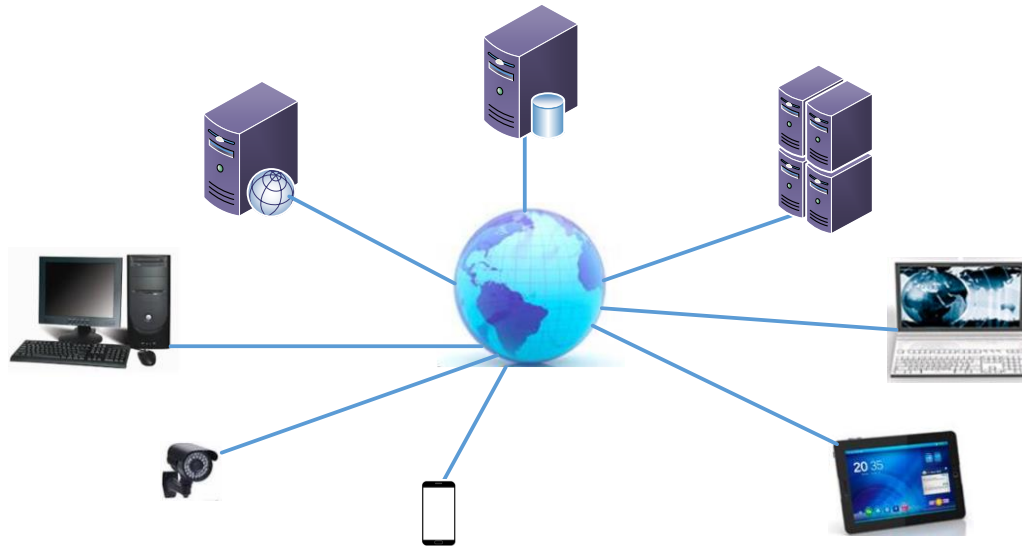


Gestão e Segurança da Informação



Prof. Dr. Márcio Andrey Teixeira
Instituto Federal de São Paulo – Campus Catanduva
Catanduva, SP
Membro Sênior do IEEE
marcio.andrey@ifsp.edu.br

CONTEÚDO

- × INTRODUÇÃO
- × O QUE É INFORMAÇÃO?
- × SEGURANÇA DA INFORMAÇÃO
- × CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO
- × CONSIDERAÇÕES FINAIS
- × REFERÊNCIAS BIBLIOGRÁFICAS
- × EXERCÍCIOS

CONTEÚDO

- × INTRODUÇÃO
- × O QUE É INFORMAÇÃO?
- × SEGURANÇA DA INFORMAÇÃO
- × CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO
- × CONSIDERAÇÕES FINAIS
- × REFERÊNCIAS BIBLIOGRÁFICAS
- × EXERCÍCIOS

INTRODUÇÃO

- ✖ Apresentar e discutir os principais conceitos relacionados a Segurança da Informação;
- ✖ Relacionar esses conceitos com a realidade do aluno e das organizações;
- ✖ Criar uma visão integrada → Segurança da Informação = Gestão Administrativa + Tecnologias de Software e Hardware.

O QUE É INFORMAÇÃO ?



Fonte: <https://conceitos.com/wp-content/uploads/2014/05/Informacao.jpg>

- ✕ Apresentar e discutir os principais conceitos relacionados a Segurança da Informação;

O QUE É INFORMAÇÃO ?

- ✖ A Informação pode ser definida por um conjunto de dados tratados e organizados de tal maneira que tragam algum significado ou sentido dentro de um dado contexto [1].
- ✖ Em um contexto geral, este conjunto de dados tem como objetivo **reduzir a incerteza ou aprofundar os conhecimentos sobre um assunto de interesse a partir do que já se possui** [2].
- ✖ Ela também se refere ao **esclarecimento do funcionamento de um determinado processo ou de um objeto.**

O QUE É INFORMAÇÃO ? (CONTI...)

- ✖ Ela também permite **resolver problemas e tomar decisões, com base no uso racional deste conhecimento adquirido através dela.**
- ✖ No âmbito da comunicação, a informação é o conhecimento que se torna público através dos meios de comunicação ou por meio da publicidade.
- ✖ Nas áreas da informática e da tecnologia, a informação pode ser a reunião dos dados processados em um computador e que são capazes de gerar resultados para um determinado projeto.

