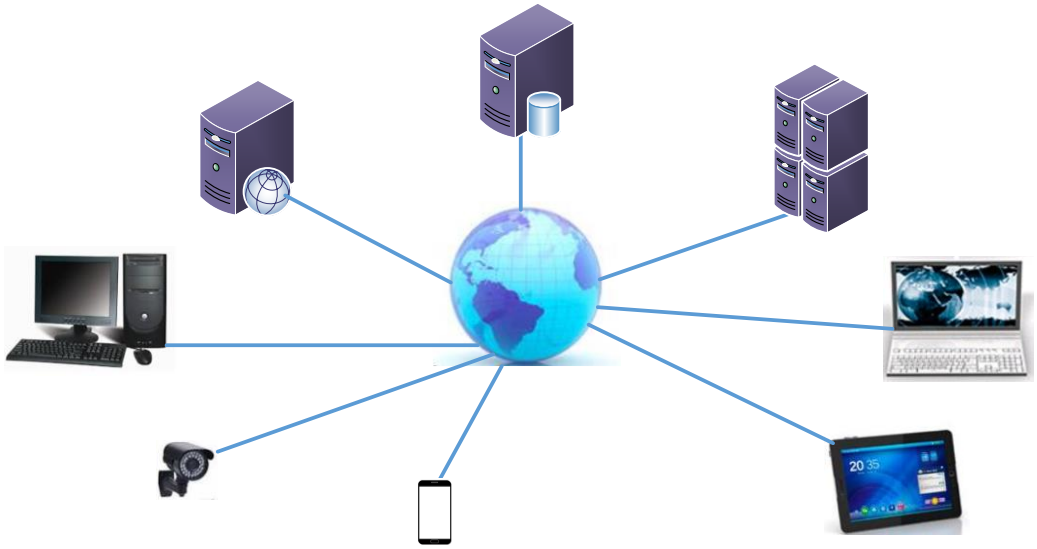
AMEAÇAS, VULNERABILIDADES E RISCOS



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

INTRODUÇÃO

- REVISÃO
- ATAQUES
- AMEAÇAS
- VULNERABILIDADES
- RISCOS
- CONSIDERAÇÕES FINAIS
- PESQUISA

CONCEITOS SOBRE SI

- 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.
- Ativos: **Informação – Suporte à informação – Pessoas**
- Segurança da informação →**Confidencialidade**
  →**Integridade**
  →**Disponibilidade**

CONCEITOS SOBRE SI

- **Ameaças:**

- Causa potencial (agente) de um incidente indesejado, que pode resultar em dano para um sistema ou organização [ISO 27002].

- A segurança da informação precisa prover mecanismos para impedir que as ameaças explorem as vulnerabilidades.

- Podem colocar em risco a confidencialidade, integridade e disponibilidade das informações.

- Não só invasão da rede ou de computadores, outras mais.

AMEAÇAS

- São classificadas em:

- **Ameaças naturais:** incêndios, catástrofes de toda ordem, enchentes.

- **Ameaças intencionais:** invasores, funcionários descontentes, sabotagem, furto, roubo, espionagem, vírus, vandalismo.
- **Ameaças involuntárias** : acidentes, negligência, falha humana, despreparo.
- Um dos objetivos da SI é impedir que as ameaças explorem vulnerabilidades.
- **Através de**: controles, estabelecimento de perímetros e prevendo as vulnerabilidades antes que sejam exploradas ou que algum invasor tome essa iniciativa.

VULNERABILIDADES

- Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças [ISO 27002].

- As vulnerabilidades devem ser gerenciadas (identificadas e corrigidas).

- São classificadas em:
- **Comunicação:** abrange todo o tráfego da informação.
- **Físicas:** instalações.
- **Hardware:** equipamento.
- **Humanas:** pessoas de dentro e fora da empresa.
- **Mídias:** onde as informações estão armazenadas.
- **Naturais:** riscos naturais, inerentes à região da empresa, localidade ou país, clima e tempo.
- **Software:** programas de computador, so, bases de dados, sites e aplicações on-line.

CONCEITOS SOBRE SI

- **Etapas de um ataque**: De maneira geral, o ataque passa por quatro processos:
- Reconhecimento;
- Análise;
- Adaptação;
- Execução.

