Segurança da Informação e Proteção ao Conhecimento

Aula 02 – Conceitos Básicos

Prof. Dalton Martins
dmartins@gmail.com

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

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

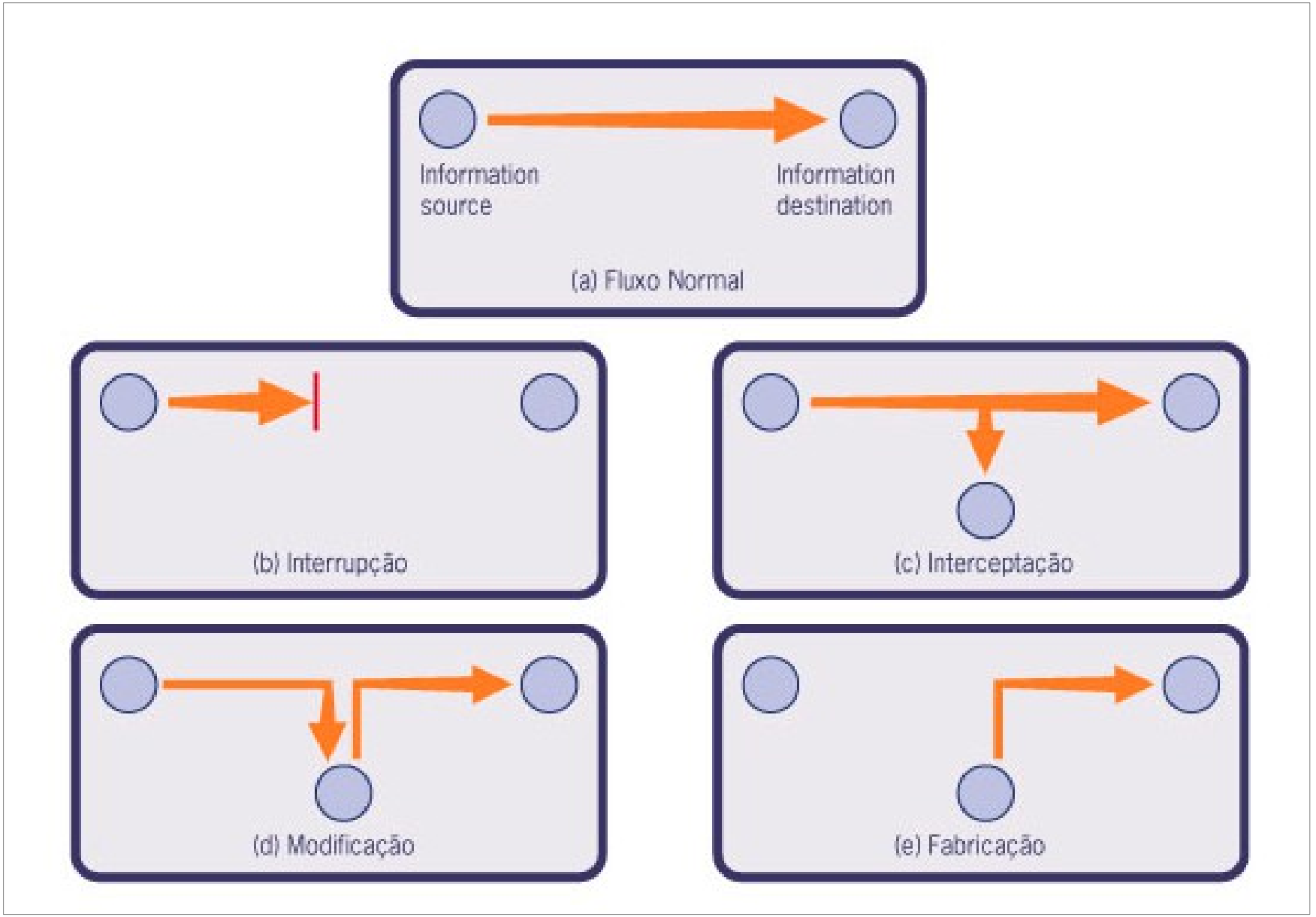
- Incidente de segurança – Corresponde a qualquer evento adverso relacionado à segurança; por exemplo, ataques de negação de serviços (Denial of Service – DoS) e obtenção de acesso não autorizado a informações.
- Ativo – Qualquer coisa que tenha valor para a organização. Alguns exemplos: banco de dados, 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