O QUE É SEGURANÇA DA INFORMAÇÃO?



Fonte: <https://www.revistaferamental.com.br/?cod=artigo/proteja-seu-negocio-invista-seguranca-informacao/>

O QUE É SEGURANÇA DA INFORMAÇÃO?

- ✖ 1) Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas. (ABNT NBR ISO/IEC 27002: 2005).
- ✖ 2) Podemos definir a Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. (Sêmola, 2003, p. 43).

O QUE É SEGURANÇA DA INFORMAÇÃO?

- ✖ 3) A segurança de informação é caracterizada pela aplicação adequada de dispositivos de proteção sobre um ativo ou um conjunto de ativos visando preservar o valor que este possui para as organizações. A aplicação destas proteções busca preservar a confidencialidade, a integridade e a disponibilidade (CID), não estando restritos somente a sistemas ou aplicativos, mas também informações armazenadas ou veiculadas em diversos meios além do eletrônico ou em papel. (Bastos & Caubit, 2009, p. 17).

O QUE É SEGURANÇA DA INFORMAÇÃO?

- ✖ Quais são os aspectos em comum nas definições acima ?????

O QUE É SEGURANÇA DA INFORMAÇÃO?

- ✖ Quais são os aspectos em comum nas definições acima ?????
- ✖ Os elementos “confidencialidade, integridade e disponibilidade” – conhecidos por diversos autores como “CID”. Tais elementos não são uma mera coincidência, mas sim, **os três pilares principais (ou princípios básicos) da Segurança da Informação.**

O QUE SE FAZ UM PROFISSIONAL DE SI?

- ✘ Basicamente: proteger os **atributos** de segurança da informação;
- ✘ Detecção de um comprometimento ou ataque sobre os **atributos**;
- ✘ Ser capaz de **reagir e corrigir** situações.

ATRIBUTOS – O QUE SÃO?

- ✗ *Confidencialidade;*
- ✗ *Confiabilidade;*
- ✗ *Integridade;*
- ✗ *Equipamentos;*
- ✗ *Informação;*
- ✗ *E muito mais.*

SEGURANÇA DA INFORMAÇÃO

- ✖ Segurança da Informação tem tomado uma posição de frente em poucos anos.
- ✖ Percebemos que na Sociedade da Informação não passamos de um **usuário** e **senha** de acesso.
- ✖ Lembrando que: *qualquer pessoa com nossas credenciais pode se passar por nós, na rede ou na Internet.*

SEGURANÇA DA INFORMAÇÃO

- ✖ O conceito de Segurança da Informação não foca somente a proteger usuários de terem suas senhas ou identidade roubada.
- ✖ As empresas, para se manterem ou se tornarem competitivas, precisam incluir em suas estratégias de negócio **serviços relacionados a TI (Tecnologia da Informação)**.
- ✖ Onde existe TI, existe a necessidade de **SI: *Segurança da Informação***.

SEGURANÇA DA INFORMAÇÃO

- ✖ Em algumas empresas, ou, podemos pensar, a maioria, a regra de negócio é tão importante que, se houver falha na segurança, o plano de vida da empresa fica todo comprometido.
- ✖ Exemplos:
 - ✖ Bancos
 - ✖ Operadoras de Cartões de Crédito
 - ✖ Planos de Saúde
 - ✖ Comércio Eletrônico (Lojas virtuais)
 - ✖ E outras mais...

SEGURANÇA DA INFORMAÇÃO

- ✖ Claro que se o problema ocorrer, nem sempre, a empresa não terá suas atividades encerradas, porém o prejuízo poderá ou será muito grande. Sendo assim a preocupação com a segurança será eterna.
- ✖ Pergunta:
- ✖ *Se a segurança de uma empresa que possui comércio eletrônico, ou seja, vendas pela Internet for comprometida por algumas horas?*

Lucro/Vendas → Prejuízo, Desconfiança, Insegurança, Concorrência

SEGURANÇA DA INFORMAÇÃO

- ✖ A Segurança da Informação nas empresas **não se limita** a problemas on-line ou sites fora do ar.
- ✖ Uma rede paralisada também causa prejuízos, transtornos (colaboradores e clientes) e dados perdidos causam prejuízos ainda maiores.
- ✖ É obrigação do técnico, consultor, gestor ou administrador de redes cuidar para que os negócios da empresa tenham continuidade. E isso se faz conhecendo os **riscos, antecipando os problemas e implementando soluções**, antes mesmo de algo sair errado.
- ✖ Faça simulações, testes e treinamentos.

