



SSC531 - Sistemas de Informação

Segurança e Qualidade de Sistemas de Informação

Simone S. Souza

ICMC/USP

Segurança em Sistemas de Informação

- Por que os SIs estão tão *vulneráveis* a destruição, erros e uso indevido?
- Qual o valor empresarial da segurança nos SIs?
- Quais são as tecnologias e ferramentas disponíveis proteger a informação?



Desastre 11 de setembro de 2001

- Em SI, o que aprendemos com o 11 de setembro?



Desastre 11 de setembro de 2001

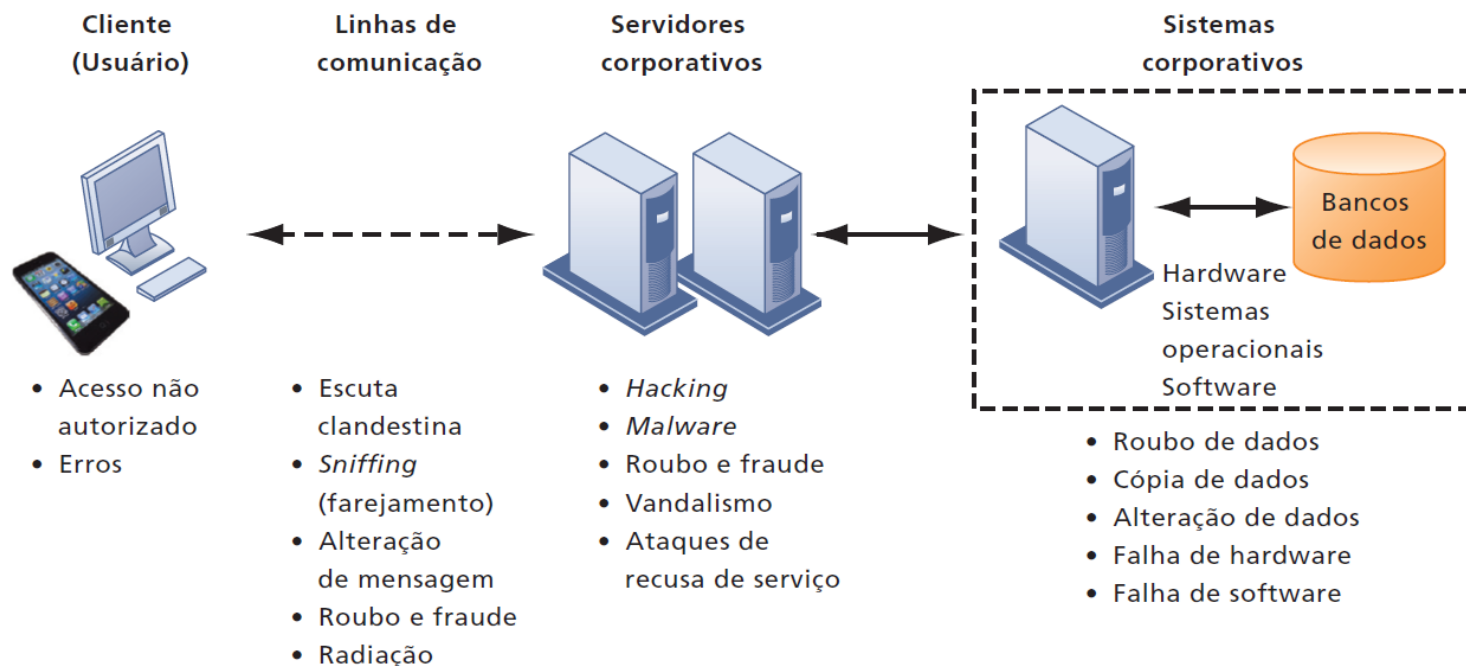
- Nem tudo está **sob controle**
- Empresas inteiras destruídas
- Gestores de Segurança mantinham backup dos DataCenter.
 - A maioria das empresas mantinha seus backups na Torre ao lado na qual trabalhava.
 - Ou seja, com a destruição das Torres, os backups que continham a vida da empresa, desapareceram.

