Sistema de Informação

Prof. Me. Sérgio Carlos Portari Júnior
Portari.uemgituiutaba@gmail.com

Segurança em Sistemas de Informação

OBJETIVOS DE ESTUDO

- **Analisar por que sistemas de informação precisam de proteção especial contra destruição, erros e uso indevido**
- **Avaliar o valor empresarial da segurança e do controle**
- **Discutir a base da estrutura organizacional para segurança e controle de informação**
- **Avaliar as mais importantes tecnologias e ferramentas disponíveis para salvaguardar recursos de informação**

5 PILARES DA SEGURANÇA DA INFORMAÇÃO

1. Confidencialidade: oferecer suporte a prevenção de revelação não autorizada da informação.
2. Integridade: prevenir a modificação não autorizada da informação.
3. Disponibilidade: prover acesso confiável a qualquer momento à informação.
4. Não repúdio: assegura que nem o emissor nem o receptor de uma informação possam negar o fato
5. Autenticidade: assegurar a integridade de origem da informação compreendendo o que denominamos de responsabilidade final.

5 PILARES DA SEGURANÇA DA INFORMAÇÃO

Os pilares refletem na organização e envolvem 3 aspectos principais:

- Pessoas – Usuários bem orientados, treinados e conscientizados.
- Processos – Regras claras para utilização dos recursos tecnológicos fornecidos pela empresa e leis que em caso de desvio de informações punam severamente o infrator.
- Tecnologia – Sistemas bem implementados para assegurar e proteger as informações da empresa

Vulnerabilidade dos Sistemas e Uso Indevido

- Um computador desprotegido conectado à Internet pode ser danificado em poucos segundos
- **Segurança:** políticas, procedimentos e medidas técnicas usados para impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação
- **Controles:** métodos, políticas e procedimentos organizacionais que garantem a segurança dos ativos da organização, a precisão e a confiabilidade de seus registros contábeis e a adesão operacional aos padrões administrativos.

BENEFÍCIOS DE UM SISTEMA DE SEGURANÇA

- **Os benefícios evidentes são reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer estes princípios básicos.**

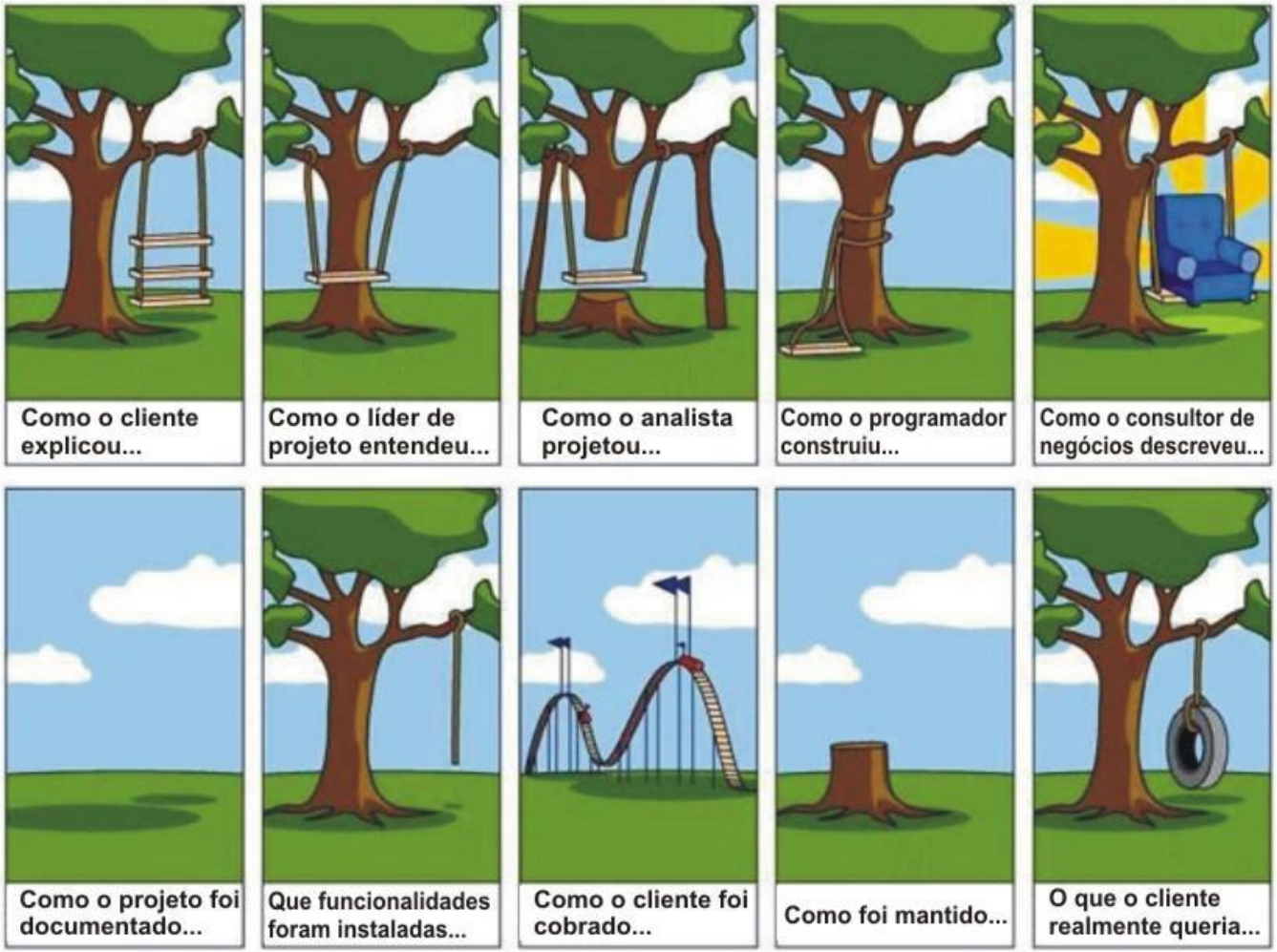
- **A segurança visa também aumentar a produtividade dos usuários através de um ambiente mais organizado, maior controle sobre os recursos de informática e finalmente, viabilizar aplicações críticas das empresas.**

- **Alguns exemplos de aplicações bem sucedidas na Internet:**
  - Internet Banking: Bradesco, Itaú, BB, CEF, etc.
  - Eleições no Brasil, desde 1994
  - Projeto Receita Net, que alcançou a expressiva quantidade de quase 500.000 contribuintes que entregaram a declaração de renda via Internet.

