Segurança da Informação e Proteção ao Conhecimento

Aula 01 - Introdução

Prof. Dalton Martins
dmartins@gmail.com

Gestão da Informação
Faculdade de Informação e Comunicação
Universidade Federal de Goiás

Apresentações

- Quem somos nós;
- O que estamos fazendo aqui mesmo;
- Para onde vamos com esse curso.

Ementa

Aspectos sociais e suas relações com os aspectos tecnológicos da Proteção ao Conhecimento e da Segurança da Informação.

Relações e interfaces entre proteção ao conhecimento e segurança da informação.

Identificação de ameaças.

Objetos e alvos de proteção.

Modelo de proteção ao conhecimento.

Implementação da segurança.

Fontes de políticas de segurança da informação.

Normas e legislação vigente.

Contextualizar as mudanças no cenário pelo viés da cultura e produção do conhecimento em formato digital

Objetivos

Contextualizar os aspectos sociais e suas relações com os aspectos tecnológicos da Proteção do Conhecimento e da Segurança da Informação. Avaliar os impactos das mudanças contemporâneas nos processos de produção do conhecimento e da cultura digital.

Conteúdo do curso

O contexto de segurança da informação;

O conceito vigente de segurança da informação;

Incidentes de segurança de informação;

A abrangência da segurança da informação;

A implementação da segurança da informação;

Aplicações de segurança da informação;

A gestão da segurança da informação;

O custo da segurança da informação;

Fontes de políticas de segurança da informação: legislação, organismos, padrões e métricas.

Proteção ao conhecimento no contexto das organizações;

Proteção ao conhecimento e suas relações com segurança da informação;

Proposta de modelo para proteção ao conhecimento.

Novos paradigmas e tendências na atualidade: os impactos da cultura e da produção do conhecimento em formato digital.

Processos e critérios de avaliação

MEDIA = 0,6 * (P1 + P2)/2 + 0,4 * PROJETO

P1 – prova 1 com questões teóricas e práticas;

P2 – prova 2 com questões teóricas e práticas;

Projeto – trabalho aprofundado da disciplina, tema de preferência dos alunos em torno dos tópicos do curso.

Mínimo de 70% de presença para aprovação!

Cronograma

10/03 Apresentação do curso, da turma, da ementa, avaliação. Introdução aos conceitos de base de segurança da informação;

12/03 O contexto de segurança da informação

17/03 O contexto de segurança da informação

19/03 O conceito vigente de segurança da informação

24/03 Incidentes de segurança de informação

26/03 Incidentes de segurança de informação: estudos de caso

31/03 A abrangência da segurança da informação

02/04 A implementação da segurança da informação

07/04 Aplicações de segurança da informação

09/04 Recesso – Espaço das Profissões

14/04 A gestão da segurança da informação e o custo da segurança da informação

16/04 Fontes de políticas de segurança da informação: legislação, organismos, padrões e métricas

21/04 Feriado

23/04 Fontes de políticas de segurança da informação: legislação, organismos, padrões e métricas

28/04 Fontes de políticas de segurança da informação: legislação, organismos, padrões e métricas

30/04 Fontes de políticas de segurança da informação: legislação, organismos, padrões e métricas

05/05 Prova P1

Cronograma

07/05 Proteção ao conhecimento no contexto das organizações

12/05 Proteção ao conhecimento no contexto das organizações

14/05 Proteção ao conhecimento e suas relações com segurança da informação

19/05 Proposta de modelo para proteção ao conhecimento

21/05 Novos paradigmas de produção do conhecimento: a cultura digital;

26/05 Novos paradigmas de produção do conhecimento: a cultura digital;

28/05 Novos paradigmas de produção do conhecimento: o trabalho imaterial;

02/06 Novos paradigmas de produção do conhecimento: as redes sociais e a produção de comum;

04/06 Novos paradigmas de produção do conhecimento: crowdsourcing;

09/06 Novas tendências: Creative Commons;

11/06 Novas tendências: Software Livre;

16/06 Novas tendências: Arquivos e repositórios abertos;

18/06 Impactos das novas tendências e novos paradigmas na segurança da informação e proteção ao conhecimento.

23/06 Recesso – Jogo da Copa

25/06 Prova P2

30/06 Projeto final

02/07 Prova Substitutiva

Bibliografia

http://creativecommons.org.br/

http://www.wired.com/wired/archive/14.06/crowds.html

http://www.gnu.org/philosophy/free-sw.pt-br.html

http://www.openarchives.org/

COELHO, Flávia Estélia Silva, BEZERRA, Edson Kowask, ARAÚJO, Luiz Geraldo Segadas. **Gestão da Segurança e da Informação: NBR 27001 e NBR 27002**. Escola Superior de Redes, 2013, 212p.

LAZZARATO, Mauricio, NEGRI, Antonio. **Trabalho Imaterial.** DP&A editora, 2001. 145p.

