

SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

Segurança da Informação

Segurança da Informação

A informação é o maior patrimônio para muitas empresas e protege-la não é uma atividade simples.

Entretanto, para que seja possível obter nível aceitável de segurança, não basta reunir um conjunto de ferramentas de software e implementá-las. Os seus resultados tornam-se mais eficazes quando sua utilização está dentro do contexto de um **Plano de Segurança**, elaborado em conjunto pelos níveis estratégicos, tático e operacional da empresa.

É claro que as medidas de segurança não asseguram 100% de proteção contra todas as ameaças, mas a definição das expectativas da Organização, com relação ao comportamento e os procedimentos necessários no manuseio dos seus bens/ativos, deverá estar mais do que nunca enraizados na cultura da empresa, pois **segurança não é só uma questão técnica, mas de política e educação empresarial**.

Segurança da Informação

Segurança da Informação

Portanto a segurança de uma empresa não está ligado somente a produtos voltados à segurança como:

- Firewall;
- Software de encriptação de dados;
- IDS;
- etc.

Mas sua abrangência vai muito além disso, como podendo-se citar:

- Análise de Risco;
- Política de Segurança;
- Controle de Acesso Físico e Lógico;
- Treinamento e Conscientização para Segurança da Informação;
- Plano de Contingência.

A segurança da informação pode e deve ser tratada como um conjunto de mecanismo conforme acima exposto, devendo ser adequada à necessidade de cada empresa.

Segurança da Informação

Segurança da Informação

Alguns pontos são importantes de determinar quanto a segurança, e a empresa deve sempre tê-los em mente:

- ✓ O que deve ser protegido?
- ✓ Contra o que será necessário proteger?
- ✓ Como será feita a proteção?

Além disso, será necessário determinar que nível de segurança é necessário, bem como avaliar a questão **custo x benefício**.

Segurança da Informação

Segurança da Informação

Exemplo:

Uma agência de publicidade, que esteja ligada a Internet, necessita de muita proteção para seus projetos, pois uma propaganda que irá veicular na mídia na semana seguinte não pode de maneira alguma cair nas mãos da concorrência.

Já em Universidade, não é necessária tanta segurança, pois suas publicações, como monografia, teses e material científico, geralmente são colocados à disposição de alunos e pesquisadores do mundo inteiro, para consulta.

Segurança da Informação

Objetivos da Segurança da Informação

Todo projeto de segurança de informação procura abranger “pelo menos” os **processos mais críticos** do negócio em questão.

O resultado esperado de um trabalho como este é, sem dúvida, que no mínimo todos os investimentos efetuados devam conduzir para:

- Redução de probabilidade de ocorrência de incidentes de segurança;
- Redução dos danos/perdas causados por incidentes de segurança;
- Recuperação dos danos em caso de desastre/incidente.

O objetivo da segurança, no que tange à informação, é à busca de disponibilidade, confidencialidade e integridade dos seus recursos e da própria informação.

Segurança da Informação

Análise de Risco

A análise de risco consiste em um **processo de identificação, avaliação dos fatores de risco presentes** e de forma antecipada no Ambiente Organizacional, possibilitando uma visão do impacto negativo causado aos negócios.

Através da aplicação deste processo, é possível determinar as prioridades de ação em função do risco identificado, para que seja **atingindo o nível de segurança desejado pela Organização**. Proporciona também informações para que se possa identificar o tamanho e o tipo de investimento necessário de forma antecipada aos impactos na Organização causados pela perda ou indisponibilidade dos recursos fundamentais para o negócio.

Portanto, como é possível prever alguns inúmeros acontecimentos que poderão ocorrer, este tipo de análise aponta os possíveis perigos e suas consequências em virtude das vulnerabilidades presentes no ambiente computacional de muitas empresas.

Por outro lado, sem um processo deste tipo, não é possível identificar a origem das vulnerabilidades, nem visualizar os riscos.

Segurança da Informação

Análise de Risco

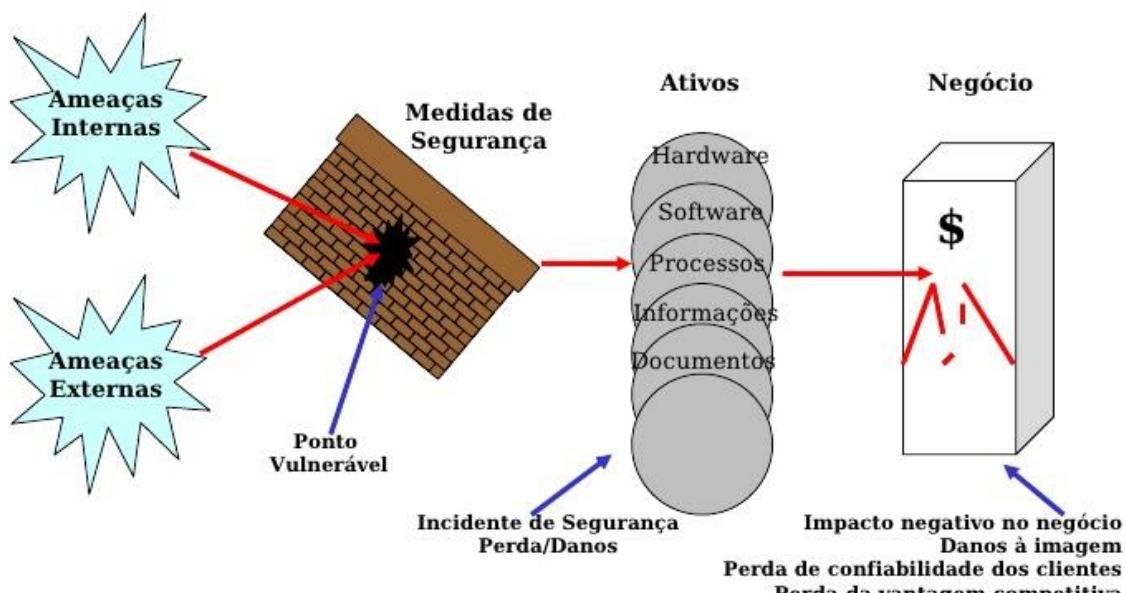
As medidas de segurança não podem assegurar 100% de proteção, e a empresa deve analisar a relação custo/benefício.

Então, a empresa precisa achar o nível de risco ao qual estará disposta a correr. Este processo deve, no mínimo, proporcionar as seguintes informações:

- Pontos vulneráveis do ambiente;
- Ameaças potenciais ao ambiente;
- Incidentes de segurança causados pela ação de cada ameaça;
- Impacto negativo para o negócio a partir da ocorrência dos incidentes prováveis de segurança;
- Riscos para o negócio a partir de cada incidente de segurança;
- Medidas de proteção adequadas para impedir ou diminuir o impacto de cada incidente.

Alguns fatores são cruciais e devem ser identificados a fim de mapear todos o negócio da empresa com o intuito de detectar a presença de riscos.

Segurança da Informação



Incidente de Segurança

Segurança da Informação

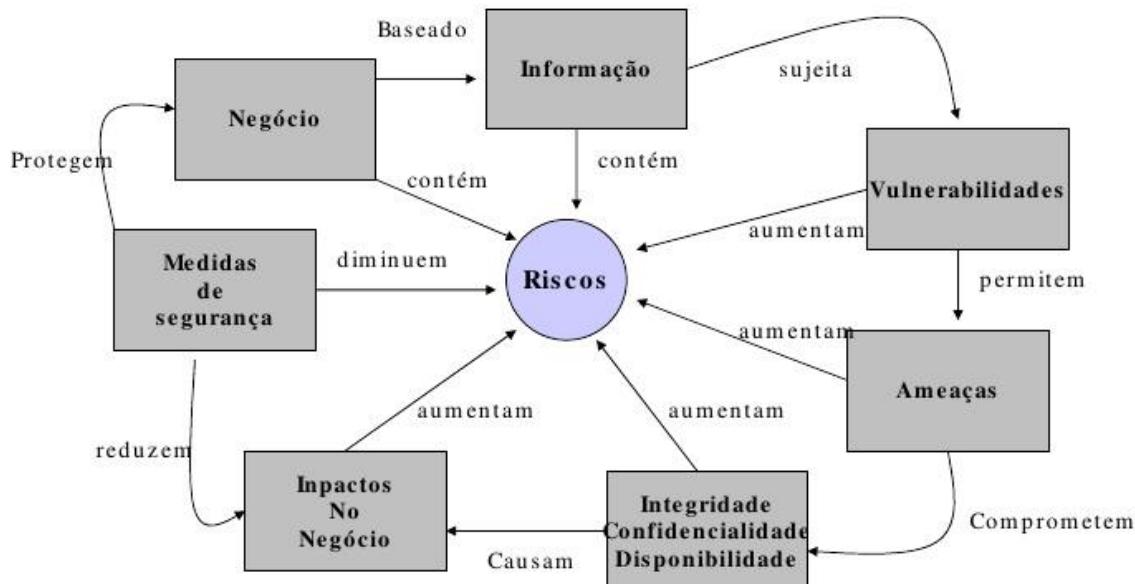
Alguns exemplos de questionamento devem ser feitos pelas empresas antes de efetuarem qualquer investimento:

- Que ativos devem ser protegidos?
- Quais ativos críticos deverão ter proteção adicional?
- Quais serviços na rede deverão estar disponíveis para os funcionários?
- Quem terá acesso a esses serviços?
- Quem poderá conceder autorização e privilégios para o acesso aos sistemas?
- Que software permitir nas estações de trabalho?
- Como proceder quando programas não-aprovados/piratas forem encontrados nas estações de trabalho?

Abrangência

O processo de análise das medidas de segurança pode ser aplicado onde seja necessário avaliar riscos potenciais, independente da área desejada, quanto maior o escopo de avaliação, menor a possibilidade de erros em virtude da abrangência dos recursos envolvidos.

Segurança da Informação



Ciclo de Segurança da Informação

Segurança da Informação

Vulnerabilidade

A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc. Condição causada muitas vezes pelas ausência ou ineficiência das medidas de proteção utilizadas com o intuito de salvaguardar os bens da empresa.

Todos os sistemas são vulneráveis, partindo do pressuposto de que não existem ambientes totalmente seguros. Até as medidas de seguranças implementadas pela empresa possuem falhas.

O nível de vulnerabilidade decai à medida em que são implementados controles e medidas de proteção adequadas, diminuindo também os riscos para o negócio.

Então podemos dizer que **os riscos estão ligados ao nível de vulnerabilidade** que o ambiente analisado possui, pois para se determinar os riscos, as vulnerabilidades precisam ser identificadas.

