documentos e Registros do ISMS

Gestão PDCA



Gestão PDCA



Empresas certificadas BS7799

200 accredited BS 7799 certificates

Region	Number of Certificates	Region	Number of Certificates
Australia	1	Italy	10
Austria	2	Japan	20
Brazil	2	Korea	9
China	4	Malaysia	1
Egypt	1	Norway	6
Finland	8	Singapore	7
Germany	8	Spain	1
Greece	2	Sweden	4
Hong Kong	6	Taiwan	3
Hungary	3	UAE	1
Iceland	1	UK	86
India	10	USA	3
Ireland	3		

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 europeias, 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 europeias 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.

Números da segurança

8^a PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO

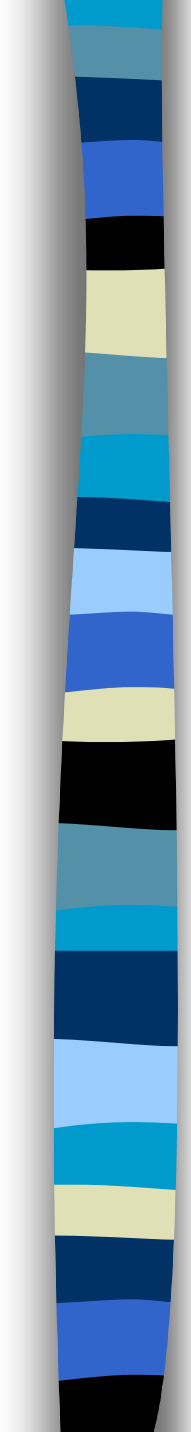


SETEMBRO 2002

Copyright © Módulo Security Solutions S.A.

Todos os direitos reservados. Autorizamos a utilização do conteúdo desta pesquisa, somente para fins de apresentação, desde que citada a sua fonte.