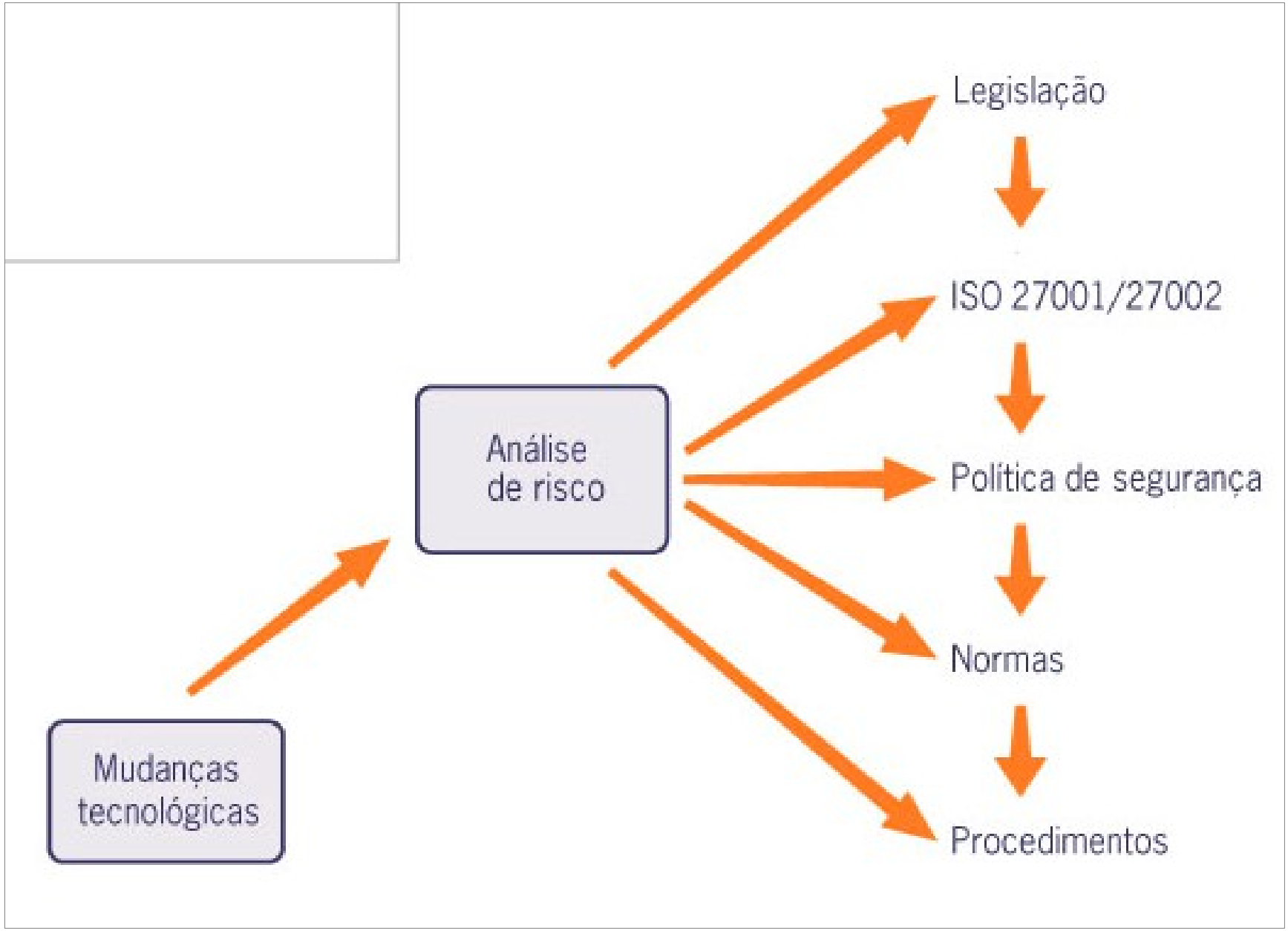
Há quatro modelos de ataque possíveis:

- 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”?