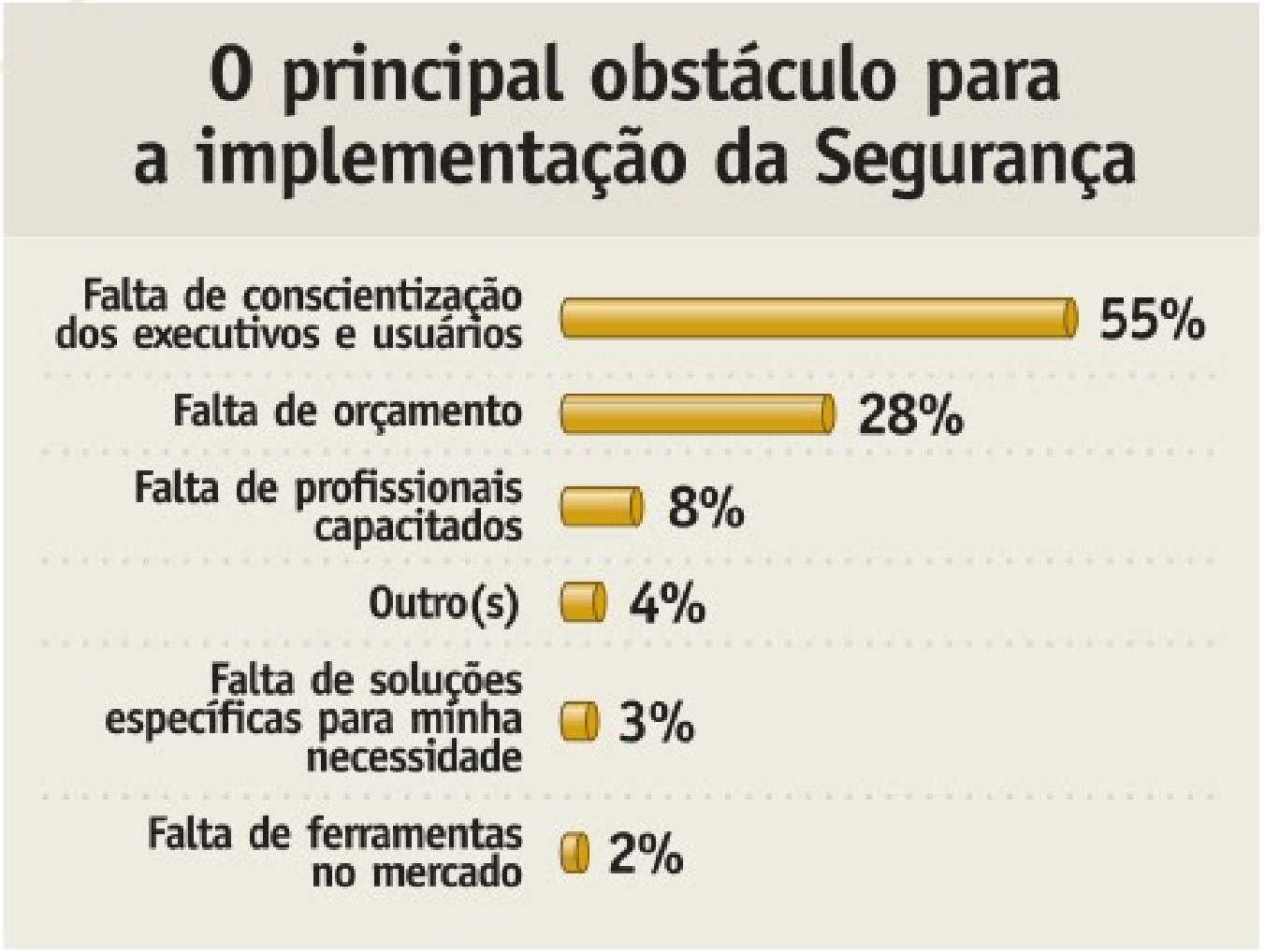
MARCIANO, João Luiz Pereira. **Segurança da Informação: uma abordem social.** Tese de Doutorado. Universidade de Brasília. 2006. 211p.

NASCIMENTO, Marta Sianes Oliveira do. **Proteção ao Conhecimento: uma proposta de fundamentação teórica.** Dissertação de Mestrado. Universidade de Brasília. 2008. 181p.