ATAQUES

- Ataques mais comuns:

- **Scan:** É um ataque que quebra a confidencialidade com o objetivo de analisar detalhes dos computadores presentes na rede (como sistema operacional, atividade e serviços) e identificar possíveis alvos para outros ataques.
- **Worm:** são alguns dos malwares mais comuns e antigos. Malwares são softwares com o intuito de prejudicar o computador "hospedeiro". Essa categoria engloba tanto os vírus quanto os worms, entre diversos outros tipos de programas maliciosos. Os worms são perigosos devido à sua capacidade se espalhar rapidamente pela rede e afetar arquivos sigilosos da empresa.

ATAQUES

- **Ataques mais comuns:**

- **Rootkit:** Esta é uma ameaça que teve origem na exploração de kits do Linux. Tem como objetivo fraudar o acesso, logando no sistema como root, ou seja, usuário com poder para fazer qualquer coisa.
- Os ataques de rootkit são feitos a partir de um malware. Quando a máquina é infectada, os arquivos maliciosos se escondem no sistema e, com essa discrição, liberam o caminho para os invasores agirem.

- **DDoS (negação de serviço):** Os ataques de negação de serviço, mais conhecidos como DDoS (Distributed Denial of Service), estão entre os mais frequentes. Eles têm como objetivo tornar um sistema, infraestrutura ou servidores indisponíveis, causando interrupção dos serviços.

ATAQUES

- **Ataques mais comuns:**

- **Ransomware:** A família ransomware é um conjunto de vírus do tipo malware e tem sido massivamente utilizada para a prática de crimes de extorsão de dados — prática também conhecida como sequestro de dados.
- O modo como o ransomware age varia conforme a sua versão, pois cada malware lançado explora uma diferente brecha do sistema operacional. Esse detalhe, inclusive, é o que torna os ataques tão repentinos e, ao mesmo tempo, fatais.
- Embora a maneira como o vírus se manifesta varie, a finalidade é a mesma: bloquear todos os arquivos do computador, impedindo que o sistema possa ser utilizado adequadamente, e encaminhando mensagens solicitando o pagamento pelo resgate.

ATAQUES

- Ataques mais comuns:

- **Phishing:** A prática de phishing consiste no envio de mensagens de email, onde o invasor se passa por uma instituição legítima e confiável (geralmente bancos e serviços de transação online), induzindo a vítima a passar informações cadastrais.
- Essa é uma das mais antigas armadilhas conhecidas na Internet e, ainda assim, continua atraindo muitas vítimas que utilizam email.

ATAQUES

- Ataques mais comuns:

- **Backdoor:** é um software malicioso muito utilizado para dar acesso remoto não autorizado ao invasor. Assim, ele pode explorar vulnerabilidades do sistema e acessar um ambiente operativo, por exemplo.

- Esse programa trabalha em segundo plano e não é identificado pelo usuário. É muito semelhante a outros malwares e vírus, e também bastante difícil de detectar. O backdoor é um dos tipos de parasitas mais perigosos, pois dá autonomia para que pessoas mal-intencionadas atuem no computador comprometido.

BARREIRAS

- Barreiras como redutor de riscos:
  - Cada uma delas tem uma participação importante no objetivo maior de reduzir os riscos e, por isso, deve ser dimensionada adequadamente para proporcionar a mais perfeita interação e integração, como se fossem peças de um único quebra-cabeça.
- Seis barreiras de segurança:

AMEAÇAS	
1ª BARREIRA	DESENCORAJAR
2ª BARREIRA	DIFICULTAR
3ª BARREIRA	DISCRIMINAR
4ª BARREIRA	DETECTAR
5ª BARREIRA	DETER
6ª BARREIRA	DIAGNOSTICAR
ATIVOS	

BARREIRAS

- **Barreira 1: desencorajar**

- Essa é a primeira das cinco barreiras de segurança, e cumpre o papel importante de desencorajar as ameaças. Estas, por sua vez, podem ser desmotivadas ou perder o interesse e o estímulo pela tentativa de quebra de segurança por efeito de mecanismos físicos, tecnológicos ou humanos. **A simples presença de uma câmera de vídeo**, mesmo falsa, de um aviso da existência de alarmes, campanhas de divulgação da política de segurança ou treinamento dos funcionários informando as práticas de auditoria e monitoramento de acesso aos sistemas já são efetivos nessa fase.