Segurança da Informação

Como Surgem as Vulnerabilidades?

As vulnerabilidades estão presentes no dia-a-dia das empresas e se apresentam nas mais diversas áreas de uma organização.



Não existe uma única causa para o surgimento de vulnerabilidade. A negligência por parte de administradores de rede e a falta de conhecimento técnico são exemplos típicos.

Algumas vulnerabilidades estão presentes nos Sistemas Operacionais que acabamos de instalar.

Normalmente os hackers são os primeiros a explorarem as vulnerabilidades.

Segurança da Informação

Qual a relação entre vulnerabilidade X medidas de Proteção?

As medidas de proteção também estão sujeitas a terem vulnerabilidades. Enquanto que para um conjunto de ocorrências (ameaças), determinadas medidas de proteção são adequadas, para outras não.

Portanto nas empresas encontramos medias adequadas para uma determinada situação e inadequadas para outras. Por isso é preciso buscar a melhor relação custo/benefício no momento da definição de sua estratégia de segurança.

O nível de vulnerabilidade do ambiente computacional decai à medida em que são implementados controles e medidas de proteção adequadas, diminuindo também os riscos para o negócio. Podemos dizer que os riscos estão ligados ao nível de vulnerabilidade e ao grau de eficiência de proteção.

Segurança da Informação

Incidentes de Segurança

Um incidente de segurança é qualquer evento que prejudique o bom andamento dos sistemas, das redes ou do próprio negócio.

Este incidente pode ser o resultado de uma violação de segurança concretizada, um acesso não-autorizado a determinadas informações confidenciais ou até mesmo um site tirado do ar pela ação de um hacker.

Os incidentes de segurança ocorrem pela ação efetiva de uma determinada ameaça através de uma vulnerabilidade encontrada. Logo, podemos afirmar que os incidentes de segurança somente podem ser concretizados quando existem ambientes propícios, ou seja, vulnerabilidades.

Segurança da Informação

Medidas de Segurança

Medidas de segurança são esforços como procedimentos, software, configurações, hardware e técnicas empregadas para atenuar as vulnerabilidades com o intuito de reduzir a probabilidade de ocorrência de ação de ameaças e, por conseguinte, os incidentes de segurança.

Como tudo envolve custo, antes de decidir pela estratégia a ser adotada, é importante atentar para o nível de aceitação dos riscos. Este sim deve definir os níveis de investimentos das medidas de segurança que serão adotadas pela empresa.

Segurança da Informação

Medidas de Segurança

Existem algumas estratégias que pode ser aplicada em um ambiente computacional. A seguir apresentamos três estratégias de segurança que podem ser utilizadas:

•**Medida Preventiva:** Este tipo de estratégia possui como foco a prevenção da ocorrência de incidentes de segurança. Todos os esforços estão baseados na precaução e, por esta razão, o conjunto de ferramentas e/ou treinamentos estão voltados para esta necessidade.

•**Medida Detectiva:** É a estratégia utilizada quando se tem a necessidade de obter auditabilidade, monitoramento e detecção em tempo real de tentativas de invasão;

•**Medida Corretiva:** O enfoque desta estratégia é propor mecanismos para a continuidade das operações, ela propõe ferramentas e procedimentos necessários para a recuperação e a continuidade de uma empresa. Esta medida é muito delicada e deve ser realizada com extremo nível de profissionalismos, por se tratar da recuperação da imagem da empresa.

Segurança da Informação

Processo de segurança

A segurança não é uma tecnologia.

Não é possível comprar dispositivos que torne sua rede segura, assim como não é possível comprar ou criar um software capaz de tornar seu computador seguro. O que é possível fazer é administrar um nível aceitável de risco.

A segurança é um processo.

Pode-se aplicar o processo seguidamente à rede e à empresa que a mantém e, dessa maneira, melhorar a segurança dos sistemas. Se não iniciar ou interromper a aplicação do processo sua segurança será cada vez pior, à medida que surgirem novas ameaças e técnicas.

“É como subir uma escada rolante que desce”.

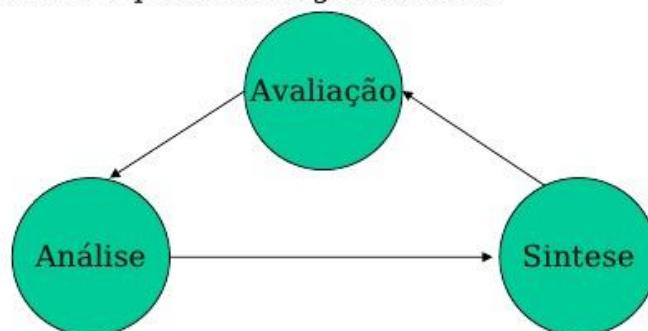
Segurança da Informação

Processo de segurança

O processo de segurança consiste em:

- **Analise** o problema levando em consideração tudo que conhece.
- **Sintetize** uma solução para o problema a partir de sua análise.
- **Avalie** a solução e aprenda em que aspectos não correspondeu a suas expectativas.

Depois, reinicie o processo seguidamente.



Segurança da Informação

Processo de segurança

Em ambientes Informatizados o processo de segurança consiste basicamente em:

- Aprenda tudo o que puder sobre ameaças que encontrar. Use a Internet para adquirir informações e lembre-se de que as informações mudam todos os dias.
- Planeje o melhor possível de acordo com o que aprendeu antes de implementar qualquer coisa. Uma reflexão em um fim de semana sobre o que foi aprendido poderá economizar uma quantidade considerável de tempo e dinheiro.
- Pense como um atacante (pensar idéias perversas) e fortaleça a segurança até torná-la a mais segura possível.
- Implemente exatamente como foi projetado.
- Verifique tudo continuamente para ter certeza de que nada foi alterado. Configurações em computadores podem ser modificadas em instantes e essa modificação poderá causar um forte impacto de segurança. Cuide para que mudanças temporárias sejam temporárias, pois não existe mecanismos capazes de chamar a atenção sobre mudanças.
- Pratique a execução para ter certeza de que comprehendeu e será capaz de operá-la de maneira correta.

Segurança da Informação

Processo de segurança

- Simplifique o que deseja que as pessoas façam. O sistema não deve ser seguro porque as pessoas não conseguem utilizá-lo. A arte de projetar a segurança de um sistema consiste em fazê-lo de forma que os usuários não precisem se preocupar com as medidas de seguranças adotadas, contanto que façam o que lhes é permitido.
- Dificulte o que não deseja que as pessoas façam. Isso se aplica para pessoas desautorizadas e autorizadas.
- Facilite a identificação de problemas. Em qualquer rede existe uma grande quantidade de informações relevantes aprenda como usar essas informações.
- Dificulte esconder o que não deseja que fique escondido. Quanto maior a quantidade de eventos registrados e quanto mais exaustivamente os analisar, maior será a chance de reconhecer rastros de ataques.
- Teste tudo o que puder testar. Comece pelos itens mais importantes e examine todos.
- Pratique tudo o que puder praticar. Para defender a rede, as pessoas precisam conhecer suas funções e estar preparadas de maneira adequada.
- Melhore tudo o que puder melhorar. Faça com que seja mais simples, mais rápido, mais robusto.
- Repita esse processo continuamente, em todos os níveis de detalhe.

Segurança da Informação

Política de Segurança

A política de segurança pode ser entendida como sendo um conjunto de normas e diretrizes destinadas a proteção dos ativos da Organização.

Política de segurança pode ser um documento, no qual deve estar descrito a forma que a empresa deseja que seus ativos sejam:

- Protegidos;
- Manuseados;
- Tratados;

O objetivo de qualquer Política de Segurança é o de definir as expectativas da Organização quanto ao uso dos seus recursos (computadores e redes), estabelecendo procedimentos com o intuito de prevenir e responder a incidentes relativos à segurança.

Segurança da Informação

Política de Segurança

Devido ao fato da informação nos dias atuais ter um grande valor estratégico e tático para as Organizações. Hoje em dia, a informação é o Ativo mais valioso de muitas empresas.

Diante deste cenário, a política de segurança passa a ter uma importante função, pois visa a proteção dos ativos da Organização para que os negócios não parem e ocorram dentro de um ambiente harmônico e seguro.

Segurança da Informação

Escrevendo uma política de segurança

Uma política de segurança atende a vários propósitos:

- › Descreve o que está sendo protegido e por quê.
- › Define prioridades sobre o que esta precisa ser protegido em primeiro lugar e com qual custo.
- › Permite estabelecer um acordo explícito com as várias partes da empresa em relação ao valor da segurança.
- › Fornece ao departamento de segurança um motivo válido para dizer “não” quando necessário.
- › Impede que o departamento de segurança tenha um desempenho fútil.

A Política de segurança de computadores é o que há de mais importante. Porém, se pedir que algum profissional da segurança mostre a política que eles utilizam, é bastante provável que, com um sorriso meio sem graça, perçam que volte mês que vem, quando estiver pronto, ou seja, quase ninguém tem realmente uma política de segurança.

Segurança da Informação

Política de segurança

A política de segurança é a medida de segurança mais importante de uma empresa, mas é muito provável que a maioria das empresas não possua uma.

As razões para isso são:

- › **Prioridade.** A política é importante, mas hoje é preciso que alguém coloque o servidor Web on-line. É necessário notar que uma política de segurança é urgente.
- › **Política interna.** Em qualquer empresa vários fatores internos afetam qualquer decisão prática.
- › **Propriedade.** Em algumas empresas existem brigas entre grupos para ser donos da política, ou o não.
- › **Dificuldade para escrever.** Uma boa política é um documento difícil de se organizar.

Segurança da Informação

Adiante são apresentadas algumas sugestões para ajudar a solucionar problemas com a aplicação (confecção) de políticas de segurança em empresas:

- Uma boa política hoje é melhor que uma excelente política no próximo ano.
- Uma política fraca, mas bem-distribuída, é melhor do que uma política forte que ninguém leu.
- Uma política simples e facilmente compreendida é melhor do que uma política confusa e complicada que ninguém se dá o trabalho de ler.
- Uma política cujos detalhes estão ligeiramente errados é muito melhor do que uma política sem quaisquer detalhes.
- Uma política dinâmica que é atualizada constantemente é melhor do que uma política que se torna obsoleta com o passar do tempo.
- Costuma ser melhor se desculpar do que pedir permissão.