SEGURANÇA DA INFORMAÇÃO

- ✖ Nos primórdios do conceito sobre da Segurança da Informação, a tendência era resolver os problemas de segurança na medida em que apareciam.
- ✖ Uma maneira de trabalhar totalmente fora de cogitação hoje em dia. As empresas estão cada vez mais dependentes de TI.
- ✖ No cenário atual, o profissional de TI antecipa o problema e o corrige. Ou nas piores urgências, tem que existir um “plano B”, ou melhor dizendo, um plano de contingência.
- ✖ Sendo assim, tornaria o impacto do incidente o menor possível e mantendo o funcionamento da empresa.

SEGURANÇA DA INFORMAÇÃO X CIBERSEGURANÇA

- ✗ Segurança da Informação é a mesma coisa que segurança cibernética?

SEGURANÇA DA INFORMAÇÃO X CIBERSEGURANÇA

- ✖ Cibersegurança é a prática de proteger informações e dados que chegam ao usuário da organização, provenientes de fontes externas e somente por meio de protocolos de internet.
- ✖ Se alguém do outro lado do mundo conseguir invadir a rede de uma empresa e violar seu sistema, esta companhia precisará de uma melhor segurança cibernética.

SEGURANÇA DA INFORMAÇÃO X CIBERSEGURANÇA

- ✖ Cibersegurança é a prática de proteger informações e dados que chegam ao usuário da organização, provenientes de fontes externas e somente por meio de protocolos de internet.
- ✖ Se alguém do outro lado do mundo conseguir invadir a rede de uma empresa e violar seu sistema, esta companhia precisará de uma melhor segurança cibernética.
- ✖ Nem tudo que é segurança da informação envolve a cibersegurança, mas toda cibersegurança envolve a segurança da informação [3].

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- + Extrair as informações dos dados exige conhecimento e equipamento.
- + A maioria de nós talvez seja incapaz de identificar um átomo, uma molécula, ou uma constelação. Mas todos estes são exemplos de dados, de onde concluímos que a informação está nos dados, mas nem todos são capazes de extrair as informações dos dados.
- + Em informática os dados são registros optoeletromagnéticos que conhecemos como bits.

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✖ Na Sociedade da Informação, o ponto mais importante dessa argumentação, é que nós deixamos de ser pessoas e temos a existência confundida com a informação que nos representa.
- ✖ Segurança da Informação é coibir, impedir e recuperar informações extraídas dos dados.
- ✖ Levando em consideração que os dados precedem a informação, proteger os dados é proteger a informação. **Quem tem acesso aos dados, tem acesso às informações.**
- ✖ O grande desafio é justamente proteger informações que sequer existem fora do meio digital. Os dados de acesso bancário a sua conta ou à conta da sua empresa só existem na forma de bits, armazenados optoeletromagneticamente em algum servidor.

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✖ Bastaria pôr um documento ou planilha impresso em um cofre para torná-lo seguro.
- ✖ Já um documento ou planilha eletrônico pode ser enviado, interceptado, copiado e distribuído, bastando um pequeno descuido da pessoa responsável.

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✖ Concluimos que Segurança da Informação é:
- ✖ “É a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidade de negócios” [ISO 27002].
 - + As informações podem existir em diversas formas;
 - + O mesmo ocorre com as vulnerabilidades e ameaças;
 - + Concluimos que: os meios utilizados para proteger documentos e objetos materializados não se aplicam aos meios digitais.
 - + Precisamos identificar os elementos que a segurança da informação busca proteger. Que elementos são estes?

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✖ Ativos
- ✖ Todo elemento que compõe o processo da comunicação: a informação, seu emissor, o meio pelo qual ela trafega, armazenamento, até seu receptor.
- ✖ Qualquer elemento que tenha valor para a organização [ISO 27002];
- ✖ Possuem um valor para as empresas e precisam ser protegidos para que os negócios da empresa não sejam prejudicados.
- ✖ Ativos em Segurança da Informação é bem diferente da definição de ativos utilizada nas áreas contábeis e financeira.
- ✖ Em TI ativos são as informações, o que dá suporte a informações e pessoas.