Contexto da área no Brasil

* Os dados a seguir foram retirados da 10ª Pesquisa Nacional Sobre Segurança da Informação, 2007 – Módulo Consultoria

Contexto da área no Brasil



Contexto da área no Brasil

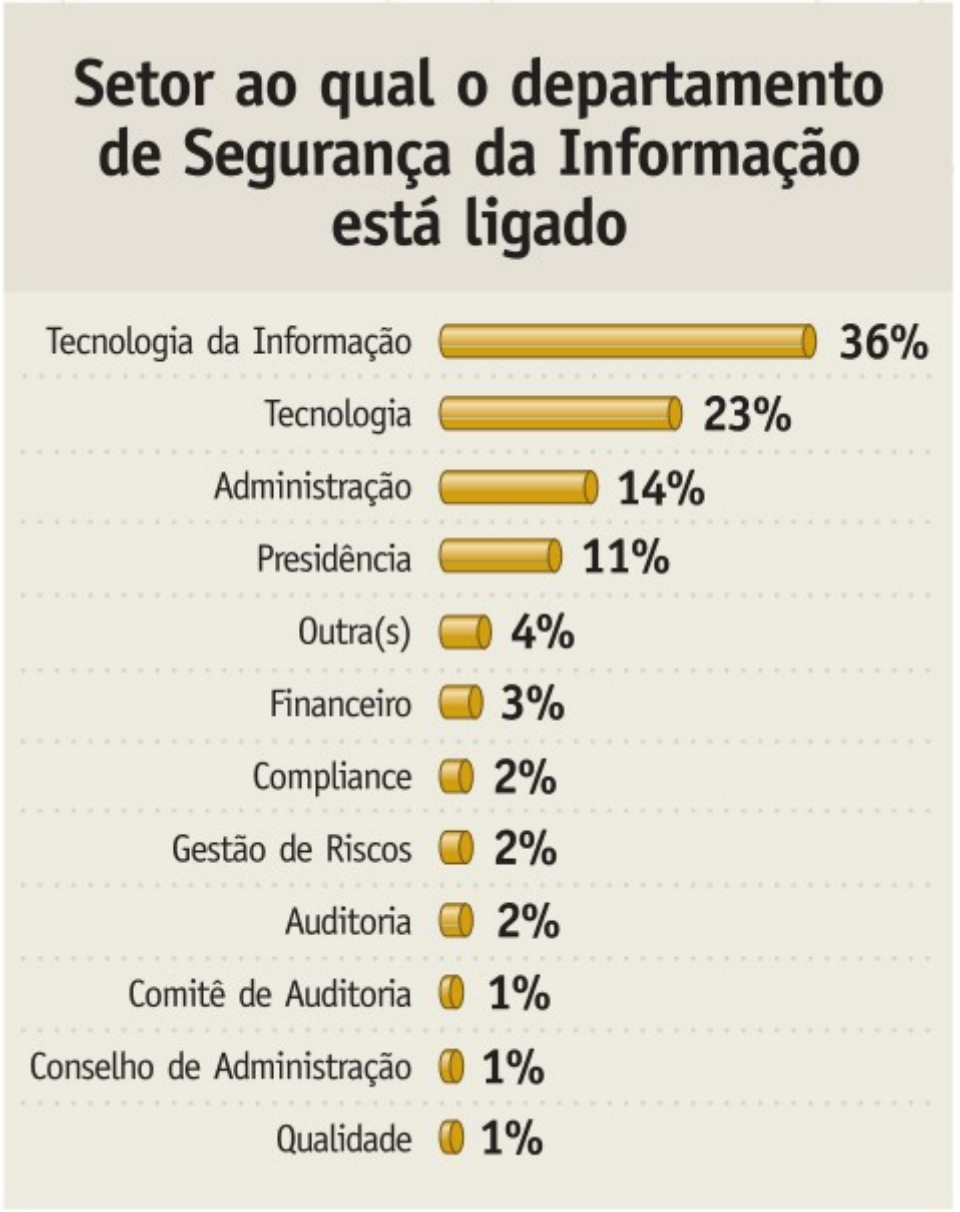
Empresas que não possuem planejamento formal de segurança (porcentagem por segmento)