Segurança da Informação

Para se escrever uma boa política execute os seguintes passos:

- 1.** Escreva uma política de segurança para sua empresa.
 - › A política deve ter no máximo 5 páginas
 - › Não tente torná-la perfeita;
 - › Procure apenas reunir algumas idéias essenciais;
 - › Não é necessário que esteja completa e não precisa ser de uma clareza absoluta.
- 2.** Descubra três pessoas dispostas a fazer parte do “comitê de política de segurança”. Elas irão criar regras e emendas para a política sem modificá-la.
- 3.** Crie um site da Web interno sobre a política e inclua uma página descrevendo como entrar em contato com o comitê de política de segurança. Mantenha sempre o site atualizado com as políticas.
- 4.** Trate a política e as emendas como regras absolutas com força de lei.
 - › Na permita que a política seja violada.
- 5.** Se alguém tiver algum problema com a política, faça com que a pessoa proponha uma emenda.
- 6.** Programe um encontro regular, fora do local de trabalho, para consolidar a política e as emendas.
- 7.** Repita o processo novamente. Exponha a política no site, trate-a como lei, envolva as pessoas da administração, acrescente emendas conforme seja necessário e revise tudo a cada ano.

Segurança da Informação

Descreva como é determinada a importância de uma violação da política e as categorias de consequências. Alguns exemplos são apresentados a seguir.

Penalidades:

Critica

- Recomendação para demissão;
- Recomendação para abertura de ação legal;

Seria

- Recomendação para demissão;
- Recomendação para desconto de salário;

Limitada

- Recomendação para desconto de salário;
- Repreensão formal por escrito;
- Suspensão não-remunerada;

OBRA NR. 2

SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

Objetivos de estudo

- Por que sistemas de informação estão vulneráveis a destruição, erros e uso indevido?
- Qual o valor empresarial da segurança e do controle?
- Quais os componentes de uma estrutura organizacional para segurança e controle?
- Quais são as mais importantes tecnologias e ferramentas disponíveis para salvaguardar recursos de informação?

Objetivos de estudo

- Por que sistemas de informação estão vulneráveis a destruição, erros e uso indevido?
- Qual o valor empresarial da segurança e do controle?
- Quais os componentes de uma estrutura organizacional para segurança e controle?
- Quais são as mais importantes tecnologias e ferramentas disponíveis para salvaguardar recursos de informação?

Boston Celtics marca pontos importantes contra spyware

- A aplicação de segurança Mi5 Networks' Webgate se posiciona entre o *firewall* e a rede do Celtics, impede que o *spyware* entre na rede e evita que as máquinas já infectadas se conectem a ela.
- Demonstra o papel da TI no combate e na manutenção da segurança dos computadores.
- Ilustra o papel da tecnologia digital na manutenção da segurança na Web.

Boston Celtics marca pontos importantes contra spyware



Vulnerabilidade dos sistemas e uso indevido

- Um computador desprotegido conectado à Internet pode ser desativado em segundos

- **Segurança:**

- Políticas, procedimentos e medidas técnicas usadas para prevenir acesso não autorizado, roubo ou danos físicos aos 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.

Vulnerabilidade dos sistemas e uso indevido

Por que os sistemas são vulneráveis

- **Problemas de hardware**

- Avarias, erros de configuração, danos causados pelo uso impróprio ou por crimes.

- **Problemas de software**

- Erros de programação, erros de instalação, mudanças não autorizadas.

- **Desastres**

- Quedas de energia, enchentes, incêndios etc.

- **Uso de redes e computadores fora dos limites e do controle da empresa**

- **Exemplo:** uso por fornecedores nacionais ou estrangeiros.

Vulnerabilidade dos sistemas e uso indevido

Por que os sistemas são vulneráveis

- Problemas de hardware
 - Avarias, erros de configuração, danos causados pelo uso impróprio ou por crimes.
- Problemas de software
 - Erros de programação, erros de instalação, mudanças não autorizadas.
- Desastres
 - Quedas de energia, enchentes, incêndios etc.
- Uso de redes e computadores fora dos limites e do controle da empresa
 - Exemplo: uso por fornecedores nacionais ou estrangeiros.

Vulnerabilidade dos sistemas e uso indevido

Vulnerabilidades e desafios de segurança contemporâneos



Normalmente, a arquitetura de uma aplicação baseada na Web inclui um cliente, 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.

Vulnerabilidade dos sistemas e uso indevido

- Vulnerabilidades da Internet
 - Rede aberta a qualquer usuário
 - O tamanho da Internet propicia que os abusos tenham um alto impacto
 - Uso de endereços de Internet fixos com conexões permanentes à rede mundial facilita a identificação por *hackers*
 - Anexos de e-mail
 - E-mails usados para transmissão de segredos de negócios
 - Mensagens instantâneas não são seguras e podem ser facilmente interceptadas

Vulnerabilidade dos sistemas e uso indevido

- Desafios da segurança sem fio
 - Bandas de rádiofrequência são fáceis de serem escaneadas
 - Identificadores de conjunto de serviços (SSIDs)
 - Identificar pontos de acesso
 - Transmitidos várias vezes
 - *War driving*
 - Espião dirige um carro entre edifícios ou estaciona do lado de fora e tenta interceptar o tráfego por redes sem fio
 - Quando os *hackers* obtêm acesso ao SSID, conseguem acessar os recursos da rede
 - WEP (Wired Equivalent Privacy)
 - Padrão de segurança para 802.11
 - Especificações básicas compartilham a mesma senha tanto para usuários quanto para os pontos de acesso
 - Usuários não fazem uso de recursos de segurança

Vulnerabilidade dos sistemas e uso indevido

Desafios de segurança em ambientes Wi-Fi

Muitas redes Wi-Fi podem ser facilmente invadidas por intrusos. Eles usam programas *sniffers* para obter um endereço e, assim, acessar sem autorização os recursos da rede.

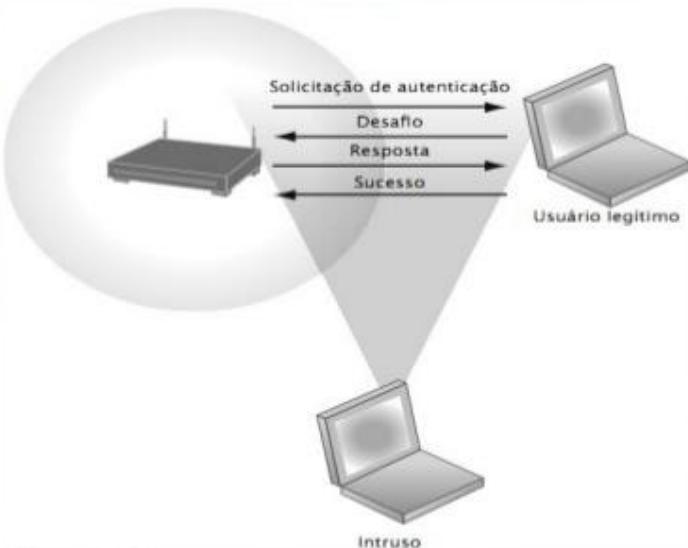


Figura 7.2

Vulnerabilidade dos sistemas e uso indevido

Software mal-intencionado: vírus, worms, cavalos de Troia e spywares

- *Malware*
 - Vírus
 - Programa de software espúrio que se anexa a outros programas de software ou arquivos de dados a fim de ser executado
 - Worms
 - Programas de computador independentes que copiam a si mesmos de um computador para outro por meio de uma rede
 - Cavalos de Troia
 - Software que parece benigno, mas depois faz algo diferente do esperado

Vulnerabilidade dos sistemas e uso indevido

Software mal-intencionado: vírus, worms, cavalos de Troia e spywares

- *Malware* (continuação)
 - *Spyware*
 - Pequenos programas que se instalam sorrateiramente nos computadores para monitorar a atividade do internauta e usar as informações para fins de marketing.
 - *Key loggers*
 - Registram cada tecla pressionada em um computador para roubar números seriais de softwares, senhas, deflagrar ataques na Internet.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- *Hackers versus crackers*
- Atividades incluídas:
 - invasão de sistemas;
 - danos a sistemas; e
 - cibervandalismo.
- Interrupção, a alteração da aparência ou até mesmo a destruição intencional de um site ou sistema de informação corporativo.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- ***Spoofing***

- Apresentar-se de maneira disfarçada, usando endereços de e-mail falsos ou fingindo ser outra pessoa.
- Redirecionamento de um link para um endereço diferente do desejado, estando o site espúrio “disfarçado” como o destino pretendido.

- ***Sniffer***

- Programa espião que monitora as informações transmitidas por uma rede.
- Permitem que os *hackers* roubem informações de qualquer parte da rede, inclusive mensagens de e-mail, arquivos da empresa e relatórios confidenciais.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- **Ataque de recusa de serviço (DoS)**

- Sobrecarregar o servidor com centenas de requisições falsas, a fim de inutilizar a rede

- **Ataque distribuído de recusa de serviço (DDoS)**

- Uso de inúmeros computadores para iniciar um DoS
- *Botnets*
 - Redes de PCs “zumbis” infiltradas por um *malware* robô

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- **Crimes de informática**

- Definidos como “quaisquer violações da legislação criminal que envolvam conhecimento de tecnologia da informática em sua perpetração, investigação ou instauração de processo”

- **Computadores podem ser alvo de crimes:**

- Violar a confidencialidade de dados computadorizados protegidos
- Acessar um sistema de computador sem autorização

- **Computadores podem ser instrumentos de crimes:**

- Roubo de segredos comerciais
- Usar e-mail para ameaças ou assédio

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- **Roubo de identidade**

- Roubo de informações pessoais (número de identificação da Previdência Social, número da carteira de motorista ou número do cartão de crédito) para se fazer passar por outra pessoa.

- **Phishing**

- Montar sites falsos ou enviar mensagens de e-mail parecidas com as enviadas por empresas legítimas, a fim de pedir aos usuários dados pessoais confidenciais.

- **Evil twins**

- Redes sem fio que fingem oferecer conexões Wi-Fi confiáveis à Internet.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- ***Pharming***

- Redireciona os usuários a uma página da Web falsa, mesmo quando a pessoa digita o endereço correto da página da Web no seu navegador.

- **Fraude do clique**

- Ocorre quando um indivíduo ou programa de computador clica fraudulentamente em um anúncio on-line sem qualquer intenção de descobrir mais sobre o anunciante ou realizar uma compra.

Vulnerabilidade dos sistemas e uso indevido

Seção interativa: Organizações O pior roubo de dados da História

- Leia a Seção interativa e responda às seguintes perguntas:

- Liste e descreva as fragilidades do controle de segurança da Hannaford Bros. e das empresas TJX. Que fatores humanos, organizacionais e tecnológicos contribuíram para esses problemas?
- Qual foi o impacto empresarial das perdas de dados da TJX e da Hannaford sobre essas empresas e seus consumidores?
- As soluções adotadas pela TJX e pela Hannaford foram eficientes? Justifique.