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✕ Para o início do planejamento, devemos inventariar os ativos, ou seja, classificá-los em categorias:
 - + **Informações:** todo tipo de informação registrada, impressas ou armazenadas em meio digital. Exemplos: cartas, documentos, livros de registro, arquivos armazenados, arquivos de configuração, crachás, etc.
 - + **Equipamentos:** todos os equipamentos que dão suporte à informação durante o seu uso, tráfego e armazenamento. Exemplos: estações de trabalho, servidores, rede, discos de armazenamento, etc.
 - + **Aplicações:** softwares de uso da empresa. Exemplos: SO., pacotes de escritório, banco de dados, e-mail, ERP, etc.
 - + **Usuários:** todos que de alguma forma tenham contato com os ativos da empresa. Exemplos: estagiários, pessoal da limpeza, fornecedores, etc.

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✖ Os ativos são três: informação, suporte à informação e pessoas.
- ✖ Podem ser reorganizados em grupos para melhor atender a estrutura organizacional da empresa.

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✖ A Segurança da Informação visa proteger os ativos, com base na preservação de **três princípios clássicos**:



CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✖ A Segurança da Informação visa proteger os ativos, com base na preservação de **três princípios clássicos**:



CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✖ **Confidencialidade:** certeza de que o que foi dito, escrito ou falado será acessado somente por pessoas autorizadas.
- ✖ Diferentes informações tem diferentes graus de sigilo: confidencial, restrita, sigilosa ou pública.
- ✖ Os critérios de classificação levam em consideração a informação e o público ao qual se destinam.
- ✖ **Obs: Informação** é diferente de **dados** (representação da informação). Um dado pode estar acessível a qualquer entidade, mas não revela a informação que ela contém!

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✘ **Integridade:** garantia de que a informação não foi alterada (de forma indevida ou não-autorizada);
- ✘ A quebra da integridade ocorre quando a informação é corrompida, falsificada ou roubada;
- ✘ A informação recebida precisa ser a mesma que foi enviada.
- ✘ Arquivos, pen drive criptografado/descriptografado, etc.

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✖ **Disponibilidade:** garantia de que a informação será acessada quando necessário; O sistema tem que estar disponível!
- ✖ A informação precisa estar disponível quando é requisitada.
- ✖ Disponibilidade (“Plano B, C ou até mais”) → estratégias de contingência em casos de incidentes, desastres, problemas no tráfego da rede, etc.
- ✖ Obs: Ataques contra a disponibilidade são os ataques de negação de serviço (*DoS - Denial of Service*), ou Distributed DoS (DDoS).
- ✖ Algumas medidas: redundância, controle de acesso físico.

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✗ **Autenticidade:** Garantir que o originador de uma mensagem seja corretamente identificado pelo seu destinatário.
- ✗ A verificação de autenticidade é necessária após todo o processo de identificação.
- ✗ Verifica se o dado é autentico.
- ✗ Esse processo deve ocorrer durante todo o processo de comunicação. Quem iniciou a conversa foi a mesma que finalizou ?

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

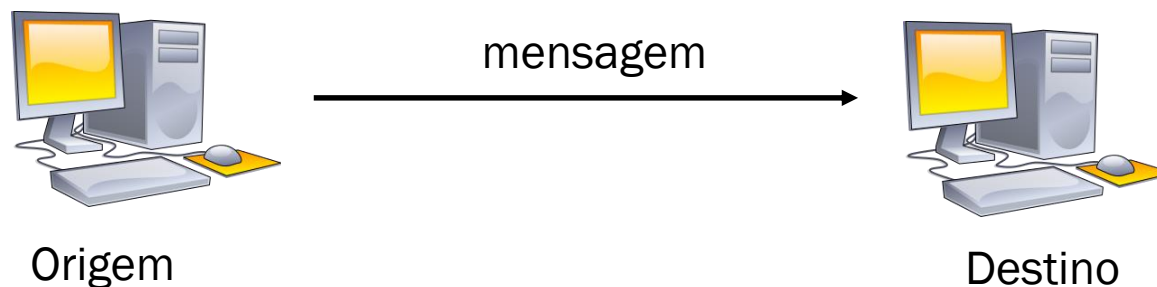
- ✗ **Irretratabilidade:** O emissor e o destinatário das informações não podem negar a sua transmissão, recepção ou posse. (Assinatura Digital).
- ✗ Relaciona a pessoa (usuário) com a assinatura digital.

CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

- ✖ Autenticidade x Irretratabilidade
- ✖ Um usuário envia uma mensagem e utiliza um carimbo para marcar a autenticidade.
- ✖ Como saber quem carimbou o documento? (Irretratabilidade)

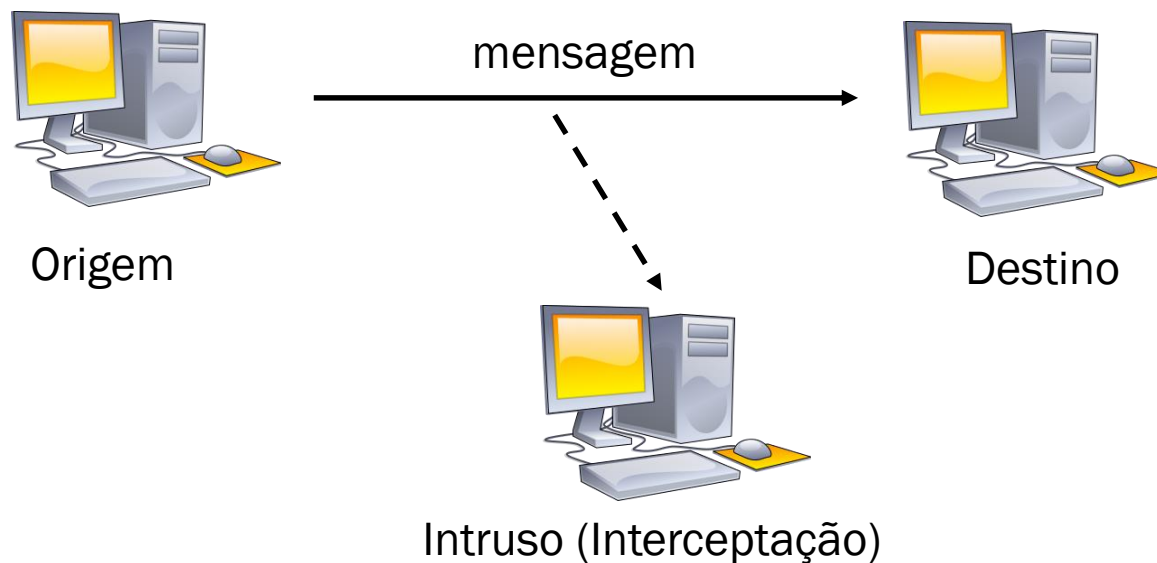
CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

✗ Exemplos de ataques!!



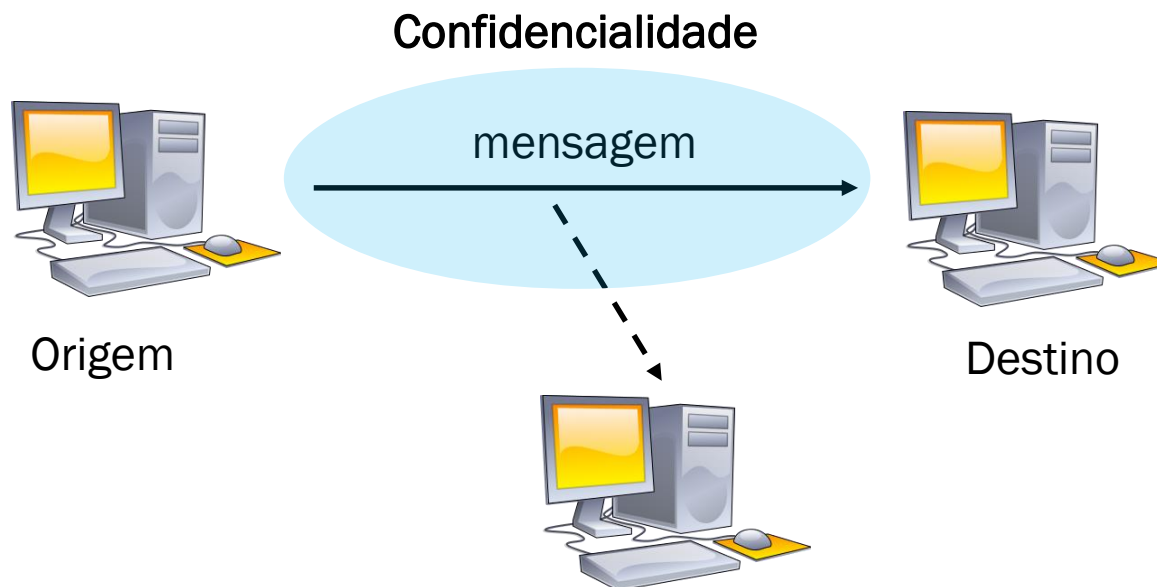
CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

