

Segurança e Controle em Sistemas de Informação

Profa. Ellen Francine
ICMC-USP

11/09: nem tudo está “sob controle”

- Com o ataque contra o World Trade Center e Pentágono, todo transporte aéreo e terrestre foi interrompido por dias.
 - Rupturas na cadeia de suprimentos por todo EUA.
 - Empresas que trabalhavam com **estoque enxuto** sofreram o impacto.
 - Ford, Chrysler, GM...
 - As empresas e os seus sistemas não estavam preparados para trabalhar nessas circunstâncias.
-

Introdução

- Sistemas de informação são vulneráveis a **destruição, erro, uso indevido e problemas de qualidade.**
 - Controles adequados devem ser utilizados.
 - Medidas devem ser tomadas para assegurar a confiabilidade, a disponibilidade e a segurança dos processos empresariais.
 - Uso de técnicas para garantir a qualidade de um software.
-

Desafios para a Segurança em SI

- SI desempenham **papel crítico** para as empresas, governo e vida diária.
 - Projetar sistemas que não sejam nem supercontrolados nem subcontrolados.
 - Aplicar padrões de garantia de qualidade a grandes projetos de sistemas.
-

Vulnerabilidade

- Os SIs concentram dados que podem ser acessados facilmente por grande número de pessoas e por grupos externos à organização.
 - Mais suscetíveis à destruição, fraude, erro e uso indevido.
-

Vulnerabilidade

- Avanço nas telecomunicações permitiu a interconexão de SIs.
 - Internet → gerou grande quantidade de informação, facilitando sua disseminação e acesso.
 - **Milhões de pessoas** conectadas.



Vulnerabilidade

- Ameaças aos SIs
 - Falha de hardware ou de software
 - Ações pessoais
 - Invasão
 - Roubo de dados e equipamentos
 - Incêndio e problemas elétricos
 - Erros de usuários
 - Problemas de telecomunicações
 - Vírus
 - ...
-

Vulnerabilidade

- Preocupações principais de desenvolvedores e usuários de SIs:
 - **Desastre**
 - Destrói hardware de computador, programas, arquivos de dados e outros equipamentos.
 - **Segurança**
 - Evitar acesso não-autorizado, alterações, roubo ou danos físicos.
-

Vulnerabilidade

- Preocupações principais de desenvolvedores e usuários de SIs:
 - **Bugs**
 - Defeitos ou erros no código do programa.
 - Fazem com que os computadores danifiquem ou destruam os registros e operações e da organização.
-

Vulnerabilidade

- Preocupações principais de desenvolvedores e usuários de SIs:
 - **Manutenção**
 - Altos custos devido à mudança organizacional, à complexidade do software e a falhas na análise e no projeto de sistema.
 - **Má qualidade dos dados**
 - Dados imprecisos ou inconsistentes com outras fontes de podem criar sérios problemas operacionais e financeiros.
-

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 and a tail pointing towards the top left. It contains the text 'Como proteger a informação??' in a black, italicized font.

*Como proteger a
informação??*

Criação de um ambiente de controle

- Criação de um **ambiente de controle**.
 - Definição de métodos, políticas e procedimentos organizacionais.
 - Garantem a **segurança dos ativos** da empresa.
 - Garantem a **precisão e confiabilidade** dos registros e **adesão operacional** aos padrões administrativos.
-

Criação de um ambiente de controle

- **Controles gerais**
 - Relacionados ao projeto, à segurança e à utilização dos programas e infraestrutura de TI.
 - Ambiente global de controle.

 - **Controles de aplicação**
 - Controles específicos de cada aplicação.
-

Controles Gerais

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

Controles Gerais

- A maioria é projetada e mantida por especialistas em SI, mas **requer supervisão de usuários finais e gerentes.**
 - Controles de software (quem pode utilizar).
 - Controles de hardware, de operações de computador, segurança de dados, de implementação, administrativos ...
 - Procedimentos manuais.
-

Controles Gerais - Exemplo (Perfis)

PERFIL DE SEGURANÇA 1

Usuário: funcionário do departamento pessoal

Localização: Divisão I

Códigos de identificação de funcionários com esse perfil:

00753, 27834, 37665, 44116

Restrições ao campo de dados

Tipo de acesso

Todos os dados de funcionários para Divisão I somente

Leitura e atualização

- Dados de histórico médico
- Salário
- Rendimentos para pensão

Nenhum
Nenhum
Nenhum

PERFIL DE SEGURANÇA 2

Usuário: gerente da divisão de pessoal

Localização: Divisão I

Códigos de identificação de funcionários com esse perfil: 27321

Restrições ao campo de dados

Tipo de acesso

Todos os dados de funcionários para a Divisão I somente

Somente leitura

Controles Gerais

- A política de segurança deve atingir todos os níveis da organização.
 - Conscientização.
 - Pode ser:
 - **Permissiva**: tudo que não é expressamente proibido é permitido.
 - **Proibitiva**: tudo que não é expressamente permitido é proibido.
-

Controles de Aplicação

- Incluem procedimentos automatizados (ou manuais) para assegurar que somente dados autorizados sejam processados pela aplicação.
 - Controles de entrada
 - Controles de processamento
 - Controles de saída
-

Controles de Aplicação

- **Controles de entrada**
 - Verificam a precisão e integridade dos dados que entram no sistema (controles de entrada, tratamento de erros, etc).
 - **Controles de processamento**
 - Determinam se os dados estão completos e precisos durante a atualização.
 - **Controles de saída**
 - Garantem que os resultados do processamento sejam precisos, completos e corretamente distribuídos.
-