Vulnerabilidade dos sistemas e uso indevido

Ameaças internas: funcionários

- Ameaças à segurança costumam ter origem na empresa
 - Conhecimento interno
 - Procedimentos de segurança frouxos
 - Falta de conhecimento do usuário
 - Engenharia social:
 - Intrusos mal-intencionados em busca de acesso ao sistema podem enganar os funcionários fingindo ser membros legítimos da empresa; assim, conseguem fazer com que revelem sua senha

Vulnerabilidade dos sistemas e uso indevido

Vulnerabilidade do software

- **Softwares comerciais contém falhas que criam vulnerabilidades na segurança**
 - *Bugs escondidos* (defeitos no código do programa).
 - A taxa zero de defeitos não pode ser alcançada porque teste completo simplesmente não é possível nos grandes programas.
 - As falhas podem tornar a rede vulnerável aos invasores.
- **Patches**
 - Os fornecedores distribuem pequenos programas que corrigem as falhas.
 - Entretanto, a infinidade de softwares em uso pode fazer com que os *malwares* sejam criados mais rapidamente do que os *patches*.

Valor empresarial da segurança e do controle

- Sistemas computacionais com problemas podem levar a uma perda substancial, senão total, das funções empresariais.
- Atualmente, as empresas estão mais vulneráveis do que nunca.
- Uma falha de segurança pode diminuir o valor de mercado da empresa quase que imediatamente.
- Controle e segurança inadequados também podem criar sérios riscos legais.

Valor empresarial da segurança e do controle

Requisitos legais e regulatórios para a gestão de registros eletrônicos

- **As empresas enfrentam novas obrigações legais no que diz respeito à retenção de documentos e à gestão de registros eletrônicos, bem como à proteção da privacidade**
 - **HIPAA:** regras e procedimentos quanto à privacidade e à segurança médicas
 - **Lei Gramm-Leach-Bliley:** exige que as instituições financeiras assegurem a segurança e a confidencialidade dos dados do cliente
 - **Lei Sarbanes-Oxley:** cabe às empresas e a seus administradores salvaguardar a precisão e a integridade das informações financeiras utilizadas internamente e publicadas externamente

Valor empresarial da segurança e do controle

Prova eletrônica e perícia forense computacional

- As evidências para os crimes de colarinho branco costumam ser encontradas em formato digital.
 - Dados armazenados em dispositivos computacionais, e-mails, mensagens instantâneas, transações de e-commerce .
- O controle apropriado dos dados pode economizar tempo e dinheiro no atendimento às solicitações de produção de provas.
- Perícia forense computacional:
 - Procedimento científico de coleta, exame, autenticação, preservação e análise de dados mantidos em meios de armazenamento digital, de tal maneira que as informações possam ser usadas como prova em juízo.
 - Inclui a recuperação de dados ambientes ou ocultos.

Como estabelecer uma estrutura para segurança e controle

- **Controles de sistemas de informação**
 - **Controles gerais**
 - Controlam projeto, segurança e uso de programas de computadores e a segurança de arquivos de dados em geral em toda a infraestrutura de TI da empresa.
 - Aplicam-se a todas as aplicações computadorizadas.
 - Combinação de hardware, software e procedimentos manuais que criam um ambiente global de controle.

Como estabelecer uma estrutura para segurança e controle

- **Tipos de controles gerais**

- Controles de software
- Controles de hardware
- Controles de operações de computador
- Controles de segurança de dados
- Controles de implementação
- Controles administrativos

Como estabelecer uma estrutura para segurança e controle

- **Controles de aplicação**

- Controles específicos exclusivos a cada aplicação computadorizada, como processamento de folha de pagamento ou pedidos.
- Incluem tanto procedimentos manuais quanto automatizados.
- Garantem que somente dados autorizados sejam completa e precisamente processados pelas aplicações.
- Incluem **controles de entrada, controles de processamento e controles de saída**.

Como estabelecer uma estrutura para segurança e controle

• Avaliação de risco

- Determina o nível de risco para a empresa caso uma atividade ou um processo específico não sejam controlados adequadamente
 - Tipos de ameaças
 - Probabilidade de sua ocorrência ao longo do ano
 - Perdas potenciais, valor da ameaça
 - Prejuízo anual esperado

Exposição	Probabilidade de ocorrência (%)	Faixa de prejuízo/média (\$)	Prejuízo anual esperado (\$)
Falta de energia elétrica	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

Como estabelecer uma estrutura para segurança e controle

• Política de segurança

- Estabelece hierarquia aos riscos de informação e identifica metas de segurança aceitáveis, assim como os mecanismos para atingi-las.
- Dá origem a outras políticas:
 - **Política de uso aceitável (acceptable use policy — AUP)**
 - Define os usos aceitáveis dos recursos de informação e do equipamento de informática da empresa.
 - **Políticas de autorização**
 - Determinam diferentes níveis de acesso aos ativos de informação para diferentes níveis de usuários.

Como estabelecer uma estrutura para segurança e controle

• Sistemas de gestão de autorização

- Estabelecem onde e quando um usuário terá permissão para acessar determinadas partes de um site ou de um banco de dados corporativo.
- Permitem que cada usuário acesse somente as partes do sistema nas quais tem permissão de entrar, com base nas informações estabelecidas por um conjunto de regras de acesso.

Vulnerabilidade dos sistemas e uso indevido

Perfis de segurança para um sistema de pessoal

Estes dois exemplos representam dois perfis de segurança ou modelos de segurança de dados que podem ser encontrados em um sistema de pessoal. Dependendo do perfil de segurança, um usuário teria certas restrições de acesso a vários sistemas, localizações ou dados da organização.

PERFIL DE SEGURANÇA 1	
Usuário: funcionário do departamento pessoal	
Localização: Divisão 1	
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 a Divisão 1 somente	Leitura e atualização
• Dados de histórico médico	Nenhum
• Salário	Nenhum
• Proventos (para cálculo de aposentadoria)	Nenhum
PERFIL DE SEGURANÇA 2	
Usuário: gerente da divisão de pessoal	
Localização: Divisão 1	
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 1 somente	Somente leitura

Como estabelecer uma estrutura para segurança e controle

Plano de recuperação de desastres e plano de continuidade dos negócios

- **Plano de recuperação de desastres:** organiza planos para restauração de serviços que tenham sofrido interrupção
- **Plano de continuidade dos negócios:** concentra-se na restauração das operações de negócios após um desastre
 - Ambos os planos devem:
 - Identificar os sistemas mais importantes da empresa.
 - Realizar uma análise de impacto nos negócios, a fim de identificar o impacto de uma suspensão em seu funcionamento.
 - A administração precisa determinar quais sistemas serão restaurados primeiro.

Como estabelecer uma estrutura para segurança e controle

O papel da auditoria

- **Auditoria de sistemas**
 - Avalia o sistema geral de segurança da empresa e identifica todos os controles que governam sistemas individuais de informação.
 - Revê tecnologias, procedimentos, documentação, treinamento e recursos humanos .
 - Pode até mesmo simular um ataque ou desastre para verificar como os recursos tecnológicos, a equipe de sistemas de informação e os funcionários da empresa reagem.
 - Lista e classifica todos os pontos fracos do controle e estima a probabilidade de ocorrerem erros nesses pontos.
 - Avalia o impacto financeiro e organizacional de cada ameaça.

Vulnerabilidade dos sistemas e uso indevido

Exemplo de listagem feita por um auditor para deficiências de controle

Este diagrama representa uma página da lista de deficiências de controle que um auditor poderia encontrar em um sistema de empréstimos de um banco comercial. Além de ajudar o auditor a registrar e avaliar as deficiências de controle, o formulário mostra os resultados das discussões dessas deficiências com a administração, bem como quaisquer medidas corretivas tomadas por ela.

Função: Empréstimos pessoais Localização: Peoria, IL		Preparado por: J. Ericson Data de preparação: 16 de junho de 2006		Recebido por: T. Barrow Data da revisão: 28 de junho de 2006	
Natureza e impacto das deficiências	Chance de erro substancial		Notificação à administração		
	Sim/ Não	Justificativa	Data do relatório	Resposta da administração	
Os registros do pagamento das prestações de empréstimos não são conciliados com os registros do tomador do empréstimo durante o processamento.	Sim	Sem um controle de detecção, os erros nos balanços de um cliente individual podem continuar passando despercebidos.	10/5/06	O relatório de comparação de taxas de juros provê esse controle.	
Não são feitas auditorias periódicas nos dados gerados por computador (débitos de juros).	Sim	A falta de uma auditoria periódica ou verificação de racionalidade pode resultar na ampla propagação de cálculos errados antes de os erros serem detectados.	10/5/06	Serão instituídas auditorias periódicas sobre os empréstimos.	
Programas podem ser incluídos nas bibliotecas de produção para cumprir metas de prazo, sem aprovação final pelo grupo de Padrões e Controles.	Não	Todos os programas exigem autorização da administração. O grupo de Padrões e Controles controla o acesso a todos os sistemas de produção e determina, para tais casos, um status de produção temporária.			

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Controle de acesso

- Políticas e procedimentos que uma empresa usa para evitar acesso indevido a seus sistemas por pessoas não autorizadas dentro e fora da organização
 - Autorização
 - Autenticação
 - Senhas de sistemas
 - *Tokens*
 - *Smart cards*
 - Autenticação biométrica

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Firewalls, sistemas de detecção de invasão e softwares antivirus

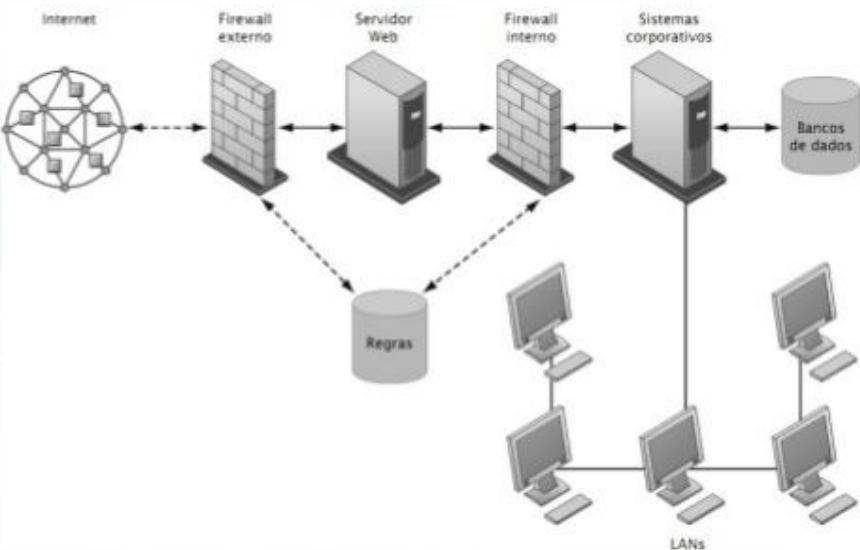
• **Firewall:**

- Combinação de hardware e software que impede que usuários não autorizados acessem redes privadas
- As tecnologias incluem:
 - Filtragem de pacotes estáticos
 - *Network address translation* (Tradução de Endereços IP)
 - Filtragem de aplicação proxy

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

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.



Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Firewalls, sistemas de detecção de invasão e softwares antivirus

- **Sistemas de detecção de invasão:**

- Monitoram os pontos mais vulneráveis de redes corporativas, a fim de detectar e inibir invasores.
- Examinam os eventos em tempo real, em busca de ataques à segurança em curso.

- **Softwares antivirus e anti-spyware:**

- Verificam os computadores a fim de detectar a presença de vírus e, muitas vezes, eliminá-los da área infectada.
- Requerem atualização contínua.

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Segurança em redes sem fio

- **O protocolo WEP oferece alguma margem de segurança se os usuários:**

- Lembrarem-se de ativá-lo.
- Atribuírem um nome único ao SSID de sua rede.
- Utilizarem a tecnologia de rede privada virtual (VPN).

- **A Wi-Fi Alliance finalizou a especificação 802.11i, que substitui o WEP por padrões de segurança mais sólidos**

- Mudança contínua de chaves.
- Sistema de autenticação criptografado com um servidor.

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Criptografia e infraestrutura de chave pública

- **Criptografia:**

- Transforma textos comuns ou dados em um texto cifrado, que não possa ser lido por ninguém a não ser o remetente e o destinatário desejados.
- Dois métodos para criptografar o tráfego de rede:
 - Secure Sockets Layer (SSL) e o seu sucessor, Transport Layer Security (TLS).
 - Secure Hypertext Transfer Protocol (S-HTTP).

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Criptografia e infraestrutura de chave pública

- **Dois outros métodos de criptografia:**

- **Criptografia de chave simétrica**
 - Remetente e destinatário usam e compartilham uma única chave.
- **Criptografia de chave pública**
 - Usa duas chaves matematicamente relacionadas: uma pública e outra privada.
 - O remetente criptografa a mensagem com a chave pública do destinatário.
 - O destinatário descriptografa utilizando a chave privada.

Tecnologias e ferramentas para garantir a segurança dos recursos de informação



Figura 7.6

Um sistema de criptografia de chave pública pode ser visto como uma série de chaves públicas e privadas que “trancam” os dados quando são transmitidos e os “destrancam” quando são recebidos. O remetente localiza a chave pública do destinatário em um diretório e a utiliza para criptografar uma mensagem. A mensagem é enviada sob forma criptografada pela Internet ou por uma rede privada. Quando ela chega, o destinatário usa sua chave privada para descriptografar os dados e ler o conteúdo.

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Criptografia e infraestrutura de chave pública

- **Certificado digital:**

- Arquivos de dados usados para determinar a identidade de pessoas e ativos eletrônicos, a fim de proteger transações on-line
- Usa uma terceira parte fidedigna, conhecida como autoridade certificadora (*Certificate Authority — CA*), para validar a identidade de um usuário
- A CA verifica off-line a identidade do usuário e, em seguida, passa a informação para um servidor da CA, que gera um certificado digital criptografado contendo a identificação do proprietário e uma cópia de sua chave pública

- **Infraestrutura de chave pública (PKI)**

- Uso da criptografia de chave pública em conjunto com uma CA
- Amplamente utilizada no comércio eletrônico

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Os certificados digitais podem ser usados para determinar a identidade de pessoas ou ativos eletrônicos.

Protegem transações on-line ao oferecer comunicação on-line segura e criptografada.



Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Como assegurar a disponibilidade do sistema

- O processamento on-line de transações requer 100% de disponibilidade e total tolerância a falhas.
- Sistemas de computação tolerantes a falhas:
 - Oferecem serviço contínuo. Exemplo: Bolsa de Valores.
 - Incluem componentes redundantes de hardware, software e fornecimento de energia elétrica, criando um ambiente que oferece serviço contínuo, ininterrupto.
- Computação de alta disponibilidade:
 - Ajuda na recuperação rápida de uma parada de sistema.
 - Minimiza, mas não elimina, o *downtime*.

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Como assegurar a disponibilidade do sistema

- **Computação orientada à recuperação**
 - Projeto de sistemas que se restabeleçam de forma rápida, com a implantação de recursos que ajudem os operadores a descobrir as fontes de falhas em sistemas compostos por múltiplos componentes
- **Controle do tráfego de rede**
 - Inspeção profunda de pacotes (*deep packet inspection — DPI*)
(bloqueio de vídeo e música)
- **Outsourcing da segurança**
 - Provedores de serviços de segurança gerenciada (MSSPs)

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Garantia da qualidade de software

- **Métricas de software:** premissas objetivas do sistema na forma de medidas quantificadas
 - número de transações;
 - tempo de resposta on-line;
 - número de contracheques impressos por hora; e
 - erros conhecidos por cento de linhas de código.
- **Teste inicial regular e completo**
- **Acompanhamento:** revisão de uma especificação, ou documento de projeto, realizada por pequeno grupo de pessoas
- **Depuração:** processo através do qual os erros são eliminados

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Seção interativa: Tecnologia Quão segura é a nuvem?

- Leia a Seção interativa e responda às seguintes perguntas:

- Que problemas de segurança e controle são descritos nesse caso? Que fatores pessoais, organizacionais e tecnológicos contribuem para esse problema?
- Quão segura é a computação em nuvem? Explique.
- Se você fosse responsável pelo departamento de sistemas de informação de uma empresa, quais pontos gostaria de esclarecer com os possíveis fornecedores?

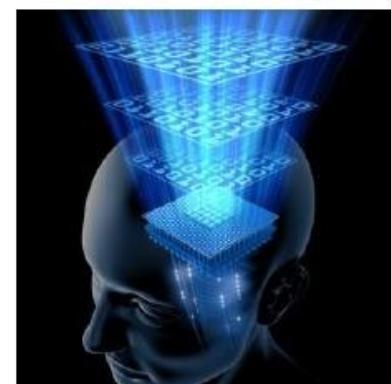
OBRA NR. 3

Princípios de Sistemas de Informações

QUESTÕES ÉTICAS E SOCIAIS NA EMPRESA DIGITAL E SOCIEDADE DA INFORMAÇÃO

1

Prof: Eduardo S. Anselmo



M-COMMERCE

- Abreviatura de móible commerce - modalidade de comércio eletrônico móvel que se diferencia do comércio eletrônico convencional porque é realizado por meio de telefones ou terminais sem fio, em vez de equipamentos fixos.
- Problemas: Privacidade e spam gerado pelo m-commerce.

2

DESAFIOS PARA A ADMINISTRAÇÃO

- Entender os riscos morais da nova tecnologia: rápida mudança tecnológica -> mudança acelerada de alternativas para os indivíduos.
- Estabelecer políticas éticas corporativas que incluem as questões dos sistemas de informação:
 - Privacidade;
 - Propriedade;
 - Prestação de contas;
 - Qualidade do sistema;
 - Qualidade de vida.



3

Aspectos éticos, sociais e políticos

- **ética:** Conjunto de princípios que estabelece o que é certo ou errado e que os indivíduos, na qualidade de agentes livres, podem utilizar para fazer escolhas que orientem o seu comportamento. (princípios)
- **o social e o político:** expectativas e regras de comportamento estabelecidas e partilhadas por uma coletividade suportadas por leis e mecanismos para sancionar as violações. (Leis e Direitos)

4

Tendências tecnológicas que levantam questões éticas

Tendência	Impacto
Poder computacional duplica cada 18 meses	As operações críticas das organizações <u>dependem</u> cada vez mais dos sistemas informáticos(Lei de Gordon E. Moore)
Rápido declínio dos custos de armazenamento	As organizações podem manter facilmente bases de dados detalhadas sobre os clientes e fornecedores
Avanços nas análises de dados	As empresas <u>podem analisar</u> grandes quantidades de dados e desenvolvem perfis do seu comportamento.
Avanços nas redes e na Internet(Cloud-Computing)	Copiar dados de um lado para outro e acessar a informações pessoais é muito mais fácil (ex: google DOCS)

RESPONSABILIDADE, PRESTAÇÃO DE CONTAS E OBRIGAÇÃO DE INDENIZAR

6

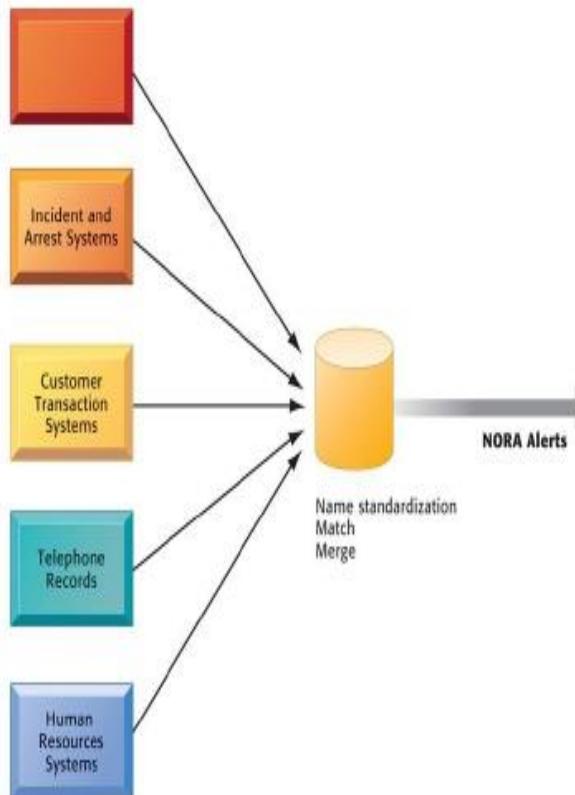
- **Responsabilidade**: Aceitação dos custos, deveres e obrigações potenciais pelas decisões que toma.
- **Prestação de contas**: Levantamento da responsabilidade por decisões e ações.
- **Obrigação de indenizar**: Permite aos indivíduos recuperar danos.
- **Devido processo legal**: Leis são conhecidas e entendidas e é possível apelar a autoridades superiores.