Desastre 11 de setembro de 2001

- Empresas começaram a agir: E se fosse na minha empresa?
 - Investimento em sistemas de proteção de incêndio, cofre anti chamas
 - Planejamento para backup efetivo e eficiente: fitas backup enviadas para outras filiais, testes de recuperação de dados, contratos com fornecimento de Servidores e DataCenter backup;
 - ...

Vulnerabilidade e uso indevido

- Formato eletrônico X formato manual.
- Desafios contemporâneos:



Vulnerabilidade e uso indevido

- A Internet é culpada pela vulnerabilidade?
- É seguro se conectar a redes sem fio em aeroportos, bibliotecas ou outros locais públicos?
 - Estamos seguros?

Em 2000, a Amazon.com perdeu 224 mil dólares a cada hora que ficou sem serviço devido ao ataque de um hacker.



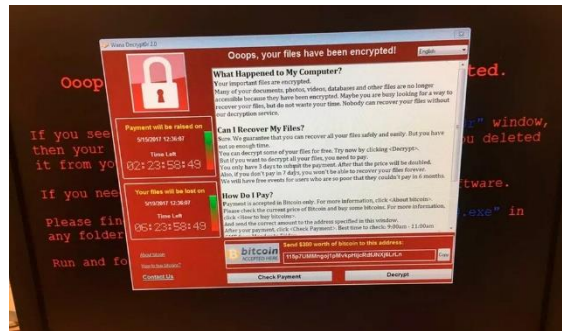
Vulnerabilidade e uso indevido

- Ameaças externas:
 - Software mal intencionado
 - Crimes de informática
- Ameaças internas
 - Funcionários (erros nas entradas dos sistemas)
 - Defeitos nos sistemas



Vulnerabilidade – Ameaça externa

- Matéria Folha São Paulo*: Ataque cibernético atingiu mais de 300 mil computadores no mundo (Maio/2017)
 - Ransomware – computadores infectados com vírus que “sequestra” arquivos. Invasores pedem um resgate ou ameaçam destruir ou compartilhar arquivos
 - Microsoft havia criado proteção mas nem todos usuários haviam atualizado o sistema e o Ransomware se aproveitou desta vulnerabilidade



* <http://www1.folha.uol.com.br/mundo/2017/05/1883484-o-que-se-sabe-ate-agora-do-mega-ataque-cibernetico-em-todo-o-mundo.shtml>

Ameaça interna: Bugs no sistema

- Bugs sempre estão presentes no software
- Correções sucessivas “deterioram” o software
- Qualidade comprometida

How people reacts differently to a single word.

"Bug"



Tester



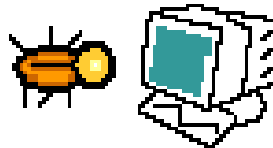
Developer



Manager

Falhas de Software mais famosas da História*

** A Collection of Well-Known Software Failures -*
<http://www.cse.psu.edu/~gxt29/bug/softwarebug.html>



Ariane 5 vôo 501 - 1996

- Levou uma década de desenvolvimento e custou 7 bilhões de dólares.
- Foguete com código reutilizado do Ariane 4 (outro hardware);
- **Overflow de inteiro: conversão de float de 64-bits para inteiro 16-bits com sinal;**
- O processador primário do foguete sobrecarrega os motores que se desintegraram em 40 segundos;
- Não tripulado (sem vítimas); prejuízo de US\$ 370 milhões



Mars Pathfinder Mission



- Robô da NASA para explorar Marte (1997)
- **Problema:** Depois de pousar com sucesso tinha a missão de enviar dados sobre Marte para a Terra. Depois de alguns dias começou a reiniciar intermitentemente e parou de enviar os dados
- **Causa:** erro no módulo de comunicação entre processos: 3 processos em execução com diferentes prioridades (H, M, L): processo M começou a executar por longo tempo e processo H ficou esperando processo L finalizar. Porém processo L não conseguiu acesso à CPU porque M estava executando! Devido ao tempo sem evoluir, o dispositivo reiniciava o sistema, que voltava a mesma situação, devido ao bug.