Requisitos de segurança

Há três fontes principais a considerar ao estabelecer os requisitos de segurança da informação de uma organização:

- Análise/avaliação de riscos – Considera os objetivos e estratégias de negócio da organização, resultando na identificação de vulnerabilidades e ameaças aos ativos. Neste contexto, leva-se em conta a probabilidade de ocorrência de ameaças e o impacto para o negócio.
- Legislação vigente – Estatutos, regulamentação e cláusulas contratuais a que devem atender a organização, seus parceiros, terceirizados e fornecedores.
- Conjunto de princípios – Objetivos e requisitos de negócio para o processamento de dados que a organização deve definir a fim de dar suporte a suas operações.

Seleção de controles

Após a identificação de requisitos de segurança, análise/avaliação dos riscos e tomadas de decisão quanto ao tratamento de riscos em uma organização, pode-se, enfim, selecionar e implementar os controles adequados.

Os controles podem ser selecionados a partir de normas preestabelecidas (por exemplo, as normas ABNT NBR ISO/IEC 27002:2005 e ABNT NBR ISO/IEC 27001:2006) ou de um conjunto de controles específicos para a organização.

Controles para a segurança da informação

Alguns controles podem ser considerados como "primeiros passos" para a segurança da informação nas organizações, tendo como base requisitos legais e/ou melhores práticas para a segurança da informação.

Controle, por definição, é um modo de gerenciar riscos, podendo incluir políticas, procedimentos, diretrizes e práticas que podem ser de natureza administrativa, técnica, legal ou de gestão.

Sob o ponto de vista legal, há os controles considerados essenciais e que dependem da legislação vigente, a saber:

- Proteção de dados e privacidade de informações pessoais;
- Proteção de registros organizacionais;
- Direitos de propriedade intelectual.

Já os controles considerados como melhores práticas para a segurança da informação compreendem:

- Documento da política de segurança da informação;
- Atribuição de responsabilidades para a segurança da informação;
- Conscientização, educação e treinamento em segurança da informação;
- Processamento correto nas aplicações;
- Gestão das vulnerabilidades técnicas;
- Gestão da continuidade do negócio;
- Gestão de incidentes de segurança da informação.

Itens relevantes para a segurança da informação

- Política de segurança da informação;
- Segurança organizacional;
- Gestão de ativos;
- Segurança em Recursos Humanos;
- Segurança física e de ambiente;
- Gerenciamento de operações e comunicações;
- Controle de acesso;
- Aquisição, desenvolvimento e manutenção de SI;
- Gestão de incidentes de segurança;
- Gestão da continuidade do negócio.

Atividades envolvidas

- Gerência de segurança dos sistemas;
- Gerência dos serviços de segurança;
- Gerência dos mecanismos de segurança;
- Gerência da auditoria de segurança.

Fatores críticos para o sucesso da segurança da informação

- Política de segurança da informação;
- Abordagem e estrutura para implementação, manutenção, monitoramento e melhorias da segurança da informação;
- Comprometimento dos níveis gerenciais;
- Entendimento dos requisitos de segurança da informação, da análise, avaliação e gestão de riscos;
- Divulgação eficiente.

Fatores criticos para o sucesso da segurança da informação

- Distribuição e comunicação de diretrizes, politicas e normas para todas as partes envolvidas;
- Provisão de recursos financeiros para a gestão da segurança da informação;
- Provisão da conscientização, treinamento e educação adequados;
- Estabelecimento de um processo eficiente de gestão de incidentes de segurança;
- Implementação de um sistema de medição da gestão da segurança da informação.