NORA

:: Non Obvious Relationship Awareness (Sistema de correlação de eventos para atividades ilícitas)

FIGURE 5-2 Nonobvious relationship awareness (NORA).

NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.



Como conduzir uma Análise Ética

- Identificar e descrever claramente os **fatos**
- Definir o conflito ou dilema e identificar os **valores** de maior ordem envolvidos (liberdade, privacidade, proteção da propriedade, e o sistema da livre empresa)
- Identificar os **interessados e afetados**
- Identificar as **opções** razoáveis **PARA AMBOS**
- Identificar as potenciais **consequências** das opções

8

Princípios éticos Eletivos Análise Ética, o que fazer...

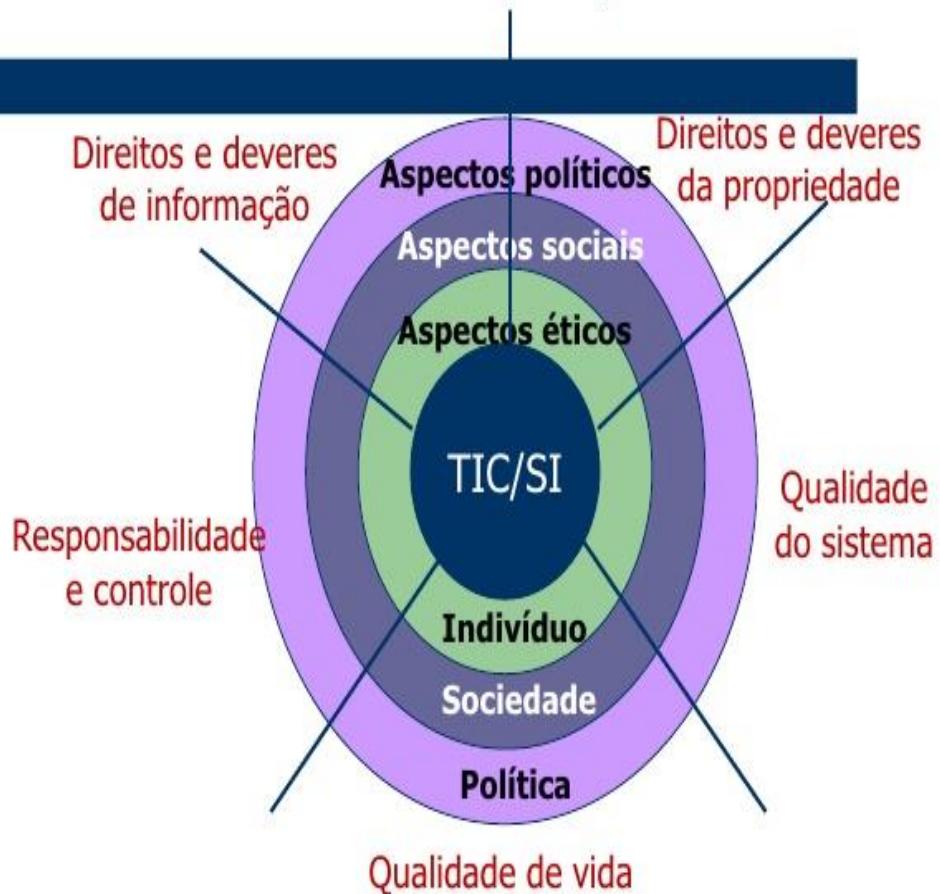
- **Regra de ouro:** Faça aos outros o que gostaria que fizessem a você.
- **Imperativo categórico de Immanuel Kant:** Se uma ação não é correta para todos, não é correta para ninguém.
- **Regra da mudança de Descartes:** Se uma ação não pode ser realizada repetidamente, então não deve ser realizada nunca.
- **Princípio utilitário:** Classifique os valores por ordem de prioridade e entenda as consequências de vários cursos de ação.
- **Princípio de aversão ao risco:** Realize a ação que causar o menor dano ou que tenha o menor custo potencial.
- **Regra ética do “nada é de graça”:** Todos os objetos, tangíveis ou intangíveis, pertencem a seu criador, que deseja uma compensação por seu trabalho ou seja, *no free lunch...* (não roubar dinheiro público / não tirar vantagem dos outros)

9

5 dimensões morais: algumas inquietações

- Deveres e direitos de informação
 - Quais direitos têm os indivíduos e as organizações em relação à sua informação?
 - O quê podem proteger? (Segurança Física e Lógica / Filtro de conteúdo)
 - Quais as suas obrigações?
- Direitos de propriedade
 - como podem ser protegidos os direitos de propriedade numa sociedade digital?
- Responsabilidade e controle
 - Quem deverá prestar contas e ser responsabilizado por danos causados aos direitos individuais e coletivos sobre a informação e a propriedade?
- Qualidade do sistema
 - Quais padrões de qualidade de dados e sistemas devem ser exigidos para proteger os direitos individuais e a segurança da sociedade? (Violação RF)
- Qualidade de vida
 - Quais valores devem ser preservados na sociedade da informação?
 - Quais instituições devem ser protegidas? (ONG's, Clubes, Governos)
 - Quais valores e práticas culturais devem ser suportadas?

**AS RELAÇÕES ENTRE QUESTÕES ÉTICAS, SOCIAIS
E POLÍTICAS NA SOCIEDADE DA INFORMAÇÃO: 5 dimensões morais**



ALGUNS DILEMAS ÉTICOS DO MUNDO REAL

- GM(Montadora) / GMAC(Banco) / EDS(Sistemas):
 - Eliminaram 450.000 postos de trabalho ao redor do mundo; GM: 250.000 / GMAC:50.000 / EDS:200.000 – 7000 posições apenas no Brasil. (Fusão e custos globais – Transição para India)
- Computer Associates International:
 - Demitiu 10 funcionários: E-mails ilícitos
- Xerox Corporation:
 - Demitiu 40 funcionários: Internet
- Detran:
 - Alteração no BD Oracle – Demissão por justa causa

12

OS DESAFIOS DA INTERNET À PRIVACIDADE

- Cookies: Arquivos minúsculos depositados no disco rígido dos visitantes; que rastreiam e monitoram suas visitas a sites.
- O que os Cookies fornecem..
 - informação pessoal registada no site pelo próprio utilizador
 - informação pessoal recolhida por outras ferramentas de monitorização da Web
 - informação pessoal recolhida de forma off-line

13

Desafios da Internet na privacidade

:: Soluções técnicas

FIGURE 5-3 How cookies identify Web visitors.

Cookies are written by a Web site on a visitor's hard drive. When the visitor returns to that Web site, the Web server requests the ID number from the cookie and uses it to access the data stored by that server on that visitor. The Web site can then use these data to display personalized information.



1. The Web server reads the user's Web browser and determines the operating system, browser name, version number, Internet address, and other information.
2. The server transmits a tiny text file with user identification information called a cookie, which the user's browser receives and stores on the user's computer hard drive.
3. When the user returns to the Web site, the server requests the contents of any cookie it deposited previously in the user's computer.
4. The Web server reads the cookie, identifies the visitor, and calls up data on the user.

OS DESAFIOS DA INTERNET À PRIVACIDADE

- **Bugs Web:** Arquivos gráficos minúsculos embutidos em mensagens de e-mail ou páginas web (Eles transmitem informações sobre o usuário e a página que está sendo examinada a um computador de monitoração).
- **Opção de retirada:** Permite a coleta de informações pessoais do consumidor até quando este determinar, especificamente, que esses dados não devem ser coletados.
- **Key Logger:** Script enviado via email ou site que grava digitação do usuário e envia as informações para atacante remoto.

15

- **Opção de adesão:** Proíbe uma empresa de coletar quaisquer informações pessoais do consumidor até que este aprove, especificamente, a coleta e a utilização das informações.

➤ SOLUÇÕES TÉCNICAS

- **P3P(Projeto Plataforma para Preferências de Privacidade):** Habilita a comunicação automática de políticas de privacidades entre um site de e-commerce e seus visitantes;
- Da ao usuário maior liberdade para selecionar o nível de privacidade que deseja manter ao interagir com o site web.

16

Diretiva Europeia à Privacidade proteção de dados

- A proteção da privacidade na Europa
 - É muito maior do que nos EUA / Brasil
- A diretiva europeia exige às empresas
 - informar as pessoas quando recolhem dados pessoais;
 - Onde e para o quê estes dados serão utilizados
 - Mas e na prática?
 - Caso da DIVEO: RH encaminhando planilha de informes de renda dos funcionários.
- “Informed consent”

Diretiva Europeia à Privacidade proteção de dados

- A proteção da privacidade na Europa
 - É muito maior do que nos EUA / Brasil
- A diretiva europeia exige às empresas
 - informar as pessoas quando recolhem dados pessoais;
 - Onde e para o quê estes dados serão utilizados
 - Mas e na prática?
 - Caso da DIVEO: RH encaminhando planilha de informes de renda dos funcionários.
- “Informed consent”

Desafios da Internet na privacidade

:: Como gerir os cookies..

- Gestor de *cookies*
- Anti Pop-Up / Navegação - InPrivet (IE8)
- Encriptação de mails ou dados
- *Anonymizers (acompanhe via HTTPWATCH)*
 - Proxies de acesso Internet anônimo
 - Impedir/retardar reconhecimento da origem
 - Exemplos
 - <http://www.kproxy.com> (msn / orkut)
 - É também um meio de burlar ISPs e empresas que limitam o acesso..
 - É ético usar esta dica do professor em benefício próprio? ;)

TABELA 5.4**FERRAMENTAS DE PROTEÇÃO À PRIVACIDADE**

Função de proteção à privacidade	Descrição	Exemplo
Gerenciamento de cookies	Bloqueia ou limita a implantação de cookies no computador do usuário.	CookieCrusher do Microsoft Explorer 5 e 6
Bloqueio de anúncios	Controla anúncios que surgem na tela com base no perfil dos usuários e evita que coletam ou enviem informação.	AdSubtract
Criptografia de e-mail ou dados	Disfarça e-mails ou dados de modo que não possam ser lidos.	Pretty Good Privacy (PGP) SafeMessage.com
Garantidores de anonimato	Permite que usuários naveguem pela Web sem serem identificados ou que enviem e-mails anônimos.	Anonymizer.com

Deveres/Direitos de informação

:: questões éticas, sociais e políticas

- **Ética**

- Em quais condições se pode invadir a privacidade dos outros? (Segurança Nacional)
 - Devemos informar às pessoas que estamos espiando-as? (Políticas e procedimentos)

- **Social**

- Expectativas de privacidade (Qual a sua?)