BARREIRAS

- **Barreira 2: dificultar**

- O papel dessa barreira e complementar a anterior através da adoção efetiva dos controles que dificultarão o acesso indevido. Como exemplo podemos citar os dispositivos de controle de acesso físico, como roletas, detectores de metal e alarmes, ou lógicos, como leitores de cartão magnético, biométricos, de senhas, de *smartcards* e de certificados digitais, além do firewall etc.

BARREIRAS

- **Barreira 3: discriminar**

- Aqui o importante é se cercar de recursos que permitam identificar e gerir os acessos, **definindo perfis e autorizando permissões.** Os sistemas são largamente empregados para monitorar e estabelecer limites de acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e bancos de dados. **Os processos de avaliação e gestão do volume de uso dos recursos, como e-mail, impressora ou até mesmo o fluxo de acesso físico aos ambientes, são bons exemplos das atividades dessa barreira.**

BARREIRAS

- Barreira 4: detectar

- Agindo de forma complementar às suas antecessoras, essa barreira deve munir a **solução de segurança de dispositivos que sinalizem, alertem e instrumentem os gestores da segurança na detecção de situações de risco, seja em uma tentativa de invasão, seja em uma possível contaminação por vírus, o descumprimento da política de segurança da empresa ou a cópia e o envio de informações sigilosas de forma inadequada.**
- Entram aqui os sistemas de monitoramento e auditoria para auxiliar na identificação de atitudes de exposição, como o antivírus e o sistema de detecção de intrusos, que reduziram o tempo de resposta a incidentes.

BARREIRAS

- **Barreira 5: deter**

- Essa quinta barreira representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio.
- O acionamento dessa barreira, ativando seus mecanismos de controle, é um sinal de que as barreiras anteriores não foram suficientes para conter a ação da ameaça.
- Nesse momento, medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, respectivamente a ambientes e sistemas, são bons exemplos.

BARREIRAS

- **Barreira 6: diagnosticar**

- Apesar de representar a última barreira no diagrama, essa fase tem o sentido especial de representar a continuidade do processo de gestão de segurança da informação.
- Pode aparecer o fim, mas é o elo de ligação com a primeira barreira, criando um movimento cíclico e contínuo. Devido a esses fatores, essa é a barreira de maior importância.
- Deve ser conduzida por atividades de análise de riscos que considerem tanto os aspectos tecnológicos quanto os físicos e humanos, sempre orientados às características e às necessidades específicas dos processos de negócio da empresa.

BARREIRAS

- **Barreira 6: diagnosticar**

- É importante notar que um trabalho preliminar de diagnóstico mal conduzido ou executado sem metodologia e instrumentos que confiram maior precisão ao processo de levantamento e análise de riscos poderá distorcer o entendimento da situação atual de segurança e, simultaneamente, a situação desejada.
- Dessa forma, aumenta a probabilidade de se dimensionar inadequadamente essas barreiras, distribuindo os investimentos de forma desproporcional, redundante, muitas vezes, e de forma ineficaz. O retorno sobre os investimentos não corresponderá ás expectativas, e a empresa não atingirá o nível de segurança adequado à natureza de suas atividades.

RISCOS

PROBABILIDADE DE:

AMEAÇAS → EXPLORAM → VULNERABILIDADES

Causando perdas ou danos aos ativos e consequente impacto no negócio.

Situação exemplo de risco: com a probabilidade de, em sua própria casa, sumir um dinheiro colocado em cima da geladeira.

Colocando uma câmera de segurança atende os requisitos da **primeira barreira** que é **desencorajar.**

Será o suficiente para garantir que o dinheiro não desapareça?

RISCOS

- Precisamos pensar e entender que as pessoas que estão do outro lado também vão buscar formas de **contornar** as **barreiras de segurança** e **explorar as vulnerabilidades**.