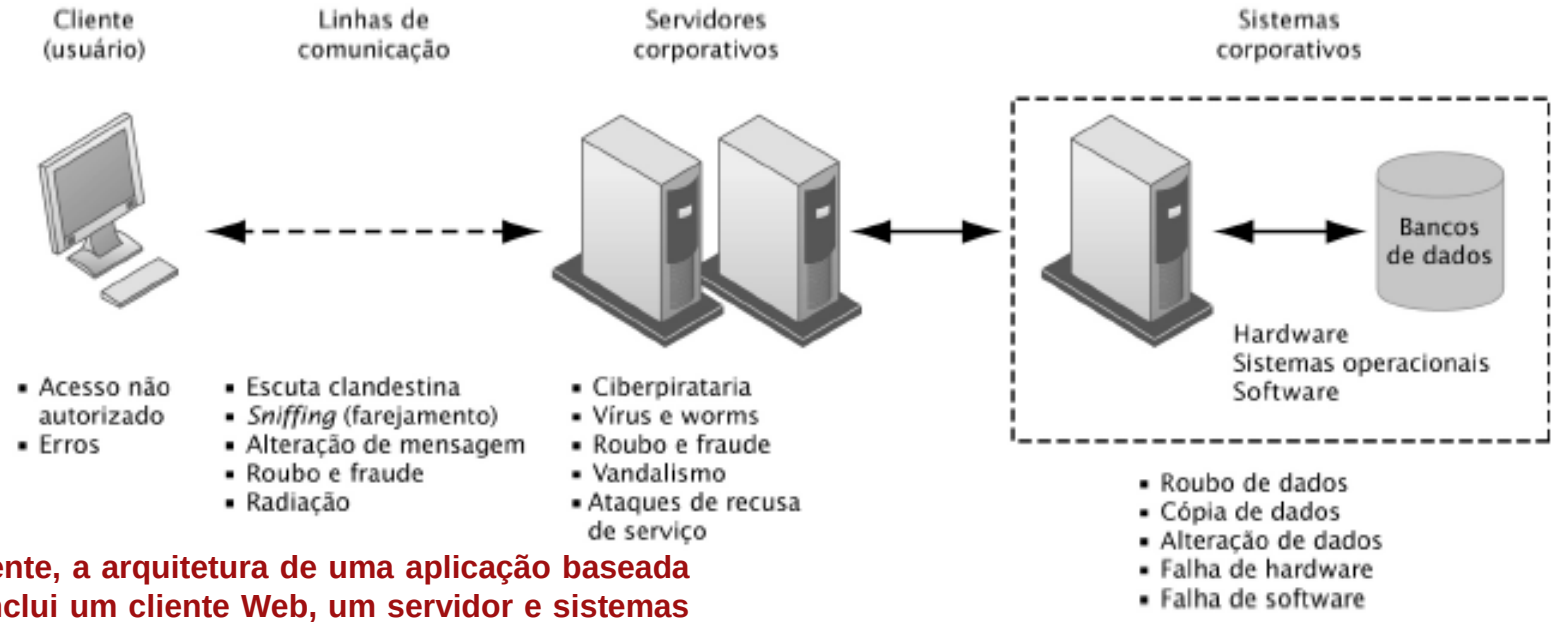
Por que os Sistemas são Vulneráveis

- Problemas de hardware (quebras, erros de configuração, danos por uso impróprio ou crime)
- Problemas de software (erros de programação, erros de instalação, mudanças não autorizadas)
- Desastres (quedas de energia, enchentes, incêndios etc.)
- Vulnerabilidades da Internet
- Desafios da segurança sem fio

Por que os Sistemas são Vulneráveis



Vulnerabilidades e Desafios de Segurança Contemporâneos



Normalmente, a arquitetura de uma aplicação baseada na Web inclui um cliente Web, um servidor e sistemas de informação corporativos conectados a bancos de dados. Cada um desses componentes apresenta vulnerabilidades e desafios de segurança.
Enchentes, incêndios, quedas de energia e outros problemas técnicos podem causar interrupções em qualquer ponto da rede.

Figura 7.1

Software Mal-intencionado: Vírus, Worms, Cavalos de Tróia e Spyware

- Malware
  - Vírus
  - Worms
  - Cavalos de Tróia
  - Spyware
  - Key loggers

Software Mal-intencionado

- **Malware:** **do inglês malicious software - Software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações.**
  - **Vírus –** programa desenvolvido para alterar a forma como um computador opera, sem a permissão ou o conhecimento do seu usuário.

  Um vírus precisa atender a dois critérios:

  1) deverá executar a si próprio, freqüentemente inserindo alguma versão do seu próprio código no caminho de execução de outro programa.

  2) ele deve se disseminar.

  - pode se copiar em outros arquivos executáveis ou em discos que o usuário acessa.
  - podem invadir tanto computadores desktop como servidores de rede.

TIPOS DE VÍRUS

- **Vírus de programa:** têm extensões como .COM, .EXE, .OVL, .DLL, .DVR, .SYS, .BIN e, até mesmo, .BAT. Exemplos de vírus de programa conhecidos são Jerusalem e Cascade.

- **Vírus de setor de boot:** infectam a área do sistema de um disco - ou seja, o registro de inicialização em disquetes e discos rígidos.

- **Vírus de macro:** infectam os arquivos dos programas Microsoft Office Word, Excel, PowerPoint e Access.
  - Variações mais recentes também estão aparecendo em outros programas. Usam a linguagem de programação interna do programa, que foi criada para permitir que os usuários automatizem determinadas tarefas neste programa. Devido à facilidade com que estes vírus podem ser criados, existem milhares deles espalhados.