Comércio	48%
Financeiro	13%
Governo	40%
Indústria	29%
Serviços	42%
Telecom	45%

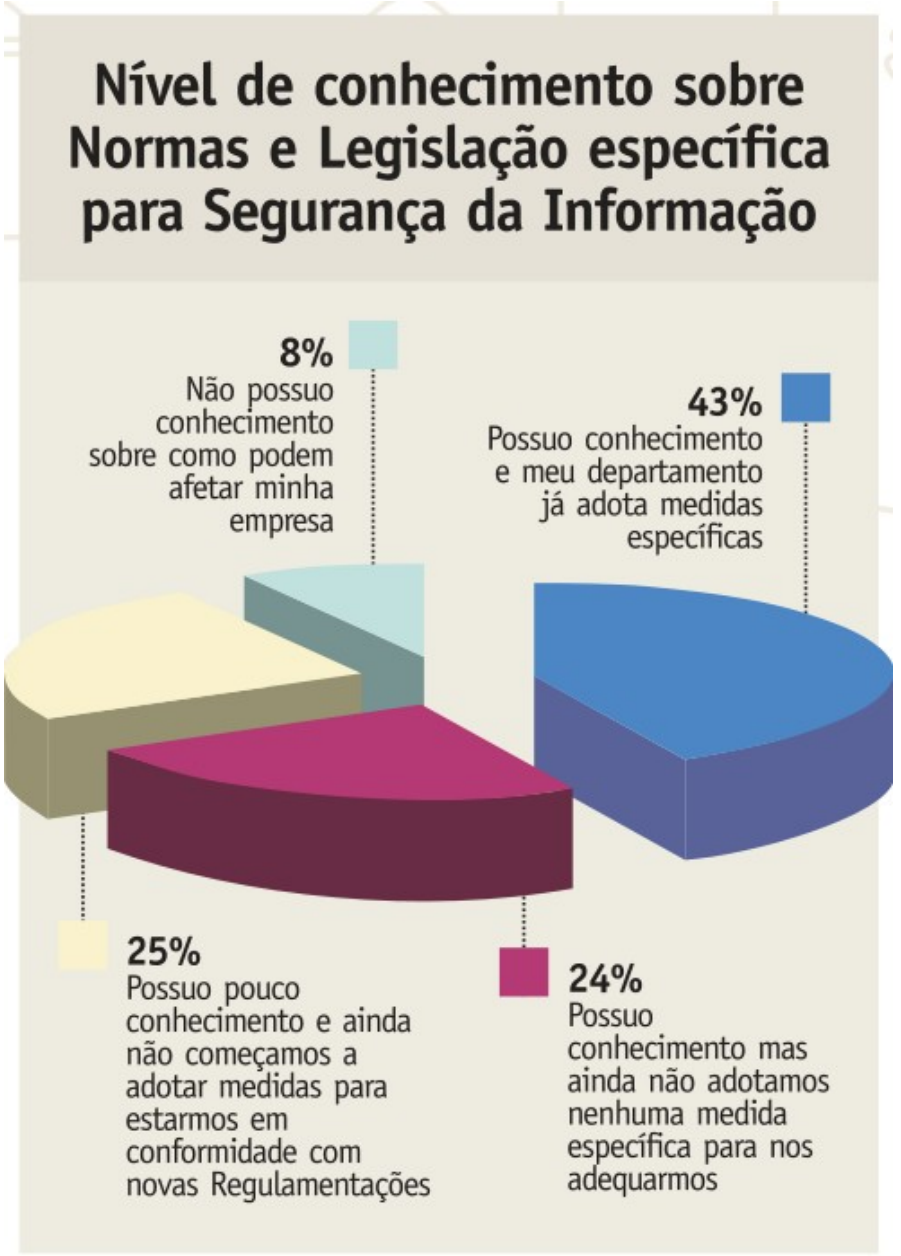
Contexto da área no Brasil

Contexto da área no Brasil

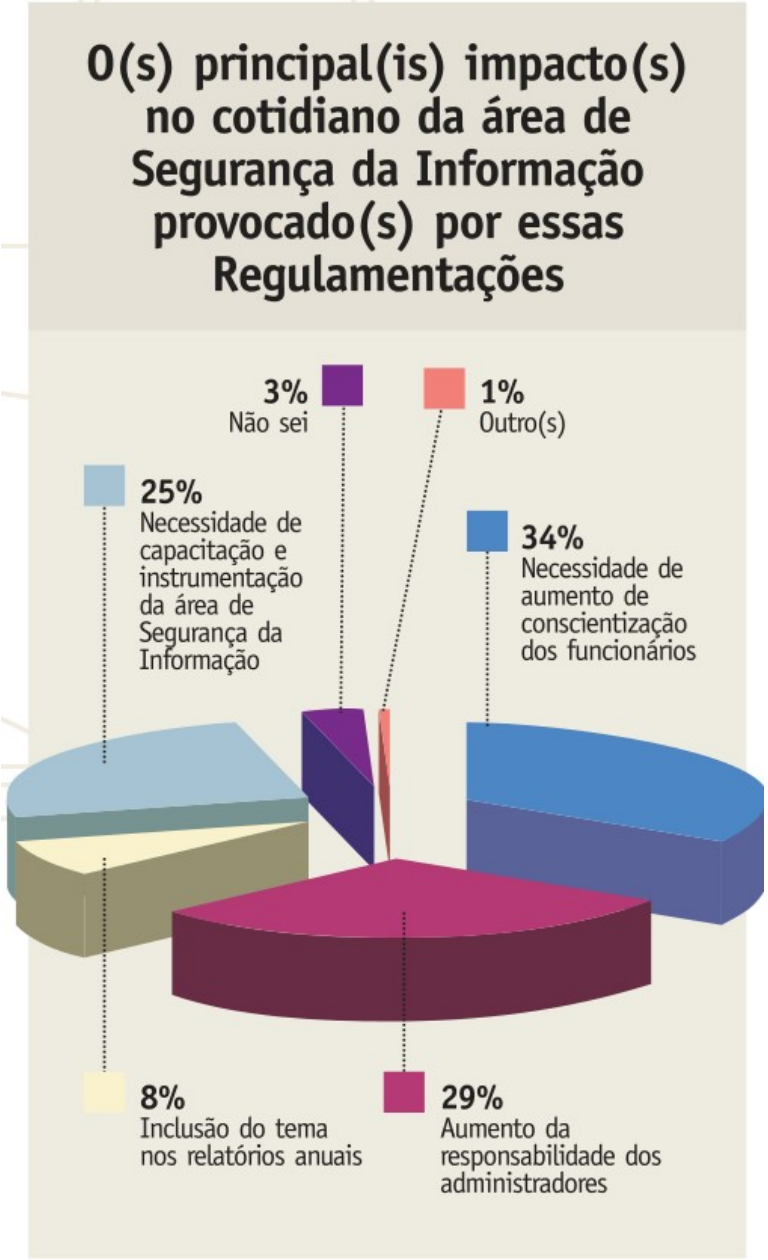
Contexto da área no Brasil



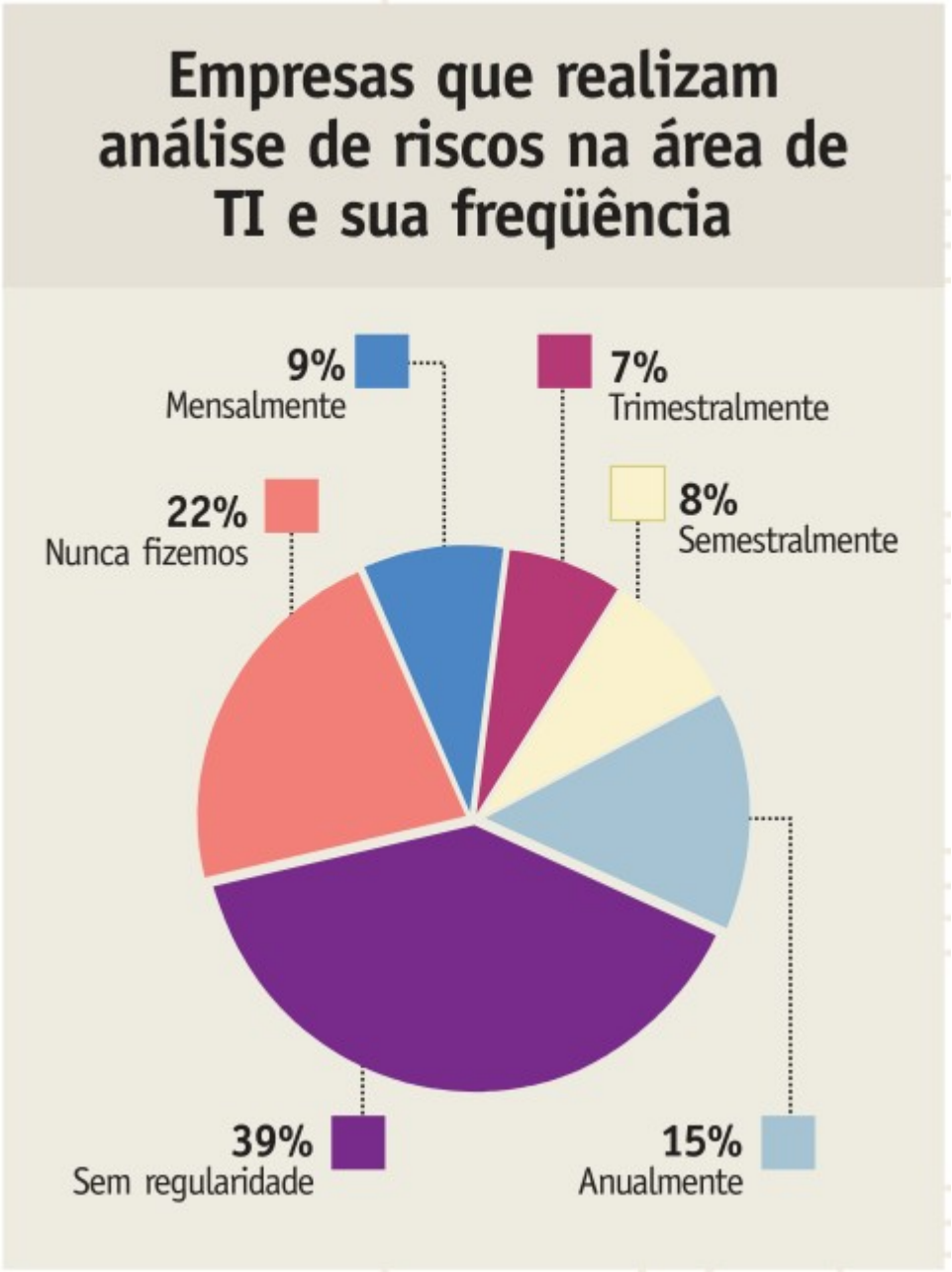
Contexto da área no Brasil



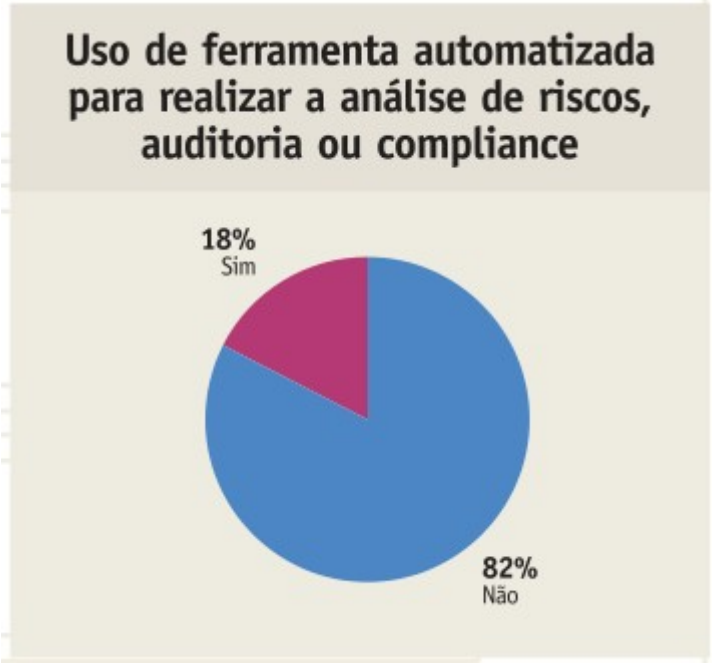