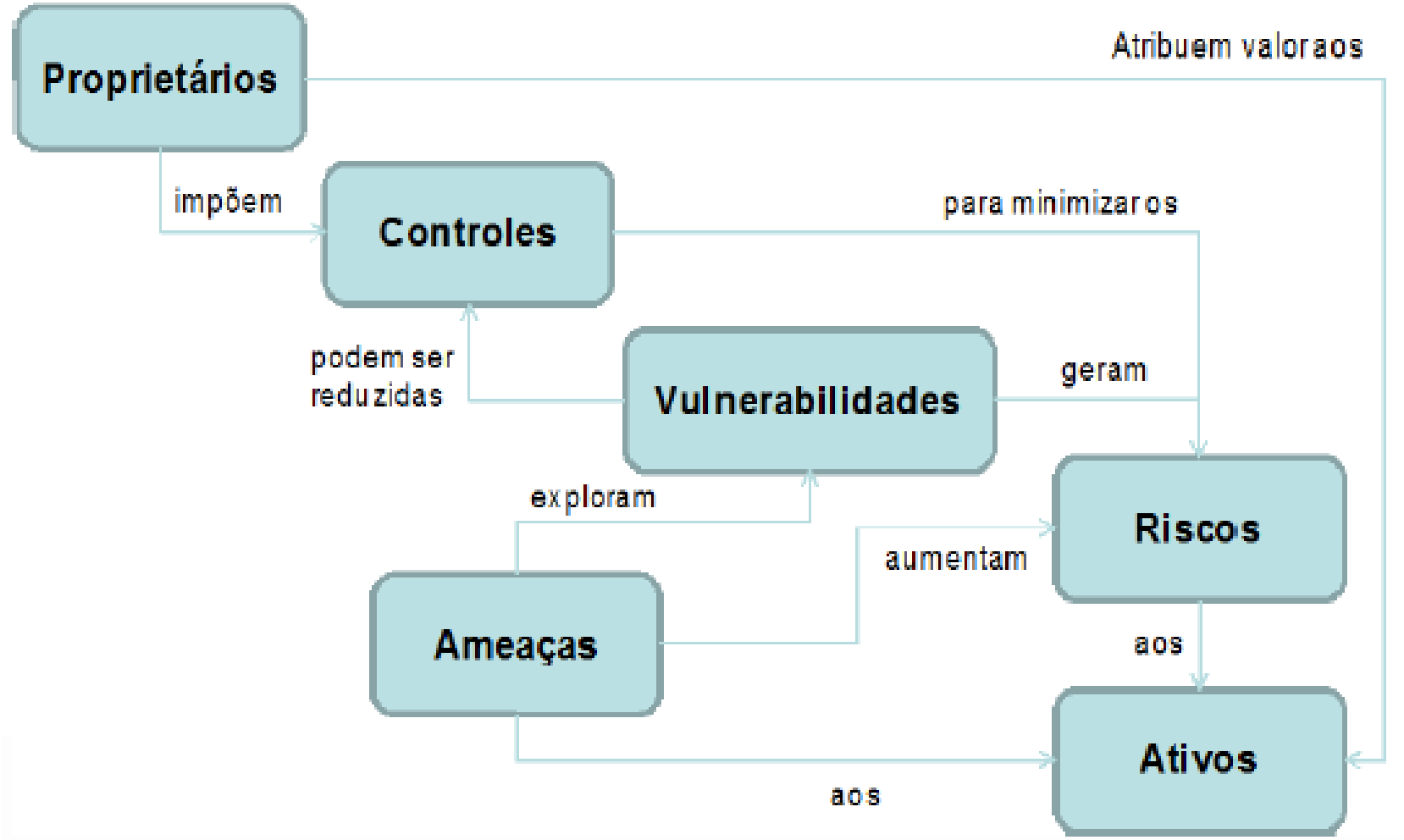
- No caso do dinheiro em cima da geladeira, a câmera de vigilância pode desencorajar, mas não será o suficiente para impedir o "furto".

- Um cofre levaria a segunda barreira de segurança, que é dificultar. Mas será que, seria o suficiente? Talvez até o cofre poderia ser levado, juntamente com a nota.

MEDIDAS DE SEGURANÇA

- São meios para eliminar as vulnerabilidades e evitar a conclusão da ameaça.
- Tudo começa com a **classificação dos ativos, passa pela identificação das ameaças, previsão das vulnerabilidades até chegar à análise de riscos.**
- Evite a criação de soluções próprias para lidar com a Segurança da Informação na empresa. Essas medidas foram muito pensadas e estudas e acabaram padronizadas por normas e procedimentos, como **ISO/IEC 17799**, incluída na série **ISO/IEC 27000** e reconhecida por empresas em qualquer parte do mundo.

SEGURANÇA É UM PROCESSO



CONSIDERAÇÕES FINAIS

- Na etapa inicial de um projeto de segurança, deve-se entender o ambiente da organização. Normalmente a situação é a seguinte:
  - Desconhecimento do ambiente/processos;
  - Baixo (ou nenhum) nível de controle implementado;
  - Alto índice de riscos;
  - Falta de uma cultura de segurança;
  - Resistência (interna e externa);

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.