Máquina de radiação Therac-25

- Evolução de modelos anteriores, a Therac-25 tinha os controles de segurança no software (1985)
- **Problema:** Devido à falha em mostrar o valor de radiação atribuído, pacientes receberam doses letais de radiação (3 mortes e 3 gravemente feridos)
- **Causa:** Problema conhecido como “condição de disputa”. O técnico tinha a impressão que o valor configurado estava correto, mas, devido ao bug, o valor era diferente do definido, aumentando os valores de radiação.

Aeroporto de Düsseldorf – Alemanha 2016

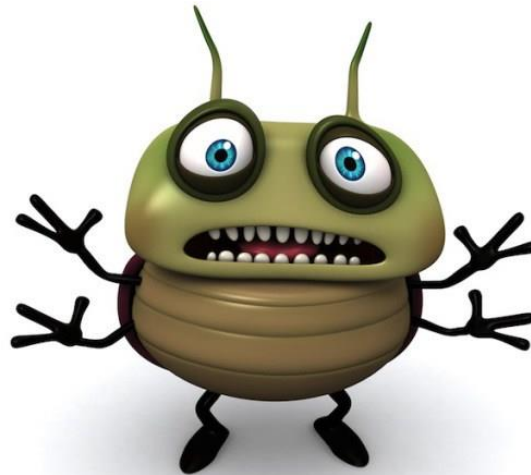
- **Malas retidas - ano bissexto – 2016**
 - Sistema de transporte de bagagem (2015) custou 70 milhões de euros não reconheceu o 29 de fevereiro.
 - Esteiras pararam – despacho manual de bagagens
 - transportadas entre 25 mil e 50 mil malas por dia!.
 - 1.200 malas acabaram não sendo despachadas

“A empresa responsável pelo software fez a reprogramação necessária, incluindo o dia 29 de fevereiro de 2016 no sistema. Daqui a quatro anos, este procedimento será novamente necessário, afirmou o porta-voz”



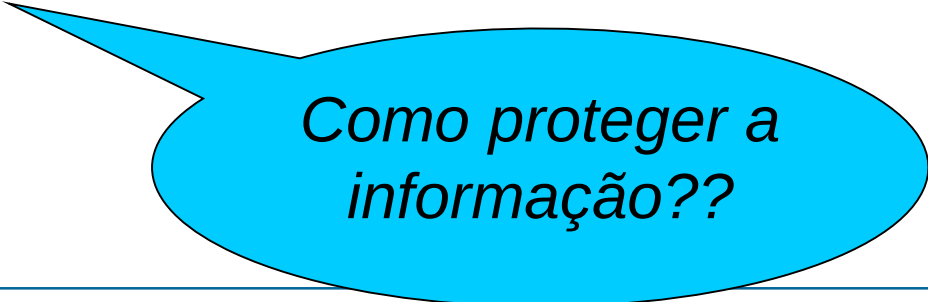
**Por que essas falhas ainda
ocorrem?**

**Podemos evitar essas falhas de
software?**



Vulnerabilidade

- INFORMAÇÃO é um ATIVO importante para todas as organizações
- Importante:
 - Armazenar e gerenciar informação.
 - Compartilhar informação.
 - **Proteger** a informação.

A light blue speech bubble with a black outline, pointing towards the 'Proteger' bullet point. It contains the text 'Como proteger a informação??' in a black, italicized font.

*Como proteger a
informação??*

Valor empresarial da segurança e controle

- Sistemas abrigam informações confidenciais
 - Impostos, ativos financeiros, registros médicos e desempenho profissional das pessoas.
- Controle e segurança inadequados podem criar sérios riscos legais.
- As empresas precisam proteger não apenas seus próprios ativos de informação, mas também os de clientes, funcionários e parceiros de negócios.
- Caso não consigam fazê-lo, podem ter de gastar muito em um litígio por exposição ou roubo de dados.

