

SSC0531 – Gestão de Sistemas de Informação

SI na Sociedade: *Segurança, Qualidade e Ética*

Simone Senger Souza

srocio@icmc.usp.br

ICMC - 2019

SI na Sociedade

- SI fazem parte da vida das pessoas
- SI fazem parte da organização
 - É parte dos principais ativos de uma organização
- Podem mudar a maneira de realizar atividades
 - Novos processos organizacionais, novos tipos de negócios
 - ...

SI na Sociedade

- Impactam na vida das pessoas
 - Soluções mais rápidas e fáceis
 - Maior quantidade de informação disponível
 - Novos serviços
- Dependência
- Vulnerabilidade
- Privacidade
- Confiabilidade

Segurança em Sistemas de Informação

- Vulnerabilidade dos SIs
 - destruição, erros e uso indevido
- Valor empresarial da segurança nos SIs
- Tecnologias e ferramentas disponíveis proteger a informação



Desastre 11 de setembro de 2001



No contexto de SI, o que aprendemos com o
11 de setembro?

Desastre 11 de setembro de 2001

- Nem tudo está **sob controle**
- Empresas inteiras destruídas
- Gestores de Segurança mantinham backup dos DataCenter.



Backups na Torre ao lado!

Ou seja, com a destruição das Torres, os backups que continham a vida da empresa, desapareceram.

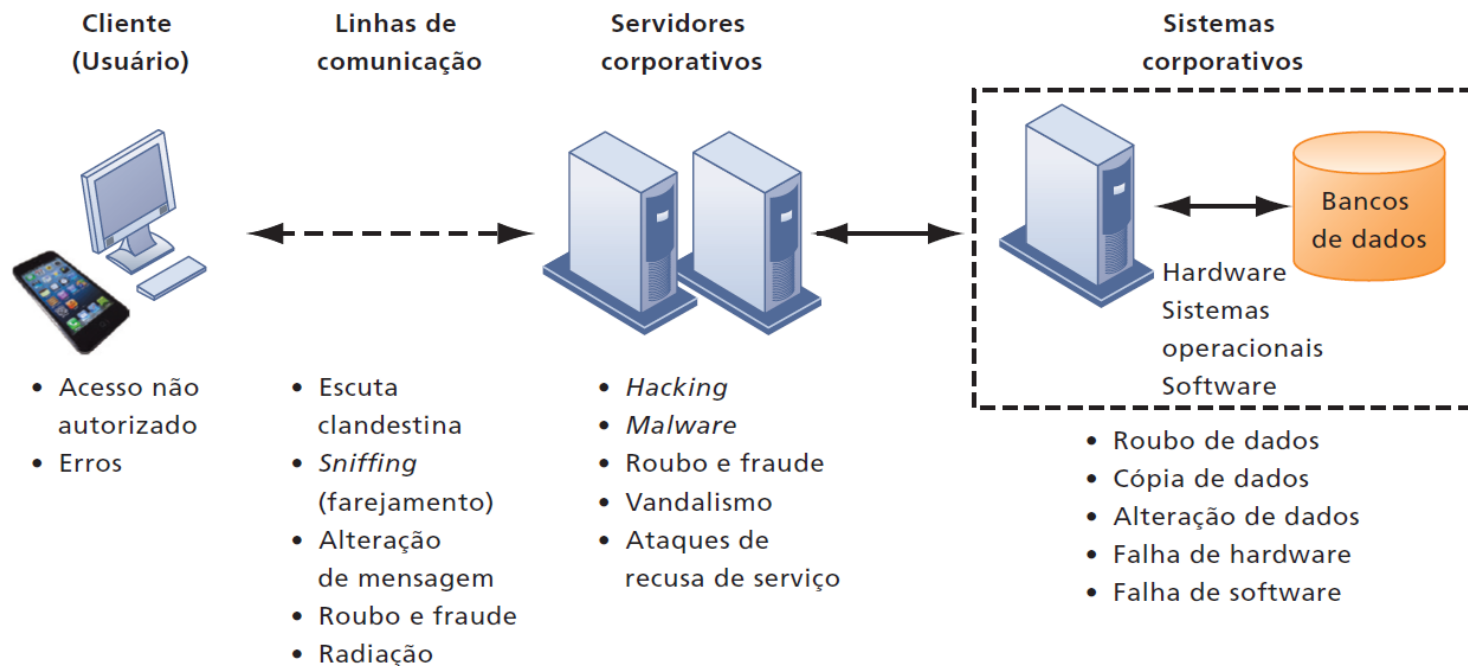
Desastre 11 de setembro de 2001

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

Vulnerabilidade e uso indevido

➤ Formato eletrônico X formato manual.