✗ Exemplos de ataques!!



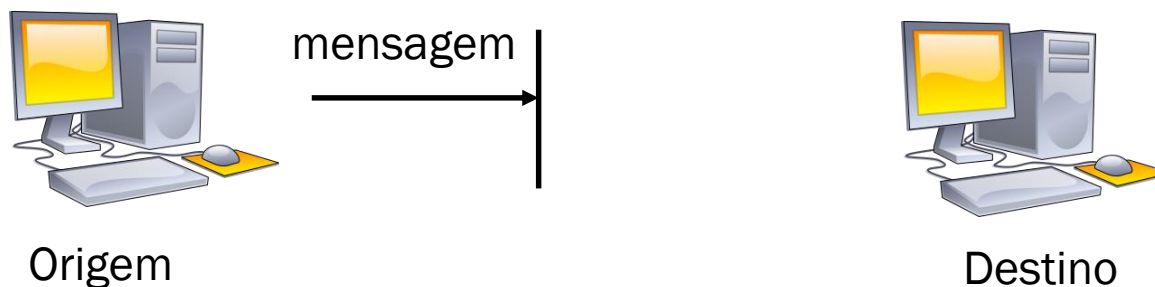
CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

✗ Exemplos de ataques!!



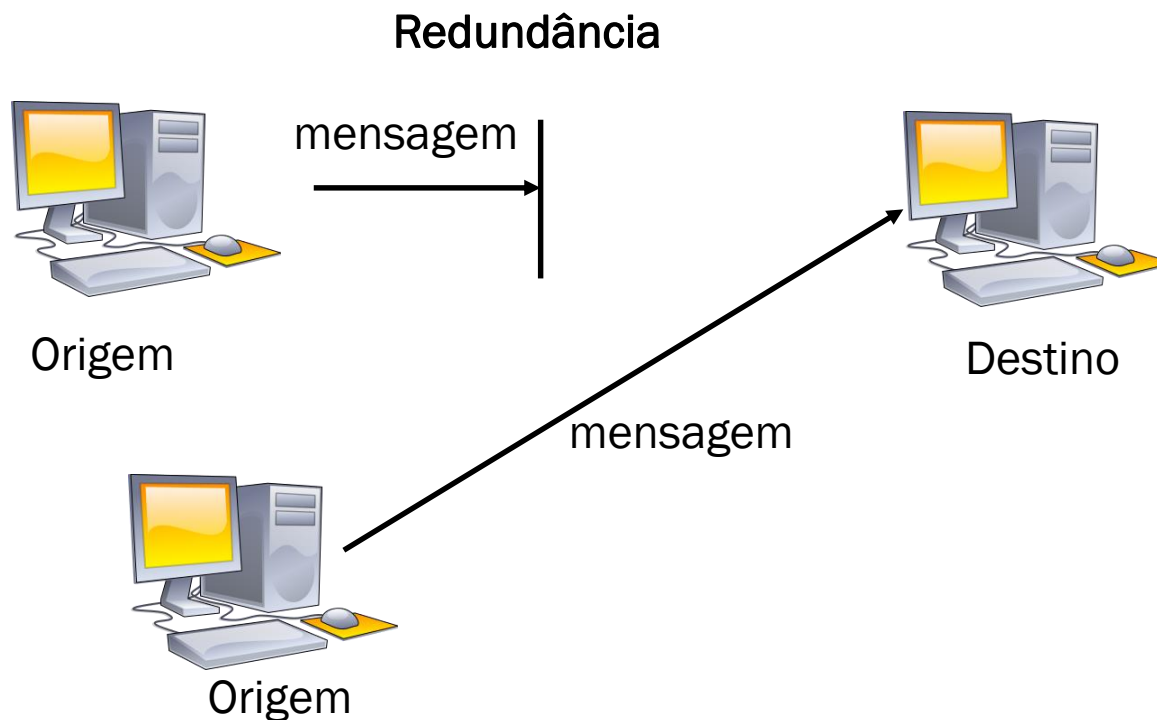
CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

✗ Exemplos de ataques!!