Prova eletrônica e perícia forense computacional

- Ação legal - pedido de produção de provas
 - Obrigação de fornecer acesso às informações que podem ser usadas como prova.

- **Perícia forense computacional** - procedimento científico de coleta, exame, autenticação, preservação e análise de dados mantidos em meios de armazenamento digital
 - Informações possam ser usadas como prova em juízo.
 - Desafios:
 - Recuperar dados sem prejudicar seu valor probatório;
 - Armazenar e administrar dados eletrônicos recuperados;
 - Encontrar informações em um grande volume de dados;
 - Apresentar as informações em juízo.

Como estabelecer uma estrutura para segurança e controle

- **Controles gerais** controlam projeto, segurança e uso de programas de computadores, além da segurança de arquivos de dados.
- **Controles de aplicação** são controles específicos exclusivos a cada aplicação computadorizada, como processamento de pedidos.
- Uma **avaliação de risco** determina o nível de risco para a empresa caso uma atividade ou um processo específico não sejam controlados adequadamente.
- **Política de segurança** é uma declaração que estabelece hierarquia aos riscos de informação e identifica metas de segurança aceitáveis, assim como os mecanismos para atingi-las.

Como estabelecer uma estrutura para segurança e controle

Tabela 8.5

Avaliação do risco no processamento de pedidos on-line.

Exposição	Probabilidade de ocorrência (%)	Faixa de prejuízo/média (US\$)	Prejuízo anual esperado (US\$)
Falta de energia	30%	5.000–200.000 (102.500)	30.750
Apropriação indébita	5%	1.000–50.000 (25.500)	1.275
Erro de usuário	98%	200–40.000 (20.100)	19.698

Plano de recuperação de desastres e plano de continuidade dos negócios

- O **plano de recuperação de desastres** inclui estratégias para restaurar os serviços de computação e comunicação após eles terem sofrido uma interrupção.
- O **plano de continuidade dos negócios** concentra-se em como a empresa pode restaurar suas operações após um desastre.
- Como a administração sabe que os controles e a segurança de seus sistemas de informação são eficientes?
- Uma **auditoria de sistemas de informação** avalia o sistema geral de segurança da empresa e identifica todos os controles que governam sistemas individuais de informação.

Tecnologias e ferramentas para garantir a segurança em SI

- **Gestão de identidade**
 - Autenticação
 - Autenticação biométrica
- **Firewall**
- **Sistemas de detecção de intrusão**
- **Software antivírus**
- **Criptografia**
- **Certificados digitais**

Garantia de Qualidade do Software

- Como melhorar a qualidade e a confiabilidade dos sistemas?
 - Métricas de qualidade
 - Teste de software

Controles Gerais - Norma de Segurança

- **NBR ISO/IEC 17799** – norma de segurança (2001)
 - Cobre os mais diversos tópicos da área de segurança, possuindo um grande número de controles e requerimentos que devem ser atendidos para garantir a segurança das informações de uma empresa.
 - A obtenção da certificação pode ser um processo demorado e muito trabalhoso.
- A certificação é uma forma clara de mostrar a sociedade que a empresa dá a segurança de suas informações e de seus clientes a importância que merecem.

Controles Gerais - Norma de Segurança

- Definir:

- **O que** proteger?
- Contra **o que/quem** proteger?
- **Como** reagir?
- **Quem** faz o quê?

Conclusões

- A administração deve ser responsável pelo desenvolvimento de uma estrutura de controle e dos padrões de qualidade desejados.
- Não existem sistemas 100% seguros.
 - Importante planejar e realizar ações preventivas.

Conclusões

- Principais ameaças: vírus, invasões, funcionários insatisfeitos e senhas.
- Aumento do uso da Internet como meio de fraudes e vazamento de informação.
- Necessidade de conscientizar os executivos, motivar os usuários e capacitar a equipe técnica.
- Necessidade de realizar análise de riscos e revisar periodicamente a política de segurança.