➤ Desafios contemporâneos:



Vulnerabilidade e uso indevido

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

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



Vulnerabilidade e uso indevido

➤ Ameaças externas:

- Software mal intencionado
- Crimes de informática

➤ Ameaças internas

- Funcionários (erros nas entradas de dados nos sistemas)
- Defeitos nos sistemas



Vulnerabilidade – Ameaça externa

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



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

Ameaça interna: Bugs no sistema

How people reacts differently to a single word.

"Bug"



Tester



Developer



Manager

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

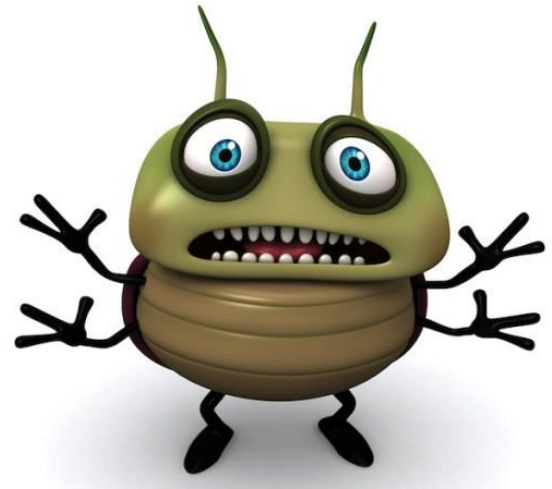
Boeing 737 MAX 8 2018 e 2019



- Jato mais vendido da Boeing, dois acidentes fatais, Etiópia e Indonésia, somam 346 mortos.
 - Custo da fatalidade para a Boeing: US\$ 1 bilhão
 - Modelo continua aterrado
- Por que os aviões caíram?
 - Um sistema automático recebeu leituras incorretas de sensores e forçou o nariz do Boeing 737 MAX 8 para baixo contra vontade dos pilotos. O capitão usava os controles para elevar o nariz do avião, mas um sistema antipane automático o empurrou para baixo.
 - Suspeita de sensores defeituosos e falha em um sistema automático de segurança
 - Os pilotos ficam sobrecarregados durante o voo: *“se múltiplos defeitos ocorrem todos de uma vez, qual deve ser priorizado?”*

Por que essas falhas ainda ocorrem?

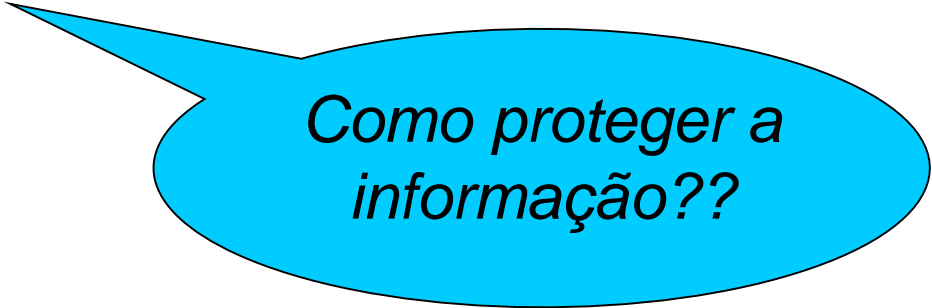
Poderiam ser evitadas?



Falhas comprometem a **qualidade** dos sistemas

Vulnerabilidade

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



*Como proteger a
informação??*

Valor empresarial da segurança e controle

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

Como estabelecer uma estrutura para segurança e controle

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

Como estabelecer uma estrutura para segurança e controle

- Exemplo: Avaliação de risco para um sistema de processamento de pedidos online

- Riscos potenciais?
 - Falta de energia elétrica
 - Erro de usuário
 - Apropriação indevida
 - ...