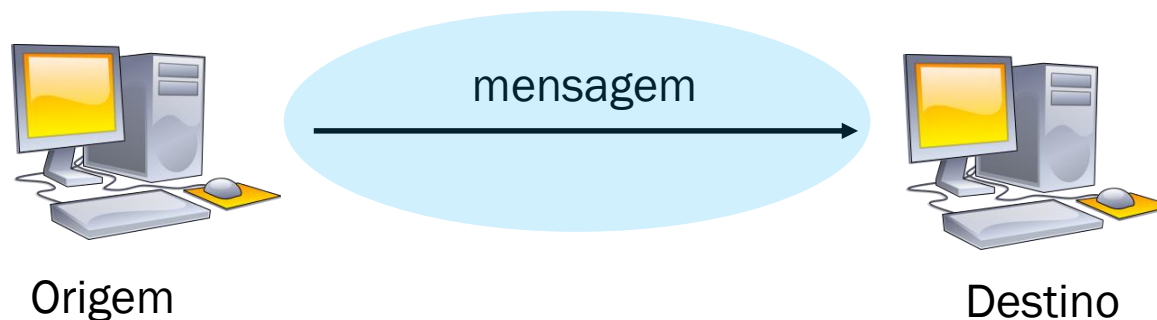
CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

✗ Exemplos de ataques!!



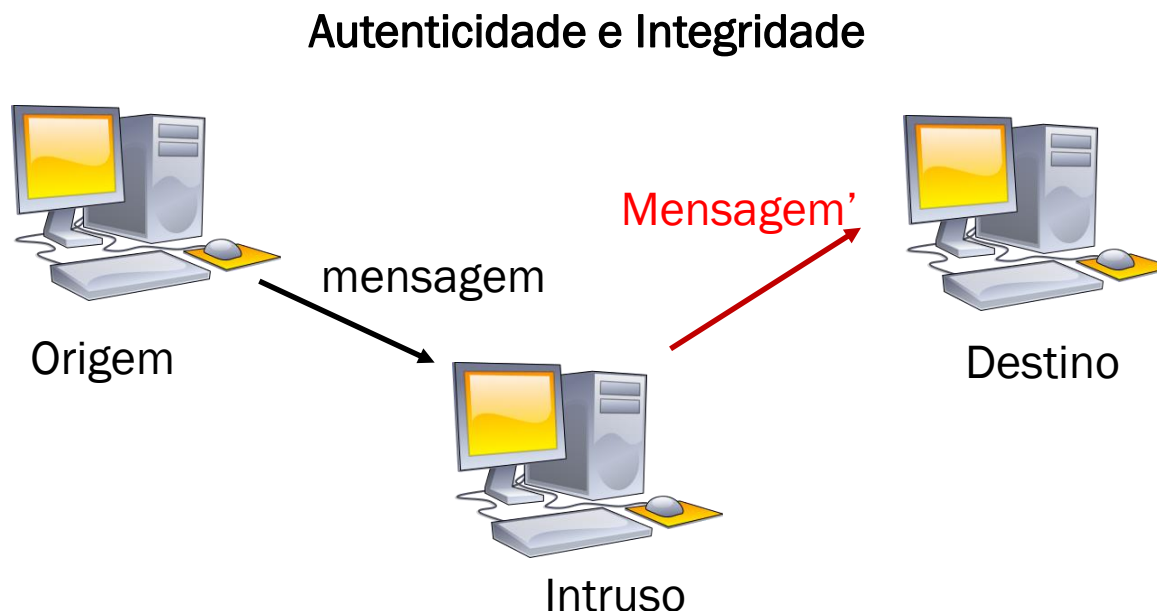
CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

✗ Exemplos de ataques!!