Criação de um ambiente de controle

- Elementos para proteção da empresa:
 - **Computação de alta disponibilidade**
 - Ferramentas e tecnologia que ajuda a empresa a se recuperar após um desastre.
 - **Tolerância a falhas**
 - Promete disponibilidade contínua e eliminação total da necessidade de se recuperar.
 - **Plano de recuperação pós-desastre**
 - Gerencia os negócios no caso da falha de um computador.
-

Criação de um ambiente de controle

- Elementos para proteção da empresa:
 - **Distribuição de carga**
 - Distribui um grande número de requisições de acesso para vários servidores.
 - **Duplicação**
 - Duplicação de todos os processos e transações de um servidor em um servidor de backup, para evitar interrupções.
-

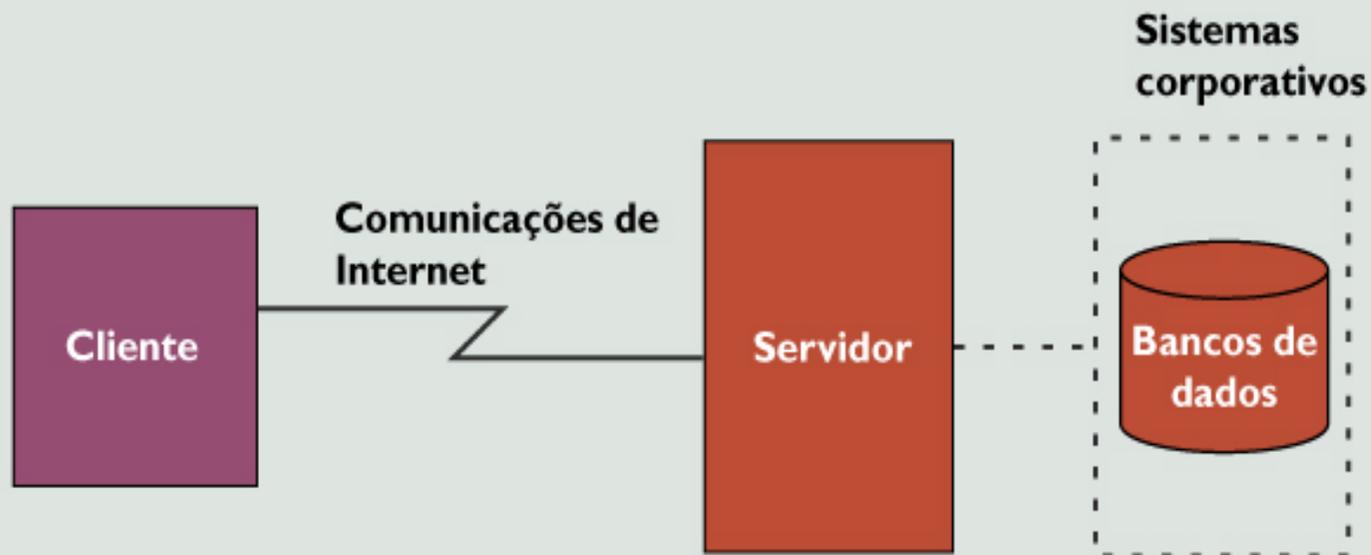
Desafios de Segurança na Internet

- O comércio eletrônico requer que as empresas sejam **mais abertas** e **mais fechadas**.
 - Estar aberta a estranhos (clientes, fornecedores e parceiros) para o gerenciamento da cadeia de suprimentos e outros processos.
 - Estar aberta a funcionários (por exemplo, quando trabalham com dispositivos móveis).
-

Desafios de Segurança na Internet

- O comércio eletrônico requer que as empresas sejam **mais abertas** e **mais fechadas**.
 - Estar fechada, protegida de ataques.
 - **Requer uma nova "cultura de segurança"**.
 - É essencial que os dados de compradores e vendedores mantenham-se privados quando transmitidos eletronicamente.
-

Desafios de Segurança na Internet



- Vírus de computador
- Grampos de linha
- Perda de máquina

- Grampeamento
- Sniffing
- Alteração de mensagem
- Roubo e fraude

- Ação de hackers
- Vírus de computador
- Roubo e fraude
- Grampos de linha
- Vandalismo
- Ataques de recusa de serviço

- Roubo de dados
- Cópia de dados
- Alteração de dados

Desafios de Segurança na Internet

- Antivírus
 - Autenticação biométrica
 - Criptografia
 - Certificado digital
 - Transação eletrônica segura
 - ...
-

Qual o grau de controle necessário?

- Desenvolvimento de uma estrutura de controle: **custo X benefícios**
 - Critérios para determinar o grau de controle necessário:
 - Importância dos dados
 - Eficiência, complexidade e custos de cada técnica de controle
 - Nível de risco – avaliação para determinar pontos de vulnerabilidade, frequência provável e o prejuízo potencial
-

Auditoria no Processo de Controle

- Como saber se os controles dos SIs são eficientes?
 - Uma **auditoria de sistemas** identifica todos os controles utilizados pelos sistemas de informação individuais e avalia sua eficácia.
 - Rever tecnologias, procedimentos, documentação, treinamento e recursos humanos.
 - Listagem de todos os pontos fracos do controle e estimativa da probabilidade de ocorrerem erros nesses pontos.
-

Auditoria no Processo de Controle

- Como saber se os controles dos SIs são eficientes?
 - Auditoria da **qualidade dos dados**.
 - Identificar informações imprecisas, incompletas, ambíguas e redundantes.
-

Conclusões

- A empresa é 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.

NÃO agir sob-demanda → Realizar ações **pró-ativas**

Segurança e Controle em Sistemas de Informação