Worms

- cria cópias de si mesmo automaticamente de um computador para outro
- 1º) controla recursos no computador que permitem o transporte de arquivos ou informações.
- 2º) depois que o worm contamina o sistema, ele se desloca sozinho.
- O grande perigo dos worms é a sua capacidade de se replicar em grande volume.
- Ex: um worm pode enviar cópias de si mesmo a todas as pessoas que constam no seu catálogo de endereços de email, e os computadores dessas pessoas passam a fazer o mesmo, causando um **efeito dominó** de alto tráfego de rede que pode tornar mais lentas as redes corporativas e a Internet como um todo.
- Quando novos worms são lançados, eles se alastram muito rapidamente.
- Eles obstruem redes e provavelmente fazem com que você (e todos os outros) tenha de esperar um tempo maior para abrir páginas na Internet.

Cavalos de Tróia

- Programas que parecem ser úteis, mas na verdade comprometem a sua segurança e causam muitos danos.
- Um cavalo de Tróia recente apresentava-se como um e-mail com anexos de supostas atualizações de segurança da Microsoft, mas na verdade era um vírus que tentava desativar programas antivírus e firewalls.
- Se alastram quando as pessoas são seduzidas a abrir o programa por pensar que vem de uma fonte legítima.
- Para proteger melhor os usuários, a Microsoft envia com freqüência boletins de segurança via email, mas eles nunca contêm anexos.

Vulnerabilidade dos Sistemas e Uso Indevido

- **Spyware**

- **Programa recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite a uma entidade externa na Internet, sem o seu conhecimento nem o seu consentimento.**
- **Podem ser desenvolvidos por firmas comerciais, que desejam monitorar o hábito dos usuários para avaliar seus costumes e vender este dados pela internet. Assim estas firmas costumam produzir inúmeras variantes de seus programas-espiões, aperfeiçoando-o, dificultando em muito a sua remoção.**
- **Muitos vírus transportam spywares, que visam roubar certos dados confidenciais dos usuários. Roubam dados bancários, montam e enviam registros das atividades do usuário, roubam determinados arquivos ou outros documentos pessoais.**
- **Costumam vir legalmente embutidos em algum programa shareware ou freeware. Sua remoção é feita quando da compra do software ou de uma versão mais completa e paga.**

- **Key loggers - registradores de teclas**

Sessão Interativa: Software Mal-intencionado

- **Visite o site do :** www.pandasoftware.com
  - **Quais são os principais vírus em termos de taxa de infecção?**
  - **Quais são as ameaças de vírus mais recentes?**
  - **Leia descrições dos principais vírus e das ameaças mais recentes**
  - **O que os downloads do Panda Software oferecem para ajudar os usuários a proteger e a reparar seus computadores?**
  - **Compare e contraste o conteúdo disponível no site do Panda Software com as ofertas do site da Symantec em http://www.symantec.com/pt/br**

DEFINIÇÕES

- **Hackers *versus* crackers**
  - Hackers: elaboram e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas.
  - Crakers: invasores de computadores, programadores maliciosos e ciberpiratas que agem com o intuito de violar ilegal ou imoralmente sistemas cibernéticos
- **Cibervandalismo**
  - Busca obter privilégios de acesso a um sistema computacional.

DEFINIÇÕES

- **Denial of Service (DoS)**
  - Uma forma de ataque que consiste no envio de informação até que a rede entre em saturação (Ataque de recusa de serviço)
  - A recusa de serviços ocorre quando alguém é privado de realizar uma tarefa ou operação desejada.
  - Maneiras comuns que hackers utilizam para causar ataques DoS:

    1. Consumo da largura de banda – a inundação de dados em uma rede
    2. Privação de recursos – esvaziamento dos recursos de um sistema
    3. Falhas na programação – exploração da lotação do buffer
    4. Roteamento e ataques DNS – manipulação de tabelas DNS para que apontem para endereços IP alternativos

DNS: *D*omain *N*ame *S*ystem - Servidor de Nomes de Domínios) é um sistema de gerenciamento de nomes Hierárquico e distribuído

DEFINIÇÕES

- **Ataque Distribuído de Recusa de Serviço (DDoS)**
  - Em um ataque DDoS, vários computadores são atacados e instruídos para inundar um site determinado com pacotes ou solicitações de dados, recusando o serviço a usuários legítimos do sistema vítima.
  - O grau de automatização em ferramentas de ataque permite que um único atacante instale suas ferramentas e controle milhares de sistemas comprometidos para utilizá-los em seus ataques.

DEFINIÇÕES

- **Botnets (‘redes de robôs’)**
  - uma coleção de softwares robôs, ou bots (diminutivo de robots) que são executados automaticamente e de forma autônoma.
  - O termo é freqüentemente associado com software malicioso, mas ele também pode referir-se à rede de computadores usando computação distribuída software.
  - Embora o termo "botnet" pode ser usado para se referir a qualquer grupo de bots, como o IRC bots, esta palavra é geralmente usada para referir-se a uma coleção de computadores infectados (computadores zumbis) executando o software, geralmente instalados através worms ou cavalos de Tróia, sob um comando e de controle das infra-estruturas.