Migração para a Internet

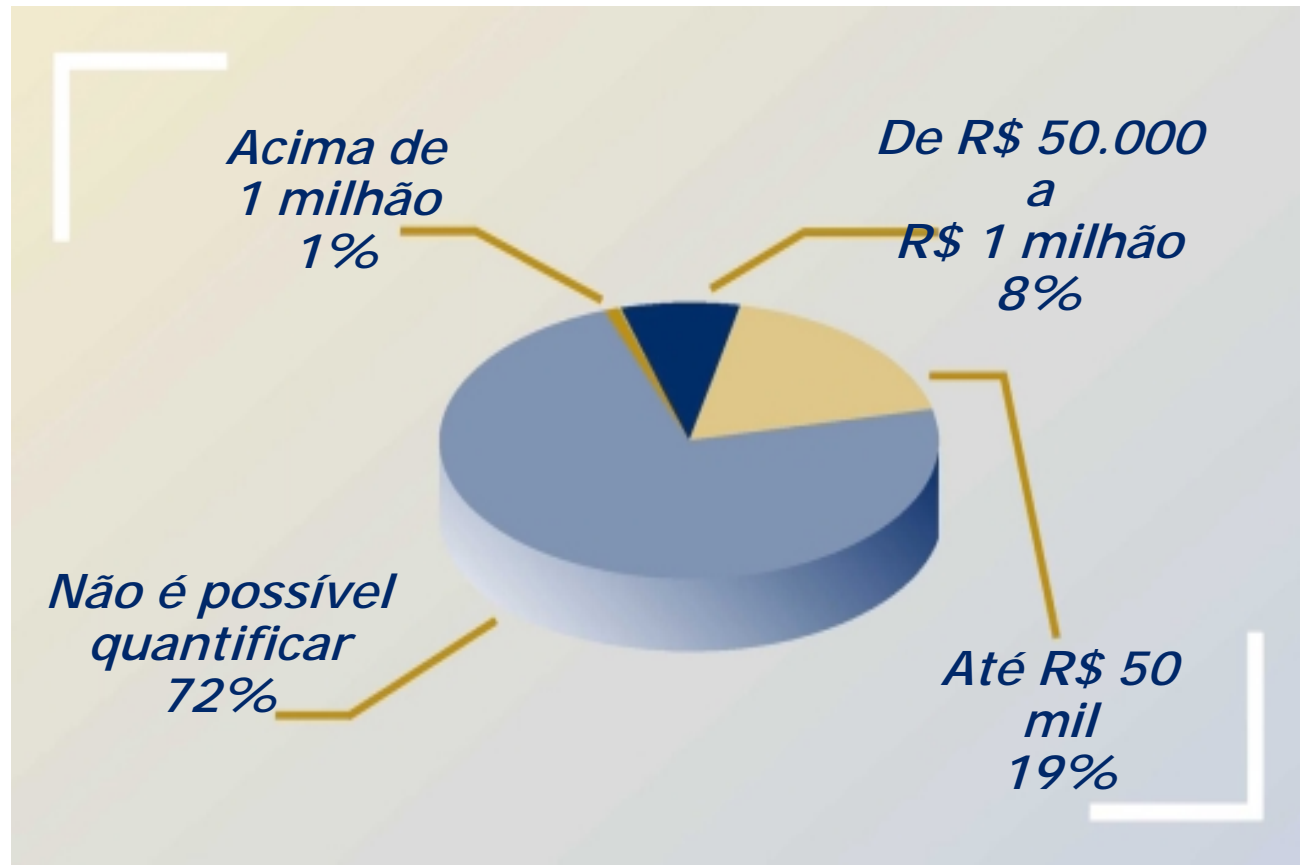


Web Site	70%
Consulta a Banco de Dados	34%
Entrada / recepção de dados	33%
Webmail	32%
Atendimento online	30%
Vendas online	16%
Internet Banking	12%
Certificação digital	10%
E-procurement	8%
Diagnóstico remoto	5%