Contexto da área no Brasil



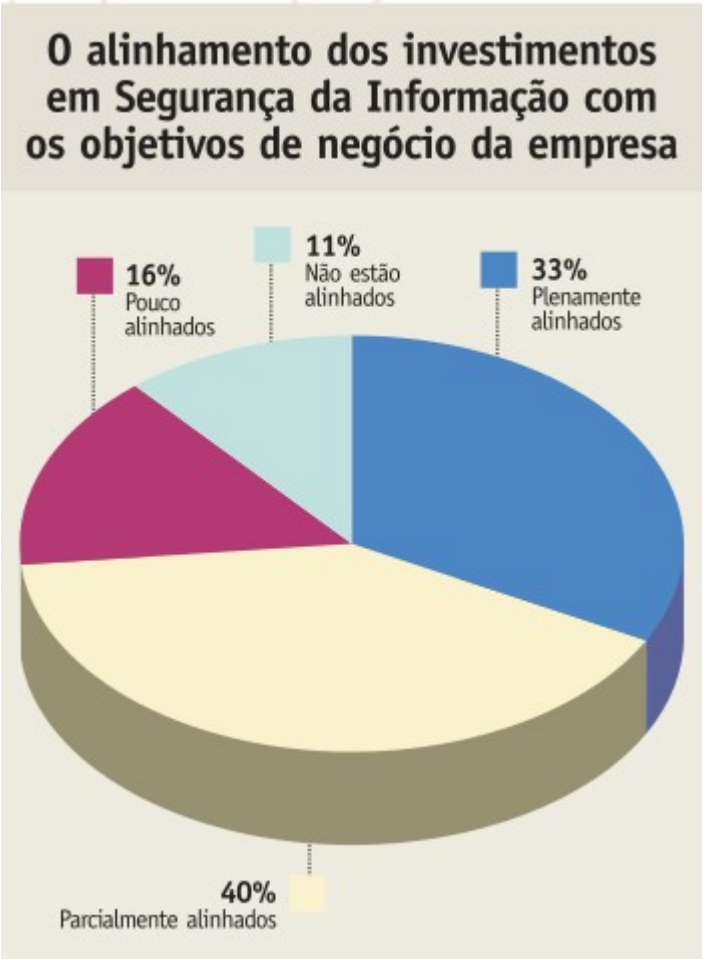
Contexto da área no Brasil



Contexto da área no Brasil



Contexto da área no Brasil



Contexto da área no Brasil

Motivação

Por que se preocupar com segurança?

Problemas mais comuns:

- Destruição de informações e outros recursos.
- Modificação ou deturpação de informações.
- Roubo, remoção ou perda da informação ou de outros recursos.
- Revelação de informações.
- Interrupção de serviços.

As organizações cada vez mais reconhecem o valor e as vulnerabilidades de seus ativos.

O que é segurança da informação

Segurança da Informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança.