DEFINIÇÕES

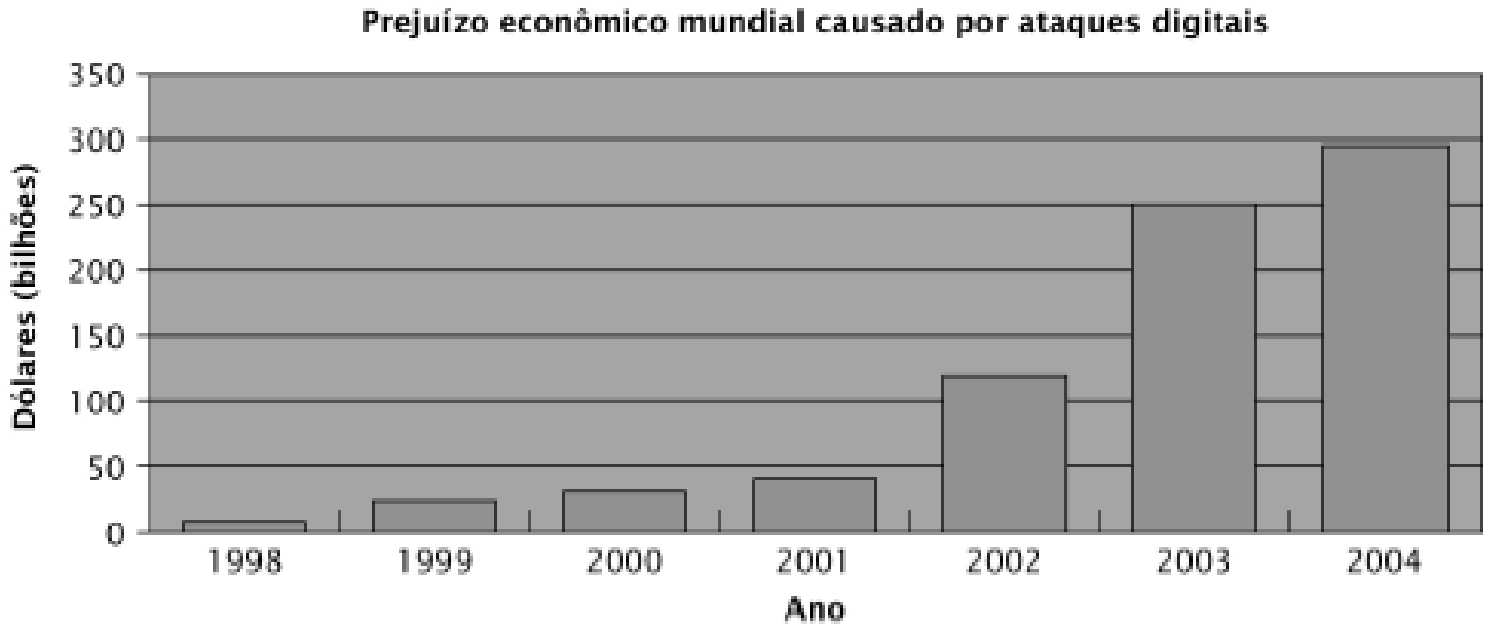
- **Spoofing:** associado ao se fazer passar por algo diferente (phishing), através de redirecionamento e utilização de falsas identidades.
- **Sniffing:** um software que analisa o tráfego na Internet.

Crimes de Informática e Ciberterrorismo

- Crime de informática: 'Quaisquer violações da legislação criminal que envolvam um conhecimento de tecnologia da informática em sua perpetração, investigação ou instauração de processo' – Departamento de Justiça dos Estados Unidos
- As empresas dos EUA perdem 14 bilhões de dólares por ano para o cibercrime.
- Roubo de identidade
- Ciberterrorismo e guerra cibernética

Vulnerabilidade dos Sistemas e Uso Indevido

Prejuízo Mundial Causado por Ataques Digitais



Este gráfico mostra a média anual estimada dos prejuízos causados por hacker, malware e spam no âmbito mundial, desde 1998. Os números baseiam-se em dados do mi2G e dos autores.

Figura 7.3

- A segurança das organizações deve ser entendida a vários níveis, em termos de segurança informática e de segurança da informação.
- Apesar dos conceitos se interligarem mutuamente, e de alguma forma poderem ser confundidos, existe uma diferença fundamental:
  - enquanto a segurança informática pretende proteger sistemas informáticos (aplicações, base de dados, sistemas operativos),
  - a segurança da informação pretende proteger a informação crítica de negócio nos seus vários suportes (documentos em papel, base de dados, pessoas, etc.).

Componentes principais de um sistema de gestão da segurança da informação (SGSI)

Confidencialidade	• Assegurar que a informação é acessível somente por aqueles devidamente autorizados
Integridade	• Salvaguardar a veracidade e complementariedade da informação bem como os seus métodos de processamento
Disponibilidade	• Assegurar que quem devidamente autorizado tem acesso á informação e bens associados sempre que necessário

NORMAS DE SEGURANÇA

ISO/IEC 27001

- Estabelece uma forma de lidar com a informação, consolidando um conjunto das melhores práticas da gestão de segurança da informação.
- Certifica as organizações em termos de gestão de segurança da informação.
- A certificação demonstra que estas organizações possuem um sistema de gestão que protege a sua informação com mecanismos de controle adequados às suas necessidades e realidade, verificados por uma entidade externa.
- Através da avaliação e gestão do risco este sistema procura garantir a continuidade de negócio e diminuir o impacto de eventuais incidentes de segurança.

ISO/IEC 27001

Ao ser certificada em termos de Gestão da Segurança da Informação a organização obtém principalmente os seguintes benefícios:

- Credibilidade comercial;
- Redução de custos de incidentes;
- Cumprimento de leis e regulamentos;
- Redução do risco de incidentes de segurança.

Ameaças Internas: Funcionários

- Ameaças à segurança freqüentemente se originam dentro da empresa
- Engenharia social

Vulnerabilidades do Software

- Softwares comerciais contêm falhas que criam vulnerabilidades de segurança
- *Patches* (remendos)

Valor Empresarial da Segurança e do Controle

- O não funcionamento dos sistemas de computador pode levar a perdas significativas ou totais das funções empresariais
- As empresas estão agora mais vulneráveis do que nunca
- Uma brecha de segurança pode reduzir o valor de mercado de uma empresa quase imediatamente
- Segurança e controles inadequados também produzem problemas de confiabilidade

Requisitos Legais e Regulatórios para o Gerenciamento de Registros Eletrônicos

- **Gerenciamento de registros eletrônicos (electronic records management — ERM): políticas, procedimentos e ferramentas para gerenciar a retenção, a distribuição e o armazenamento de registros eletrônicos.**
- **HIPAA**
- **Lei Gramm-Leach-Bliley**
- **Lei Sarbanes-Oxley**

Valor Empresarial da Segurança e do Controle

Legislação e conformidade

- As empresas de serviços financeiros devem utilizar as tecnologias de segurança e os produtos de gerenciamento de proteção de conteúdo que lhes auxiliem a conquistar e manter o cumprimento das atuais leis.

- Empresas de serviços financeiros, como bancos de investimentos, bancos comerciais e de varejo, seguradoras, ou até mesmo empresas que prestam serviços de hospedagem para o setor de serviços financeiros, devem cumprir essas leis.