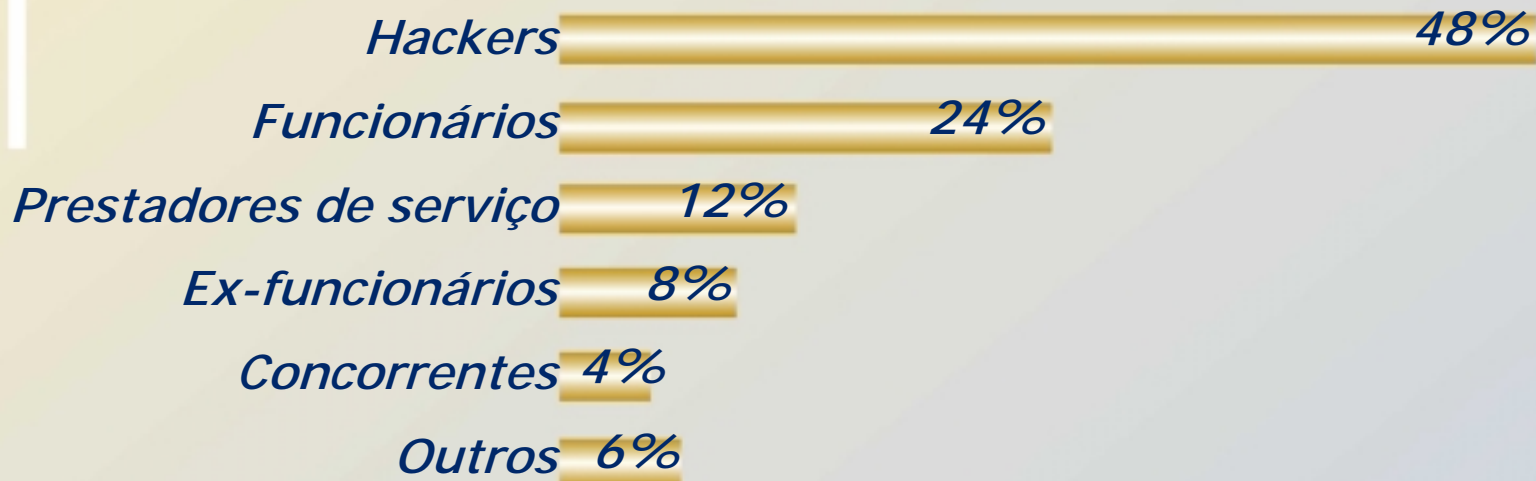
Principais ameaças



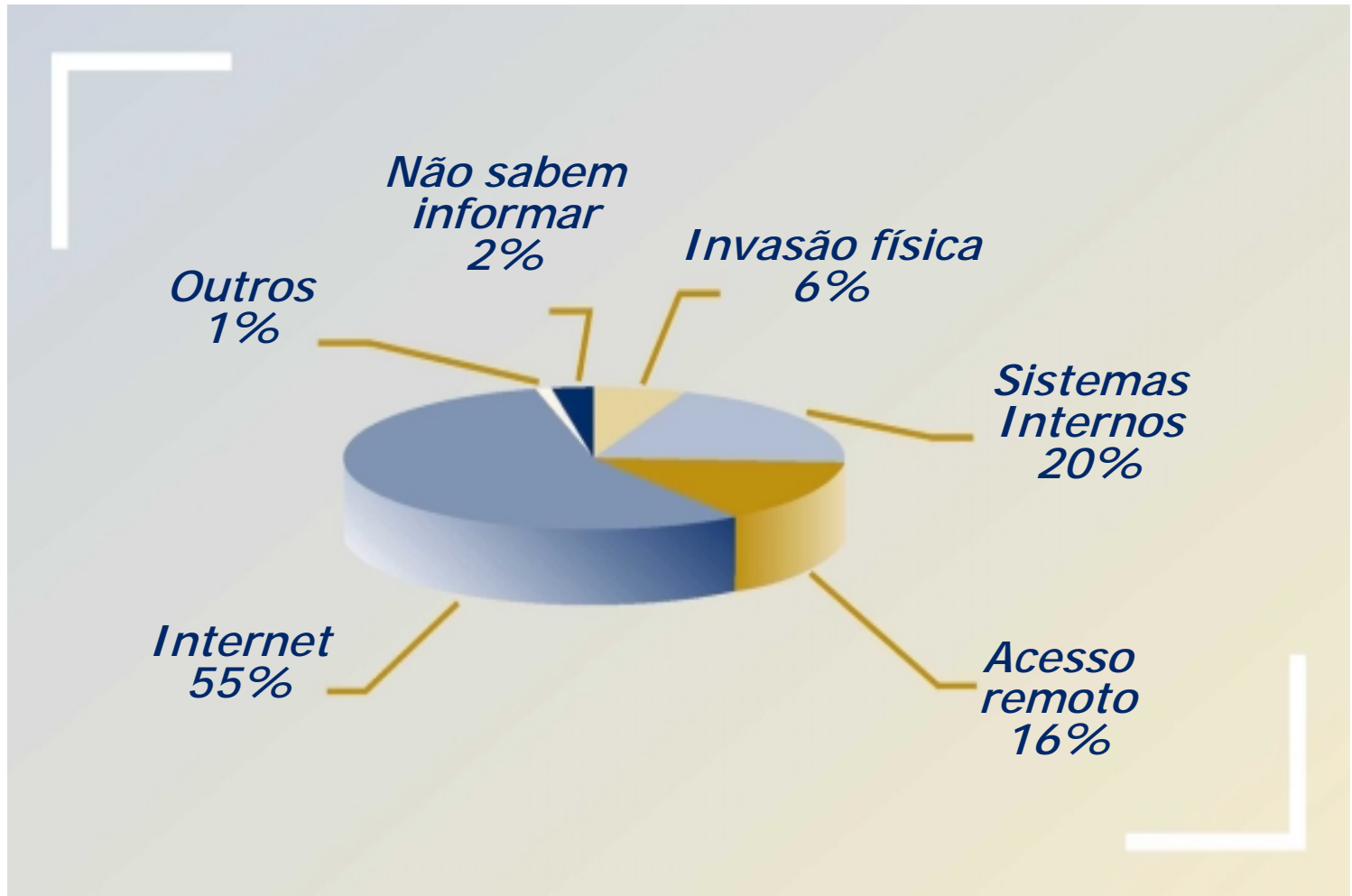
Prejuízos contabilizados



Principais responsáveis



Pontos de invasão



Obstáculos



GAP da Segurança Corporativa



SÊMOLA, Marcos.
Gestão da
Segurança da
Informação –
uma visão
executiva.
Ed.Campus, 2003

R\$35,00




Proposta do livro

- Conscientizar os diversos níveis hierárquicos
- Fundir as visões técnica e de negócio
- Compartilhar uma visão integrada dos riscos
- Subsidiar um Plano Diretor de Segurança
- Orientar para um processo de gestão de riscos
- Otimizar os investimentos em segurança
- Criar sinergia com a norma ISO17799

Viabilizar a segurança como um elemento gerador de valor para as empresas, em prol da sua competitividade e sobrevivência.



Visão integrada dos riscos da informação para a gestão contínua da segurança



Não existe segurança 100%
Segurança é risco tendendo a zero.