Conceitos de base

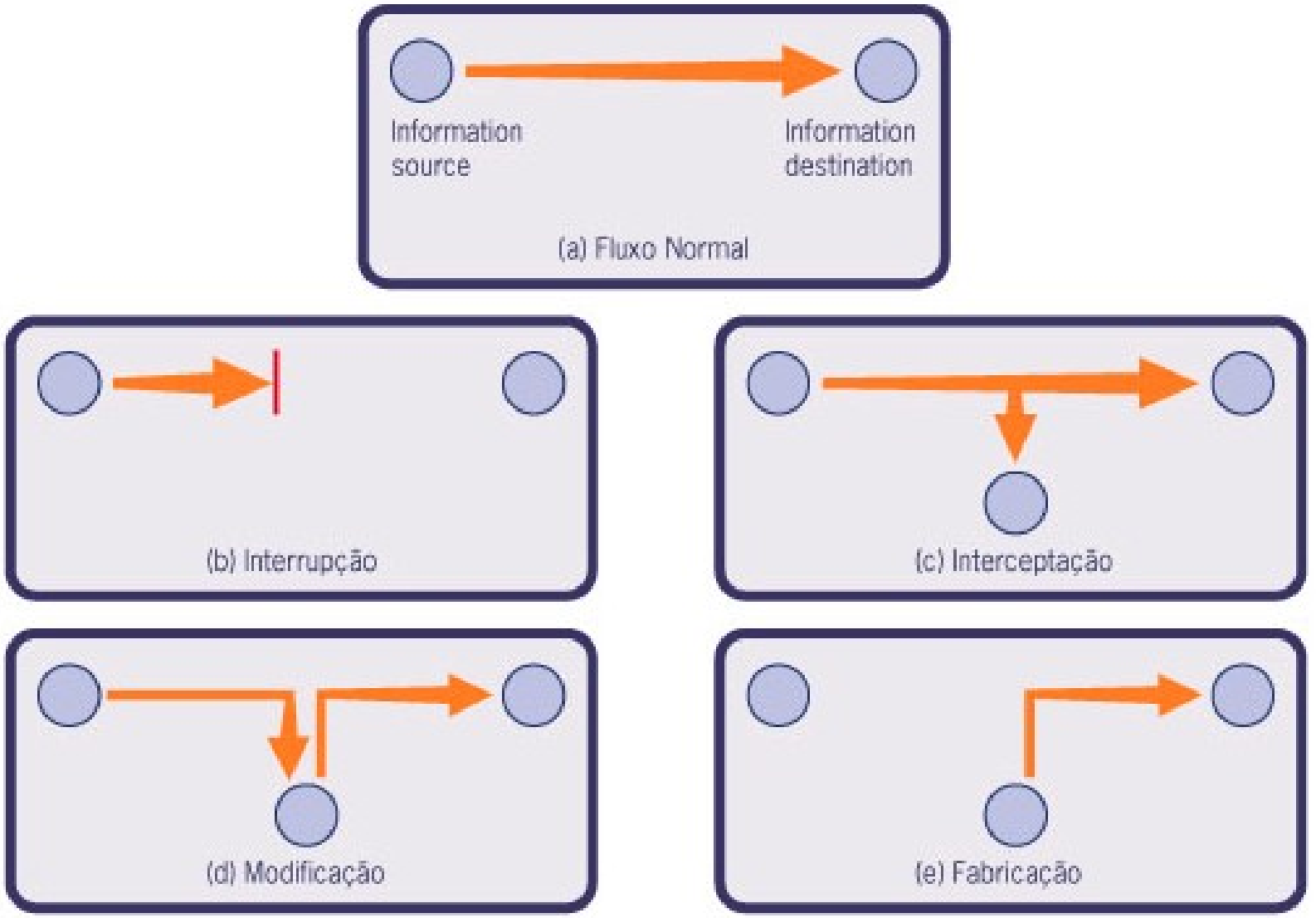
- Incidente de segurança – Corresponde a qualquer evento adverso relacionado à segurança; por exemplo, ataques de negação de serviços (Denial of Service – DoS) e obtenção de acesso não autorizado a informações.
- Ativo – Qualquer coisa que tenha valor para a organização. Alguns exemplos: banco de dados, softwares, equipamentos (computadores, notebooks), servidores, elementos de redes (roteadores, switches, entre outros), pessoas, processos e serviços.
- Ameaça – Qualquer evento que explore vulnerabilidades. Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (vide item 2.18 ABNT NBR ISO/IEC 27002:2007).
- Vulnerabilidade – Qualquer fraqueza que possa ser explorada e comprometer a segurança de sistemas ou informações. Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças (vide item 2.17 ABNT NBR ISO/IEC 27002:2007). Vulnerabilidades são falhas que permitem o surgimento de deficiências na segurança geral do computador ou da rede. Configurações incorretas no computador ou na segurança também permitem a criação de vulnerabilidades. A partir desta falha, as ameaças exploram as vulnerabilidades, que, quando concretizadas, resultam em danos para o computador, para a organização ou para os dados pessoais.
- Risco – Combinação da probabilidade (chance da ameaça se concretizar) de um evento ocorrer e de suas consequências para a organização. Algo que pode ocorrer e seus efeitos nos objetivos da organização.
- Ataque – Qualquer ação que comprometa a segurança de uma organização.
- Impacto – Consequência avaliada de um evento em particular.