- Cada lei trata de uma questão diferente, tendo seus próprios requisitos básicos de conformidade; entretanto, as leis não dizem explicitamente às organizações de serviços financeiros o que devem fazer para cumpri-las.

Valor Empresarial da Segurança e do Controle

- **HIPAA - Health Insurance Portability and Accountability Act**
  - Determina que todas as organizações de saúde devem efetivamente atender aos requisitos de segurança Administrativa, Técnica e Física para proteger a privacidade das informações dos pacientes, e manter a integridade dos dados para funcionários, cliente e acionistas.
  - Certificação de conformidade HIPAA
  - Soluções de vários provedores, como IBM

Valor Empresarial da Segurança e do Controle

- **Lei Gramm-Leach-Bliley**
  - promulgada em 1999, define o que as empresas de serviços financeiros podem fazer com as informações pessoais confidenciais que coletam durante suas atividades de consultoria de investimentos.
  - trata da confidencialidade, pois as empresas devem garantir que haja uma separação entre as áreas de M&A (Fusões e Aquisições) e corretagem, por exemplo.

Valor Empresarial da Segurança e do Controle

- **Lei Sarbanes-Oxley**
  - trata da integridade, garantindo que os relatórios financeiros sejam completos e precisos ou pelo menos garantindo a precisão dos controles que os geram.
  - aprovada pelo Congresso dos Estados Unidos em 2002, responsabiliza pessoalmente os CEOs (Chief Executive Officers) e CFOs (Chief Financial Officers) pela precisão dos seus relatórios financeiros.

Prova Eletrônica e Perícia Forense Computacional

- Grande parte das provas para ações legais são encontradas hoje em formato digital
- O controle adequado de dados pode economizar dinheiro quando for necessário apresentar informações
- Perícia forense computacional: procedimento científico de coleta, exame, autenticação, preservação e análise de dados mantidos em — ou recuperados por — meios de armazenamento digital, de tal maneira que as informações possam ser usadas como prova em juízo.

Legislação sobre Crimes Eletrônicos

A Lei sobre Fraude e Abuso de Computadores dos Estados Unidos de 1986 define o crime informatizado como uma das atividades envolvendo acesso a computadores de interesse federal ou operando no comércio interestadual ou exterior:

- Com o intuito de fraudar;
- Para obter acesso a certos sistemas de computação médica;
- Para traficar senhas de acesso a computadores.

Legislação sobre Crimes Eletrônicos

A Associação dos Profissionais de Tecnologia da Informação define o crime informatizado como:

- O uso, acesso, modificação e destruição não autorizadas de recursos de hardware, software, dados ou rede.
- A divulgação não autorizada de informações;
- A cópia não autorizada de softwares;
- A negação de acesso a um usuário
- final aos seus próprios recursos de hardware, software, dados ou rede; O uso ou conspiração para uso de recursos de computação para obter ilegalmente informações ou propriedade tangível.

Legislação sobre Crimes Eletrônicos

Lei de Crimes Eletrônicos / Brasil

- Aprovação da alteração do Estatuto da Criança e do Adolescente (PL 3773/08),
- tramitação final do Projeto de Lei de Crimes Eletrônicos (PLC 89/03)

Lei de Crimes Eletrônicos / Brasil

- Muitas instituições estão revendo suas políticas internas de uso de ferramentas de trabalho tecnológicas, para passar a proibir a guarda de conteúdo pessoal (em geral feito em pastas particulares no próprio computador ou no servidor), além também do uso de telefones inteligentes corporativos, notebooks e pen-drives.

- Para evitar o risco de serem responsabilizadas caso seja encontrado material de pedofilia em seus equipamentos.
- É dever da empresa, e diretamente do gestor de TI, por alçadas e poderes, saber o que tem dentro de seus equipamentos.

Legislação sobre Crimes Eletrônicos: Brasil

Projeto de Lei de Crimes Eletrônicos (PLC 89/03)

CONDUTA	CRIME	LEGISLAÇÃO ALTERADA	PENA
Disseminar phishing scam (e-mails fraudulentos contendo malwares e outros códigos maliciosos)	ESTELIONATO ELETRÔNICO	Art. 171, parág. 2º, VII, Cód. Penal	Reclusão, de 1 a 3 anos.
Roubar senhas bancárias através de phishing scam.	ESTELIONATO ELETRÔNICO	Art. 171, parág. 2º, VII, Cód. Penal	(Majoração da pena se o agente se vale de nome falso ou identificação de terceiros.
Falsificar cartão de crédito.	FALSIFICAÇÃO DE DADO ELETRÔNICO OU DOCUMENTO PARTICULAR	Art. 298, Cód. Penal	Reclusão, de 1 a 3 anos.
Destruir, inutilizar ou deteriorar dado eletrônico alheio.	DANO	Art. 163, Cód. Penal	(Majoração da pena se o agente se vale de nome falso ou identificação de terceiros.
Inserir ou difundir códigos maliciosos em dispositivos de comunicação, redes, sistemas, causando dano.	INSERÇÃO OU DIFUSÃO DE CÓDIGO MALICIOSO SEGUIDO DE DANO	Art. 163-A, parág. 1º, Cód. Penal	Reclusão, de 1 a 5 anos, e multa.
Inserir ou difundir códigos maliciosos (vírus, worms, trojans, etc.) em dispositivos de comunicação, redes , sistemas.	INSERÇÃO OU DIFUSÃO DE CÓDIGO MALICIOSO	Art. 163-A, Cód. Penal	Detenção, de 1 a 6 meses, ou multa.
Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida.	ACESSO NÃO AUTORIZADO	Art. 285-A, Cód. Penal	Reclusão, de 2 a 4 anos, e multa.
Obter ou transferir dado ou informação sem autorização (ou em desconformidade à autorização).	OBTENÇÃO NÃO AUTORIZADA DE INFORMAÇÃO	Art. 285-B, Cód. Penal	CONDUTA
Divulgar, sem autorização, informações pessoais disponíveis em banco de dados.	DIVULGAÇÃO NÃO AUTORIZADA DE INFORMAÇÕES PESSOAIS	Art. 154-C, Cód. Penal	CONDUTA
Atentado contra a segurança de serviço de utilidade pública	ATAQUES A REDES E INVASÕES	Art. 265, Cód. Penal	CONDUTA
Interrupção ou pertubação de serviço telebráfico, telefônico, informático, telemático, dispositivo de comunidação, rede de computadores ou sistemas informatizados	ATAQUES A REDES E INVASÕES	Art. 266, Cód. Penal	CONDUTA
Falsificação de dado eletrônico ou documento público.	FALSA IDENTIDADE, FALSIDADE IDEOLÓGICA DIGITAL, FRAUDE	Art. 297, Cód. Penal	CONDUTA
Falsificação de dado eletrônico ou documento particular.	FALSA IDENTIDADE, FALSIDADE IDEOLÓGICA DIGITAL, FRAUDE	Art. 298, Cód. Penal	CONDUTA
Preconceito	PRECONCEITO DIGITAL	Art. 20, §3º, II, Lei 7.716/89	CONDUTA
Pedofilia	PEDOFILIA DIGITAL	Art. 241, Lei 8.069/90	