- **Política**

- Estatutos que regem as relações entre os que guardam a informação e os indivíduos.

Deveres/Direitos de propriedade

- “**Trade Secret**”
 - trabalho ou produto intelectual utilizado para um propósito de negócio
 - classificado como um **objeto privado do negócio** porquanto não está baseado em informação pública
- O *software* pode ser um *trade secret*

21

Direitos da Propriedade Intelectual

:: Conceitos

- **Copyright:** Garantia estatutária que protege os criadores de uma propriedade intelectual contra a sua cópia por um mínimo de 70 anos
- **Patente:** Um documento legal que garante ao seu proprietários o exclusivo monopólio das ideias por trás da invenção durante 20 anos
 - Utilizado para garantir aos inventores a recepção de benefícios pela comercialização dos seus inventos
- **Tipos de Produção:** Produto ou técnica / Processo tecnológico / Software

22

Direitos da Propriedade Intelectual

:: Conceitos

- **Propriedade intelectual:** Propriedade intangível criada por indivíduos ou corporações, que são protegidas por Lei.
- **Segredos comerciais:** Obra intelectual ou produto que pertença a empresa, não ao domínio público (O proprietário para manter esse status deve manter funcionários e clientes sob contrato que proíbam a divulgação).
- **Direito autoral:** Concessão regida por lei, que garante a propriedade intelectual ao criador e proíbe a cópia de seu trabalho por outros (isso em um período de 28 anos).

Desafios da Internet sobre os direitos de propriedade

- A Internet foi desenhada para transmitir informação livremente pelo mundo
 - inclusivamente a informação protegida por copyrights
- Caso **napster**
 - cópia livre de música em formato mp3
 - com violação dos direitos de propriedade sobre música protegida
- A maneira em que a informação é apresentada na Web complica esta proteção
 - Quem possui as partes?

24

Deveres/Direitos de Propriedade :: questões éticas, sociais e políticas – 5 dimensões

- **Ética**
 - Proteção da propriedade intelectual de software e música, livros e vídeos digitais.
- **Social**
 - Todos violam estes direitos em maior ou menor grau!
- **Política**
 - Criação de novas medidas de proteção da propriedade intelectual destes produtos

25

Responsabilidade e controle

- Exemplo:
 - 1993, **um raio** cai na EDS em Clifton, NJ e a operação de **5.200 multi-bancos** em **12 redes diferentes** afetando **1 milhão de clientes**. A recuperação tomou **2 semanas**. Entretanto, a rede alternativa só permitia saques de 100\$
 - A EDS tinha um plano de recuperação de desastres mas não tinha uma unidade de backup dedicada
 - Quem paga pelos prejuízos causados?
- Expectativas de infalibilidade do software/hardware ou até DRP.

26

Responsabilidade e controle

:: questões éticas, sociais e políticas

- **Ética**
 - Os indivíduos e as organizações que criam, produzem e vendem sistemas são responsáveis pelas consequências do seu uso?
- **Social**
 - Gera expectativas que deveriam ser permitidas a volta do serviço fornecido pelo SI
- **Política**
 - Debate entre fornecedores de informação e utilizadores dos serviços

27

Qualidade e erros dos sistemas

:: questões éticas, sociais e políticas

● Ética

- Em quê momento o software tem um nível de qualidade aceitável para o seu uso? **PATCH e SP2 Microsoft**

● Social

- Queremos encorajar a expectativa da infalibilidade do software?
- Ou queremos uma sociedade cética que questione o output dos sistemas?
- ou pelo menos uma sociedade informada dos riscos?

● Política

- Desenvolvimento de leis de responsabilidade e accountability

Qualidade de vida

:: igualdade, acesso e fronteiras afetadas pelos SIs

- Velocidade das mudanças
 - reduzido tempo de resposta a concorrência (< DOWNTIME)
- Manutenção das fronteiras
 - família, trabalho e lazer (Tempo disponível para isso)
- Dependência e vulnerabilidade
- O crime digital
 - spamming, hacking, viruses, sniffing, spoofing, fishing, etc..
- Emprego
 - a perda do trabalho pela reengenharia vs novas formas de trabalho
- Igualdade e acesso
 - maiores ou menores distâncias sociais e raciais?
- Saúde
 - L.E.R.(Lesão por Esforço Repetitivo), Síndrome da Tela do Computador e Tecnostress.

29

Ações da gerência

:: um código de ética corporativa

➤ IGUALDADE DE OPORTUNIDADES E ACESSO

- Todos têm oportunidades iguais de participar da era digital?
- Os grupos de defesa do interesse público estão querendo diminuir esse “divisor digital”, disponibilizando os serviços de informação digital.

30

Obrigado!!
esanselmo@gmail.com

OBRA NR. 4

**CEETEPS – CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA
“PAULA SOUZA”
ETEC FERNANDO PRESTES**

TÉCNICO EM INFOMÁTICA

CÓDIGO DE ÉTICA NA INFORMÁTICA

**Sorocaba – SP
2014**

**Luiz Fernando Nº 09
Michel Paiva Nº 12
Silvana Franco Nº 19
Wesley Germano Nº 20**

CÓDIGO DE ÉTICA NA INFORMÁTICA

Pesquisa referente ao código de
ética na área da informática para a
Disciplina de ECO.
Professor: Mateus

**Sorocaba-SP
2014**

SUMÁRIO

1. INTRODUÇÃO – O QUE É ÉTICA?.....	4
2. CÓDIGOS DE ÉTICA.....	6
2.1 POR QUE UM CÓDIGO DE ÉTICA?.....	8
3. REGULAMENTAÇÃO DA PROFISSÃO.....	10
4. CONCLUSÃO.....	13
5. BIBLIOGRAFIA.....	15

1. INTRODUÇÃO – O QUE É ÉTICA?

A evolução das técnicas computacionais e o crescimento da popularidade da informática na sociedade tem causado o aumento das discussões sobre ética na computação. Mas o significado da palavra **ética** tem confundido muitos ao ser comparado com o significado de **moral**. Moral é aplicada quando se quer ditar regras de conduta a uma pessoa ou a um grupo. Ética é a ciência que estuda as várias morais, comparando-as e verificando se são legítimas, se não são influenciadas, se realmente são modelos de referência para a tomada de decisões.

A ética se baseia muito no bom senso pessoal para estabelecer se uma moral atende às necessidades e desejos de um grupo/pessoa sem agredir os direitos da sociedade em volta. Essa atitude subjetiva tem criado controvérsias, pois toda ciência baseada no senso comum é duvidosa, porque cada pessoa pensa de um jeito e o que é "certo" para alguém pode ser "errado" para outrem. E como é baseada nas morais, que são bem variadas, a ética não é imutável, variando com o lugar, a época e fatores externos, deixando de ser uma ciência 100% confiável.

Para se ter uma idéia da variabilidade dos conceitos morais e éticos e para exemplificar a diferença entre eles, analisemos o caso da pirataria de software. A moral que é oficializada pela maioria das leis determina que este ato é anti-ético em todos os seus sentidos, enquanto em uma comunidade que apóia o software livre, a idéia de copiar programas jamais é associada à ilegalidade. Mas a moral que é adotada pela maior parte das pessoas é a que divide a pirataria em duas modalidades: uma mais tênué, que envolve empréstimos inofensivos de cds a amigos e uso remoto de programas em uma pequena rede e outra forma mais criminal, que visa o lucro à custa do prejuízo do "proprietário intelectual" do programa.

A ética é quem define se cada uma das morais é válida no ambiente em que atuam, determina se são boas fontes de aconselhamento na hora de fazer um escolha do tipo “copiar ou não copiar?” e verifica se não está havendo alguma influência política ou social de alguma organização ou grupo no estabelecimento destes conceitos. Num futuro próximo, talvez as opiniões sejam outras e fatores tecnológicos, jurídicos, etc. podem mudar o ponto de vista ético da situação.

2. CÓDIGOS DE ÉTICA

A maior dificuldade em se falar de ética na computação é que, como qualquer pessoa de qualquer área de estudo pode estudar informática, inclusive pessoas que não fazem qualquer curso superior, fica difícil de se criar uma regulamentação que todo profissional do setor deve seguir ao se deparar com situações em que é preciso julgar o que é correto e o que é incorreto. Não existe um código de ética oficial, como na Medicina ou no Direito, mesmo porque se houvesse, não abrangeria a todos os praticantes da área, atingindo apenas àqueles que tomassem conhecimento através de disciplinas da graduação, talvez eletivas.

Não sendo a profissão regulamentada, não existem órgãos fiscalizadores ou estruturas sindicais que zelam pelo bom desempenho do profissional. Em alguns países, foram criadas sociedades que tentam suprir essa necessidade, como a ACM (Association for Computer Machinery), que possuem inclusive códigos de ética, entretanto a punição pela não-obediência às diretrizes geralmente limita-se ao banimento da associação, sendo o comportamento dos membros praticamente determinado pela consciência individual.

No Brasil existe a SBC (Sociedade Brasileira de Computação), que exerce grande influência na comunidade da área de informática, uma vez que a maioria dos professores universitários da área são seus associados, ajudando a formar profissionais qualificados. Porém a SBC não possui um código de ética para orientar seus membros, apenas um projeto baseado no código da ACM e da British Computer Society. A SUCESU é outra entidade atuante no ramo, mas que também não possui um código destinado a indivíduos por ser composta basicamente por instituições. O Instituto para Ética da Computação criou um pequeno código de conduta que ficou conhecido como "Os Dez Mandamentos para Ética na Informática", transscrito a seguir:

1. Você não deverá usar o computador para produzir danos em outra pessoa;
2. Você não deve interferir no trabalho de computação de outra pessoa;
3. Você não deve interferir nos arquivos de outra pessoa;
4. Você não deve usar o computador para roubar;
5. Você não deve usar o computador para dar falso testemunho;
6. Você não deverá usar software pirateado;
7. Você não deverá usar recursos de computadores de outras pessoas;
8. Você não deverá se apropriar do trabalho intelectual de outra pessoa;
9. Você deverá refletir sobre as consequências sociais do que escreve;
10. Você deverá usar o computador de maneira que mostre consideração e respeito ao interlocutor.

Aos profissionais formados nos novos cursos de engenharia da computação é dada a possibilidade de se afiliar ao CREA (Conselho Regional de Engenharia, Arquitetura e Agronomia) e, com isso adotar suas normas e o Código de Ética do CONFEA (Conselho Federal de Engenharia e Agronomia). Entretanto, as recomendações desse código não são específicas para a informática, negligenciando temas de repercussão na atualidade, como a privacidade, confidencialidade, propriedade, etc. Criado há mais de vinte anos, este guia visava esclarecer dúvidas éticas no campo da engenharia tradicional, não sendo propriamente destinado a trabalhadores de computação, a não ser que passe por uma atualização para abranger essas novas necessidades.