Tipos de ataques

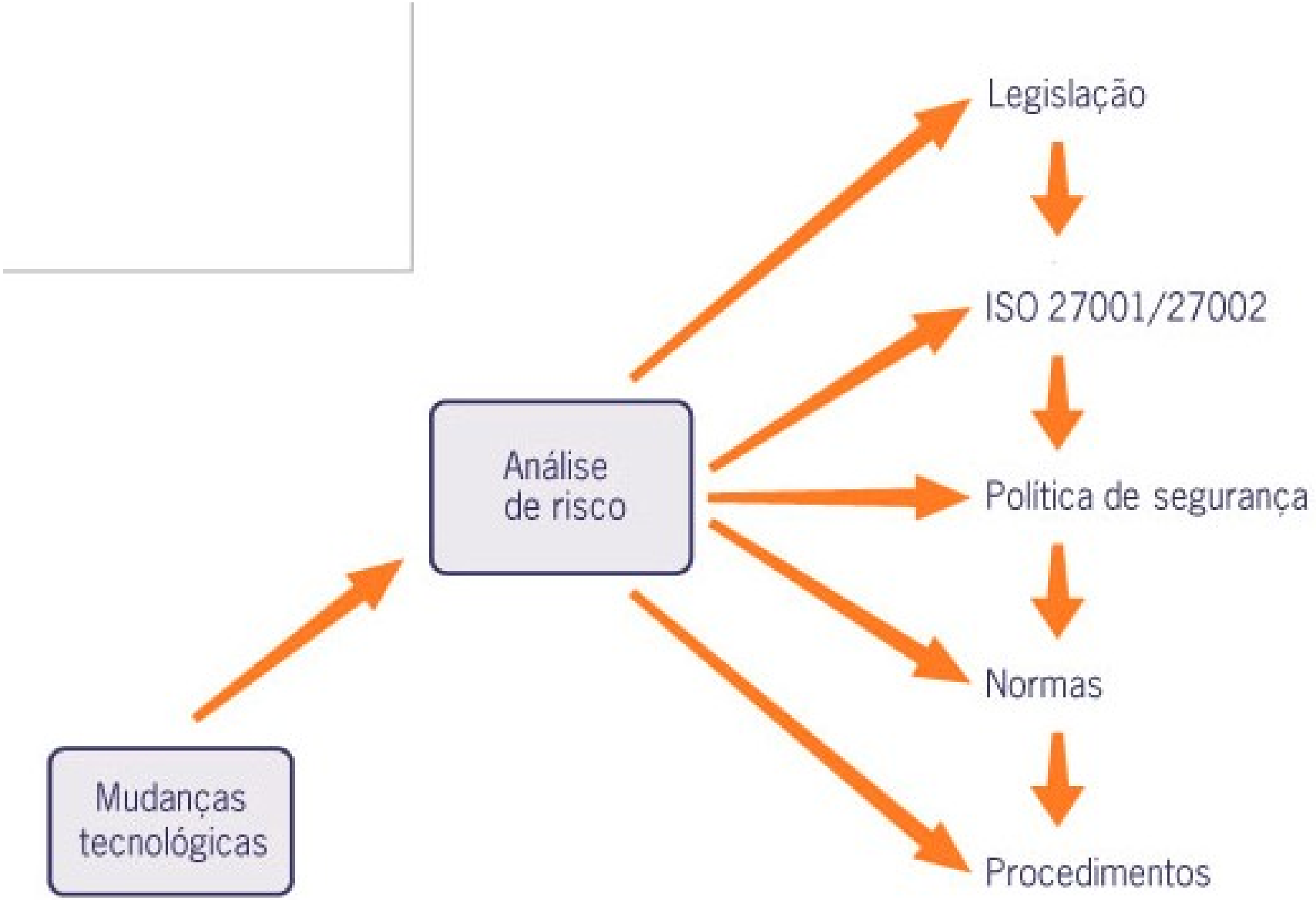
Há quatro modelos de ataque possíveis:

- Interrupção – Quando um ativo é destruído ou torna-se indisponível (ou inutilizável), caracterizando um ataque contra a disponibilidade. Por exemplo, a destruição de um disco rígido.
- Interceptação – Quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador), caracterizando um ataque contra a confidencialidade. Por exemplo, cópia não autorizada de arquivos ou programas.
- Modificação – Quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador) e ainda alterado, caracterizando um ataque contra a integridade. Por exemplo, mudar os valores em um arquivo de dados.
- Fabricação – Quando uma parte não autorizada (pessoa, programa ou computador) insere objetos falsificados em um ativo, caracterizando um ataque contra a autenticidade. Por exemplo, a adição de registros em um arquivo.

Tipos de ataques



Ciclo da Segurança da Informação



Ciclo da Segurança da Informação

Preparando a organização

Antes de pensar em gestão da segurança da informação em uma organização, é preciso ter em mente as respostas aos seguintes questionamentos:

- O que proteger?
- Contra o quê ou quem?
- Qual a importância de cada recurso?
- Qual o grau de proteção desejado?
- Quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança desejados?
- Quais as expectativas dos diretores, clientes e usuários em relação à segurança da informação?

Exercício de nivelamento 1
Fundamentos de segurança da informação

O que é segurança para você?

O que você entende por segurança da informação?

Explique o que são ativos.

Como você explicaria na sua organização o termo “vulnerabilidade”?