Autoria Tabela: PATRICIA PECK PINHEIRO ADVOGADOS – Dra. Patricia Peck, Dra. Gisele Truzzi, Dr. Raphael Loschiavo.

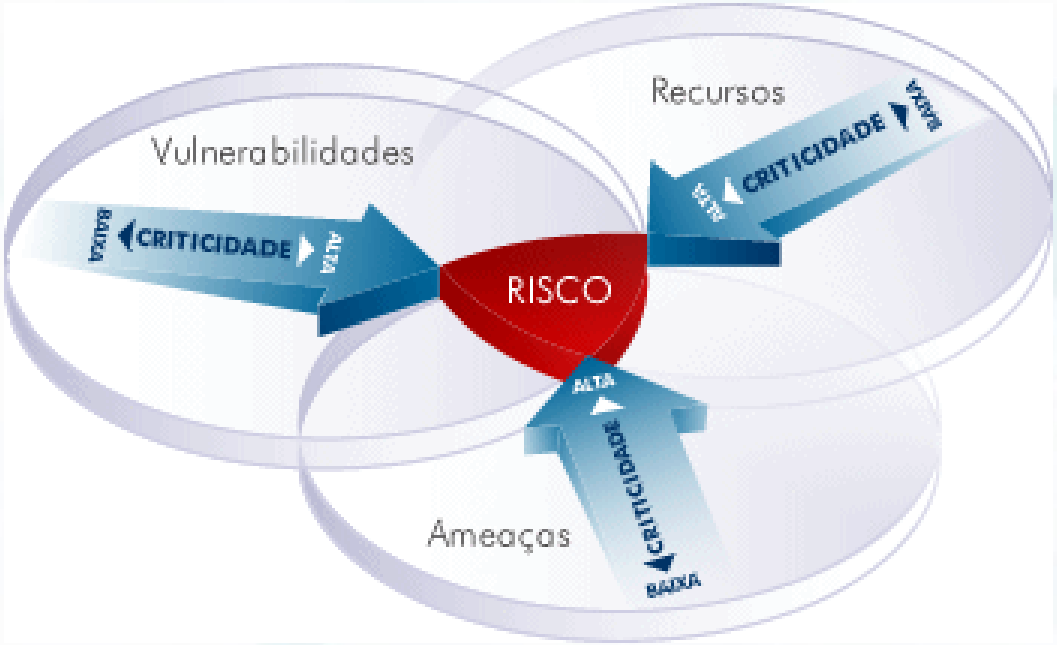
Como Estabelecer uma Estrutura para Segurança e Controle

- **ISO 17.799**
  - Norma de Segurança da Informação.
  - O padrão é um conjunto, de recomendações para práticas na gestão de Segurança da Informação. Ideal para aqueles que querem criar, implementar e manter um sistema.
  - Tem como objetivo confidencialidade, integridade e disponibilidade das informações são fatores muito importantes para segurança e integridade das informações.

Como Estabelecer uma Estrutura para Segurança e Controle

- **Política de segurança**
  - Chief security officer (CSO)
  - Política de uso aceitável (AUP)
  - Políticas de autorização
  - Sistemas de gerenciamento de autorização

Avaliação de Riscos



Como Assegurar a Continuidade dos Negócios

- ***Downtime*** – períodos em que o sistema não está disponível: para fins de manutenção, troca de equipamento, arquivamento de dados antigos, etc.
- **Sistemas de computação tolerantes a falhas**
  - a sistemas de computador que continuam a operar em um nível reduzido, porém aceitável, depois de uma falha do sistema.

Como Assegurar a Continuidade dos Negócios

- **Computação de alta disponibilidade**
  - De forma ampla: todo o tipo de soluções redundantes de equipamento informático e serviços, no sentido de manter o funcionamento contínuo desses sistemas e, consequentemente, da empresa.
  - Num sentido mais restrito digamos que se trata de um sistema alternativo, de segurança, que entra em funcionamento logo que o sistema (ou parte do sistema) principal/operacional falhar e que, especialmente, mantenha a disponibilidade de todos os dados.
- **Computação orientada a recuperação**
  - Recuperação de bases de dados

Como Assegurar a Continuidade dos Negócios

- **Plano de recuperação de desastres**
  - estratégias para restaurar os serviços de computação e comunicação após eles terem sofrido uma interrupção
- **Plano de continuidade dos negócios**
  - Análise de cada área da empresa e aponta os locais mais vulneráveis.
- ***Outsourcing* da segurança (provedores de serviços de segurança gerenciada)**

Como Assegurar a Continuidade dos Negócios

- **Controles Biométricos:**
  - **medidas de segurança fornecidas por dispositivos de computador que medem características físicas que tornam cada indivíduo único. Isto inclui: Verificação de voz; Análise de digitação; Impressões digitais; Escaneamento de retina; Geometria de mão; Reconhecimento facial; Dinâmica de assinatura; Análise de padrões genéticos.**

Certificado Digital

- um arquivo presente no computador que permite identificar uma pessoa ou um computador.
- alguns aplicativos, como seu navegador ou seu leitor de correio eletrônico, utilizam esse arquivo para comprovar a identidade do computador ou da pessoa com a qual você está conectado.