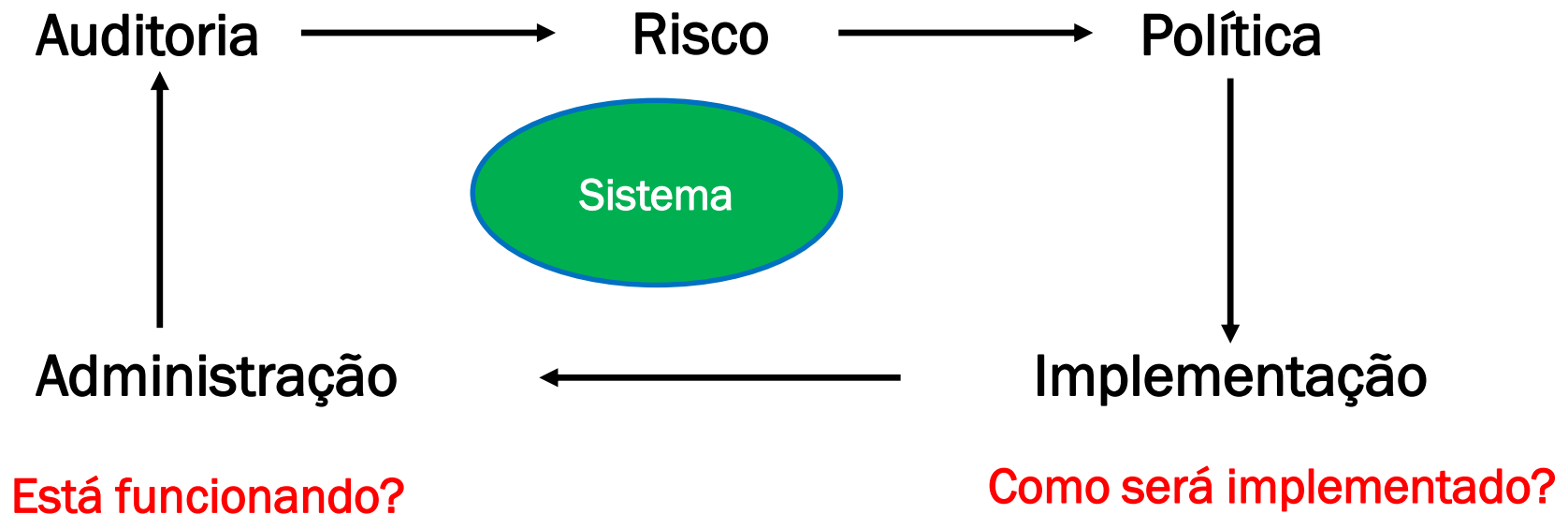
CONCEITOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

✗ Exemplos de ataques!!



SEGURANÇA É UM PROCESSO

✕ O que um sistema de segurança precisa fazer?



CONSIDERAÇÕES FINAIS

- ✗ **Requisitos de Segurança da Informação**
- ✗ Quais os requisitos de SI? Como obter esses requisitos?
- ✗ **Implementação**
- ✗ A Segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados as necessidades da organização;
- ✗ Controles precisam ser estabelecidos, implementados, monitorados, analisados e melhorados para garantir que os objetivos do negócio e de segurança sejam atendidos.

REFERÊNCIAS BIBLIOGRÁFICAS

- ✖ Sêmola, Marcos. **Gestão da Segurança da Informação: uma visão Executiva**. Rio de Janeiro, 2. ed. Campus, 2014.
- ✖ ABNT NBR ISO/IEC 27002:2013. **Código de Prática para a Gestão da Segurança da Informação**.
- ✖ Centro de Estudos, Respostas e Tratamento de Incidentes. **CERT.Br** - <http://www.cert.br/> e <http://cartilha.cert.br>
- ✖ Ramos, Anderson. **Guia Oficial para Formação de Gestores em Segurança da Informação**.

EXERCÍCIOS

- ✖ 1 – É correto afirmar que devemos resolver os problemas em TI, somente quando os mesmos venham a ocorrer? O que podemos fazer, para melhorar e agilizar a solução destes problemas?
- ✖ 2 – Defina o que é um Ativo em uma organização. Cite exemplos.
- ✖ 3 – Considere um ativo de uma determinada categoria, descreva quais são as possíveis vulnerabilidades e ameaças, que este poderá apresentar para a organização.