Acredita-se que os profissionais da área de informática se comportam ora como engenheiros ou arquitetos, construindo ou supervisionando a elaboração de especificações, ora como contadores, analisando financeira e comercialmente o mercado antes de iniciar o desenvolvimento de softwares e sistemas. Sendo assim, o Código de ética dos Contabilistas também pode ser uma boa fonte de consulta, principalmente para consultores, peritos, auditores, proprietários de

micro-empresas de informática ou para qualquer pessoa que trabalhe ou se relacione com pessoas da área contábil.

2.1 POR QUE UM CÓDIGO DE ÉTICA?

Um código de ética é formado basicamente de diretrizes voltadas para seis aspectos de obrigações éticas:

- para com a sociedade em geral, zelando pelo bem estar de todas pessoas sem qualquer discriminação, visando construir ou manter uma sociedade livre, justa e solidária;
- para com os empregadores, usualmente quando estes não tem conhecimento na área e o supervisionamento técnico do trabalho é todo realizado com base na confiança;
- para com os clientes, se estes forem leigos como no caso dos empregadores, quando o profissional é um prestador de serviços ou consultor;
- para com a sociedade de classe, no caso, a comunidade computacional, com o intuito de proteger os interesses da associação criadora do código e de seus membros.
- para com os colegas de profissão, que compartilham os mesmos interesses e colaboram para o bem estar de todos.
- para com a profissão em geral, com o objetivo de não difamar os outros trabalhadores da área e evitar que a profissão não seja mal-vista pelo restante da sociedade.

Não é raro acontecer de alguma dessas obrigações entrar em conflito com outra, sendo necessário que o bom senso decida a prioridade entre elas. Geralmente a obrigação com a profissão tem prioridade sobre a com os colegas e a obrigação para com a sociedade em geral é superior a todas as outras em praticamente todos os contextos.

Um código de ética consiste também em um conjunto de diretrizes que esclarecem as circunstâncias em que cada um dos mandamentos se aplicam. Ou pode haver um conjunto de casos para estudo comparativo, auxiliando na resolução de novas situações. O código, junto com seus suplementos, serve como base para julgamento de casos mais complexos, utilizando princípios éticos que derivam de diretivas mais gerais.

A necessidade de um código de ética se mostra quando nos deparamos com uma divergência de opiniões devido aos envolvidos em uma ocorrência se acharem ambos prejudicados e protegidos pelos preceitos éticos, às vezes mal interpretados. Nestes casos, uma análise detalhada dos mandamentos acompanhada de bom senso de partes neutras podem definir a atitude correta nesses casos.

Não há dúvida da importância da ética para o desenvolvimento da humanidade, pois sem um conjunto de princípios humanitários visando o bem comum, as civilizações já teriam se auto-destruído. Mas um código de ética não é o suficiente para o progresso moral de um povo. É preciso que haja uma concordância mínima entre as nações sobre princípios básicos como justiça, igualdade, dignidade, cidadania, solidariedade, etc. para que estes possam ser postos em prática. E isso ainda não é o bastante. É necessário que cada cidadão assimile estes princípios e incorpore-os na prática diária, zelando pelo seu cumprimento.

3. REGULAMENTAÇÃO DA PROFISSÃO

Como os códigos de ética não dão garantia nenhuma da obediência a seus estatutos, tem se pensado em regulamentar as profissões da área de computação, criando um conselho com autoridade para fiscalizar e penalizar aqueles que não cumprirem seu regulamento. Por outro lado, muitos não concordam com a criação de tal instituição e essa divergência tem causado debates calorosos entre defensores das duas ideias.

No Brasil, a SBC mostra-se a maior defensora da não-regulamentação defendendo a liberdade do exercício do profissionalismo sem necessidade de submissão a instituições que só burocratizariam e limitariam a atuação do profissional em prol de seus interesses. Enquanto a FENADADOS (Federação Nacional dos Empregados de Empresas de Processamento de Dados) é sua maior rival, defendendo a criação do CONIN (Conselho Nacional de Informática) e de projetos de lei pra regulamentação da profissão chamada provisoriamente de "informata".

Os argumentos de cada lado são muito convincentes, embora haja pontos de concordância nas opiniões acerca da qualidade de ensino e da criação de um código de ética. Entre as argumentações a favor da regulamentação se destacam:

- Os serviços prestados seriam de melhor qualidade.
- Formandos qualificados teriam emprego garantido.
- A ética profissional seria melhor estabelecida.
- Trabalhadores anti-profissionais ou anti-éticos não teriam vez no mercado.
- Um conjunto de normas técnicas seria criado.
- Unificação das variadas profissões da área e nomenclatura apropriada.
- Fim da separação entre os profissionais de computação e demais profissões regulamentadas.

- Criação de um conselho de classe específico com normas mais cabíveis pra área.

A oposição a essas alegações se dá com as seguintes justificativas:

- Um diploma não é garantia de qualidade, assim como a falta de um não significa falta de profissionalismo.
- Há uma grande dificuldade em definir quem exerce a profissão devido a grande quantidade de programadores informais que atuam em outras áreas.
- Seria estabelecido um currículo mínimo, o que num contexto dinâmico como o da informática, se tornaria obsoleto rapidamente.
- A velocidade das mudanças no setor dificultaria a definição das atribuições do profissional e a legislação não conseguaria acompanhá-las com seu ritmo lento.
- A sociedade já possui leis suficientes pra punir um mal profissional da informática.
- Normas Técnicas e um código de ética podem ser estabelecidos sem a necessidade de regulamentação da profissão.
- Há necessidade de testes de qualidade apenas para os "produtos", os softwares, não para os profissionais.
- Devido a reserva de mercado, bons profissionais ficariam fora do mercado.
- A fiscalização só pode ser realizada por outros integrantes da classe.
- Aumento do preço dos produtos produzidos pelos "profissionais qualificados".
- A necessidade de registro para exercer a profissão criaria reserva de mercado para profissionais estrangeiros, auxiliando o crescimento do desemprego no Brasil.
- As normas técnicas não poderão dar garantia de qualidade total aos programas, pois a natureza destes não permite que os programadores

assumam total responsabilidade pelos problemas (bugs) que venham a apresentar.

4. CONCLUSÃO

Apesar de tantas objeções, a SBC assume que a regulamentação da profissão é inevitável, e cedo ou tarde algum projeto de lei, como o do deputado Silvio de Abreu (PDT/MG), que regulamenta a profissão de analista de sistemas, será aprovado. Portanto, ela toma a frente, criando sua própria proposta bem ao estilo do copyleft do projeto GNU, dando ampla liberdade para o exercício profissional, utilizando de um artifício legal e citando inclusive artigos da Constituição para justificar sua posição. Mas não apóia a criação de qualquer conselho para proteger seu código.

Com ou sem regulamentação, a sociedade necessita de um conjunto de normas para serem seguidas não só pelos profissionais de informática como por qualquer aventureiro que se atreva a experimentar o poder da computação e verificar o quão frágeis são as pessoas frente ao computador. Esse normativo precisa ser dinâmico para acompanhar a constante aceleração das mudanças que ocorrem no contexto da ética na informática.

Seguir um código de ética pode ser essencial para assegurar nossos direitos e suprimir de situações adversas. No âmbito empresarial temos empresas que instituem suas próprias regras a seus funcionários de TI, que muitas vezes instituída em um contrato, onde pode ser assimilada a política de segurança da empresa. A informática como sabemos é estendida para diversos ramos, então em razão disso a falta de um código de ética na informática, faz com que seguimos códigos de outra profissão, onde podemos ter a descaracterização de nosso ofício.

Essas normas se existissem se entenderiam ao setor comercial e autoral, onde a pirataria (criação de conteúdo sem autorização) poderia ser minimizada e até extinta, os direitos autorais poderiam não ser mais deferidos, o que faria com que as produtoras obtivessem mais lucros, mas vendo por outro lado não abrangeira a camada mais pobre.

A criação de normas devem ser feita em conjunto com as demais profissões para abranger e caracterizar o ofício do profissional de TI, onde certas normas poderiam formar uma sociedade até mais conscientizada com a questão da pirataria.

5. BIBLIOGRAFIA

1. Masiero, Paulo César. *Ética para Profissionais em Computação*. São Paulo, 1994. Disponível em <www.uri.com.br/~mzp/cursos/ETICA.htm>. Acesso em 02/08/2003.
2. Yuka, Cristiane. *Ética e Profissionalismo*. Recife, 2001. Disponível em <planeta.terra.com.br/arte/yuka/etica.htm>. Acesso em 04/08/2003.
3. *Ética: uma visão sobre Privacidade e Pirataria na Informática*. Vitória, 2002. <www.inf.ufes.br/~fvarejao/cs/etica/etica01.htm>
4. Schneider, Sérgio de Mello. *Posição da SBC em Audiência Pública sobre a Regulamentação da Profissão*. São Paulo, 1999. Disponível em <<http://www.sbc.org.br/profissao/posicao.html>>. Acesso em 05/08/2003.

ANEXOS

CONTROLE DE ACESSO

Define quem pode ou não obter acesso a alguma informação ou local onde possam haver informações sigilosas.

Existem várias maneiras de definir esses acessos:

- Reconhecimento de íris, voz, face, expressões;
- Biometria;
- Senha;
- Cartão com chip/Token;

CONTROLE DE ACESSO

O Controle de acesso tem ligação direta com a Autenticação.



VOZ



Íris



Mão



Retina



Rosto



Impressão



Plano de Segurança

• Combate a Ataques e Invasões

1. Antivírus

- Programas de computador que previnem, descobrem e destroem vírus que podem contaminar o computador.

Norton
from symantec

AVG

PANDA
SECURITY



BULLGUARD

webroot

TREND
MICRO

McAfee



KASPERSKY



Recomendações Finais para Pais e Filhos

- Deve conversar com o seu filho ou filha para preservar a sua privacidade e a dos amigos (não publicando fotografias, imagens ou outras informações que possam ser constrangedoras);
- Orientar os filhos para conversar com um adulto caso receba ameaças, provocações ou algum conteúdo inconveniente;
- Recomendar aos filhos para não fazer intimidações, nem manter-se em silêncio caso saiba que outra pessoa ou colega está a ser intimidado;
- Ser educado – tratar mal alguém pode dar início a uma perseguição ou ao **cyberbullying**.