Certificado Digital

- Exemplos:
- Quando você consulta seu banco através de seu Website, este se identifica através de um certificado digital que aparece como um cadeado na interface de seu navegador.
- Clicando no cadeado você pode confirmar que o Banco é realmente quem diz ser.
- Esta operação de identificação das partes permite ainda que as informações que trafegam entre o site do banco e o seu computador sejam protegidas de forma que impossibilitem a interceptação de dados confidenciais de sua conta.
- Como uma carteira de identidade, um Certificado Digital confirma a autenticidade dos sites.

O Papel da Auditoria no Processo de Controle

- **Auditoria de sistemas**
  - **Identifica todos os controles que governam sistemas individuais de informação e avalia sua efetividade.**
  - **O auditor entrevista indivíduos-chave e examina os controles de aplicação, os controles gerais de integridade e as disciplinas de controle.**

Controle de Acesso

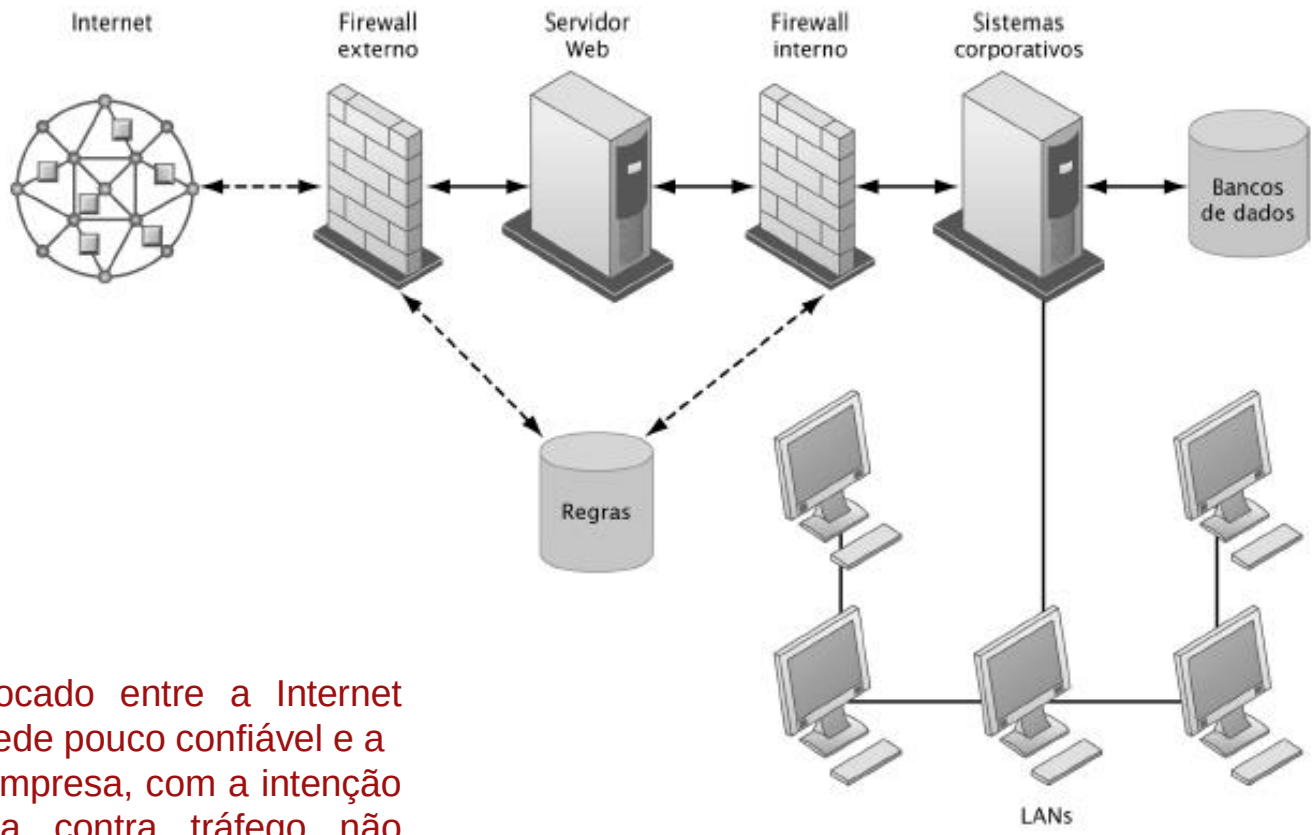
- **Autenticação:** processo que busca verificar a identidade digital do usuário de um sistema, normalmente, no momento em que ele requisita um *log in* em um programa ou computador.
- **Tokens:** Chave eletrônica - conjunto de caracteres (de um alfabeto, por exemplo) com um significado coletivo.
- **Smart cards:** cartão de plástico com tarja magnética. Usado em cartões bancários/crédito e de identificação pessoal, também nos celulares GSM ("chip“). Possui capacidade de processamento - embute um microprocessador e memória (que armazena vários tipos de informação na forma eletrônica), ambos com sofisticados mecanismos de segurança.
- **Autenticação biométrica**

Firewalls, Sistemas de Detecção de Invasão e Software Antivírus

- **Firewall:** combinação de hardware e software que controla o fluxo de tráfego que entra ou sai da rede
- **Sistemas de detecção de invasão monitoram em redes corporativas para detectar e deter intrusos**
- **Software antivírus e *antispyware:*** verifica a presença de malware em computadores e freqüentemente também é capaz de eliminá-lo

Tecnologias e Ferramentas para Garantir a Segurança

Um Firewall Corporativo



O firewall é colocado entre a Internet pública ou outra rede pouco confiável e a rede privada da empresa, com a intenção de proteger esta contra tráfego não autorizado.

Figura 7.6

Um Firewall Corporativo

•Um firewall de rede é um sistema de computador guardião que protege as intranets e outras redes de computadores de uma empresa contra a invasão, funcionando como um filtro e ponto seguro de transferência para acesso à Internet e outras redes.

•Um computador de rede firewall filtra todo o tráfego de rede em busca de senhas corretas ou outros códigos de segurança e somente permite transmissões autorizadas para dentro e para fora da rede.

•Os firewalls se tornaram um componente essencial de organizações que se conectam com a Internet, em virtude da vulnerabilidade e falta de segurança da Internet.

•Os firewalls podem deter, mas não evitar inteiramente, o acesso não autorizado (hacking) às redes de computadores.

Segurança em Redes Sem Fio

Algoritmos e métodos de criptografia

- A segurança WEP *(Wired Equivalent Privacy)* pode ser melhorada quando usada com a tecnologia VPN *(Virtual Private Network)* - Rede privada trafegando pela web (pública), com protocolos de criptografia.
- Especificações Wi-Fi Alliance/Acesso Protegido (WPA - Wi-Fi Protected Access)
- Protocolo de Autenticação Extensível (EAP) - permite métodos de autenticação arbitrários que utilizam trocas de informações e credenciais de tamanhos arbitrários.
- Proteção contra redes falsas

Sessão Interativa: Segurança em Redes Sem Fio

- Você utiliza tecnologia sem fio?
- Em caso positivo, que tipos de informação você transmite através da rede sem fio?
- Que tipos de informação você evita enviar através de redes sem fio? Por que você se preocupa em enviar esses tipos de informação?
- Se você não tem acesso a uma rede sem fio, isso se deve a questões de segurança?

Criptografia e Infra-Estrutura de Chave Pública

- **Criptografia: transformar textos comuns ou dados em um texto cifrado, que não possa ser lido por ninguém a não ser o remetente e o destinatário desejado.**
  - ***Secure Sockets Layer (SSL)***
  - ***Transport Layer Security (TLS)***
  - ***Secure Hypertext Transfer Protocol (S-HTTP)***
  - **Criptografia de chave pública**
  - **Assinatura digital**
  - **Certificado digital**
  - **Intra-estrutura de chave pública (PKI)**

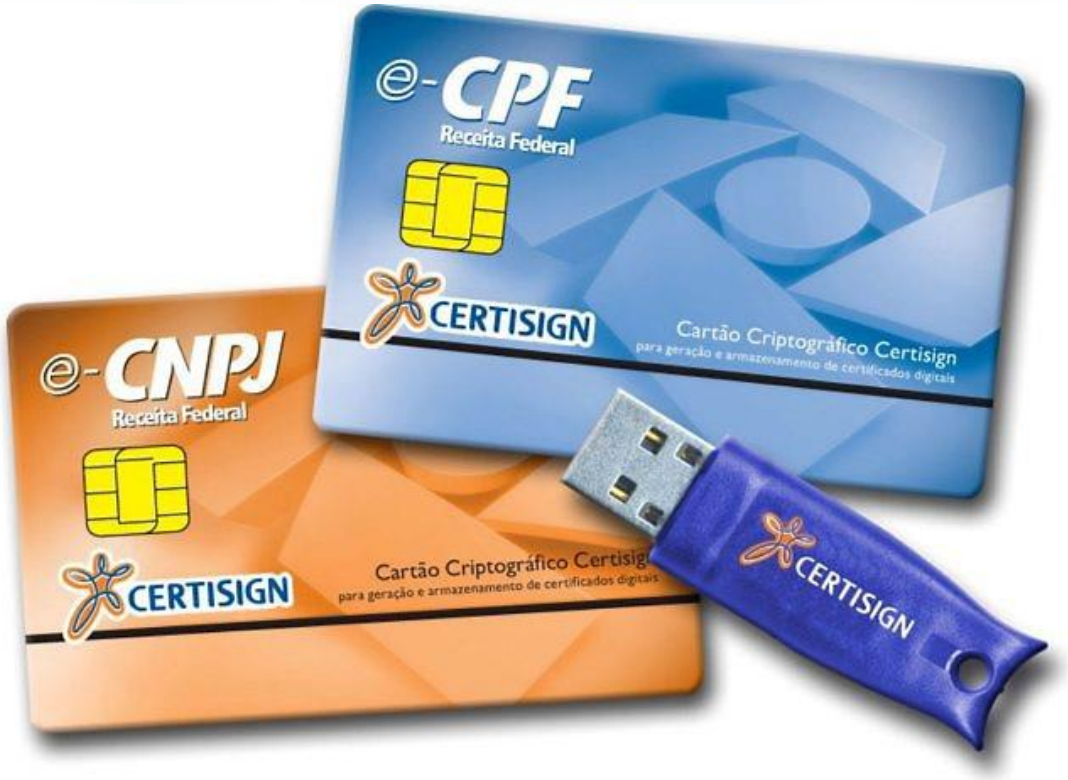
Criptografia e Infra-Estrutura de Chave Pública

Intra-estrutura de chave pública (PKI)

- A PKI refere-se a um processo que utiliza chaves públicas e Certificados Digitais para garantir a segurança do sistema e confirmar a identidade de seus usuários.
- baseia-se em um sistema de confiança, no qual duas partes (pessoas ou computadores) confiam mutuamente em uma CA (Autoridade Certificadora) para verificar e confirmar a identidade de ambas as partes.

Tecnologias e Ferramentas para Garantir a Segurança

e-CPF / e-CNPF – cartão criptográfico



e-CPF / e-CNPF – cartão criptográfico

- O e-CPF é o documento de identificação na internet. Com ele, é possivel assinar documentos eletrônicos com validade jurídica, autenticar-se em sites, realizar serviços da Receita Federal, como entrega de declarações e acesso ao e-CAC, tanto para a pessoa física quanto para as empresas das quais você for o representante legal.

- O e-CNPJ é o documento de identificação de uma empresa. Com ele, é possível assinar documentos eletrônicos com validade jurídica, autenticar-se em sites, realizar serviços da Receita Federal, como entrega de declarações e acessar o e-CAC.

Criptografia e Infra-Estrutura de Chave Pública

- **Criptografia:**
  - tornou-se uma maneira importante de proteger dados e outros recursos de rede de computadores, principalmente na Internet, intranets e extranets.

  Características da criptografia incluem:

  - Senhas, mensagens, arquivos e outros dados que podem ser transmitidos de forma embaralhada e desembaralhados pelos sistemas de computadores apenas para usuários autorizados.
  - O uso de algoritmos matemáticos especiais, ou chaves, para transformar dados digitais em um código embaralhado antes que esses dados sejam transmitidos e para decodificá-los quando forem recebidos.