- Qual a probabilidade de ocorrência de cada risco?
- Qual o impacto de cada risco?
- Como evita-los ou mitiga-los?

Plano de recuperação de desastres e plano de continuidade dos negócios

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

Tecnologias e ferramentas para garantir a segurança em SI

- **Gestão de identidade**

- Autenticação
- Autenticação biométrica

- **Firewall**

- **Sistemas de detecção de intrusão**

- **Software antivírus**

- **Criptografia**

- **Certificados digitais**

Controles Gerais – Norma de Segurança

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

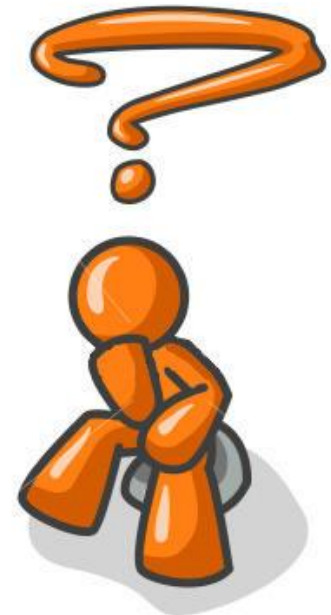
Controles Gerais – Norma de Segurança

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



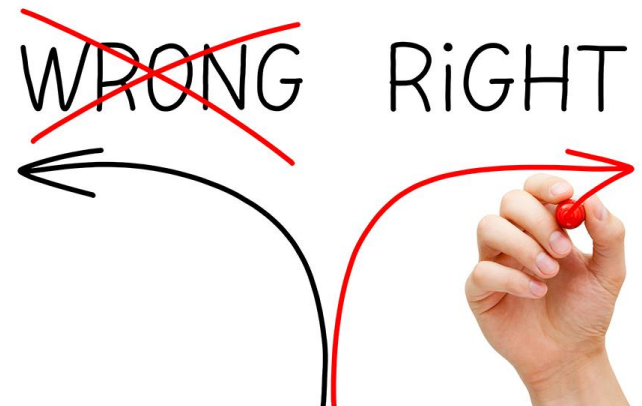
SI na Sociedade

- Conclusão até aqui:
 - SI precisa estar seguro e funcionar o mais correto possível!
- Além disso:
 - Impacto do uso correto de SI
 - O que é **ético** fazer com o apoio de SI?



Ética

Ética refere-se aos princípios do que é **certo e errado** que os indivíduos, **agindo como seres moralmente livres**, usam para **tomar as decisões** que guiam o seu comportamento.



Tendências em TI que suscitam questões éticas, sociais e políticas

- Capacidade de computação dobra a cada 18 meses (*Lei de Moore*) – dependência dos dados
- Custos de armazenagem de dados reduzindo rapidamente - privacidade
- Progressos nas técnicas de análise - privacidade
- Avanços das redes e da Internet
- Determinação de perfil
- Detecção de relações não óbvias (*Nonobvious relationship awareness* – NORA)

Ética e SI

- SI provocam novas questões éticas:
 - Criam oportunidades de mudanças sociais intensas (progresso social);
 - Pode ser usado para cometer crimes ou ameaçar comportamentos sociais importantes para a humanidade
 - Responsabilidade pelas consequências dos SI
 - ...

TIM RADAR

SEU FUNCIONÁRIO SEMPRE NO LUGAR CERTO.

Acompanhe a localização aproximada de seus funcionários com o TIM Radar, o novo aplicativo da TIM para melhorar a gestão da sua empresa.

APENAS

R\$ 9,90 /MÊS

POR FUNCIONÁRIO

Ética na Sociedade da Informação

- Conceitos básicos:
 - responsabilidade
 - prestação de contas (*accountability*)
 - obrigação de indenizar (*liability*)
- Análise ética:
 - identificar envolvidos, mapear as controvérsias e conflitos, grupos interessados/implicados, alternativas, consequências
- Códigos de conduta profissional:
 - ACM (Associação de Máquinas de Computação)
 - IEEE
 - SBC – Sociedade Brasileira de Computação

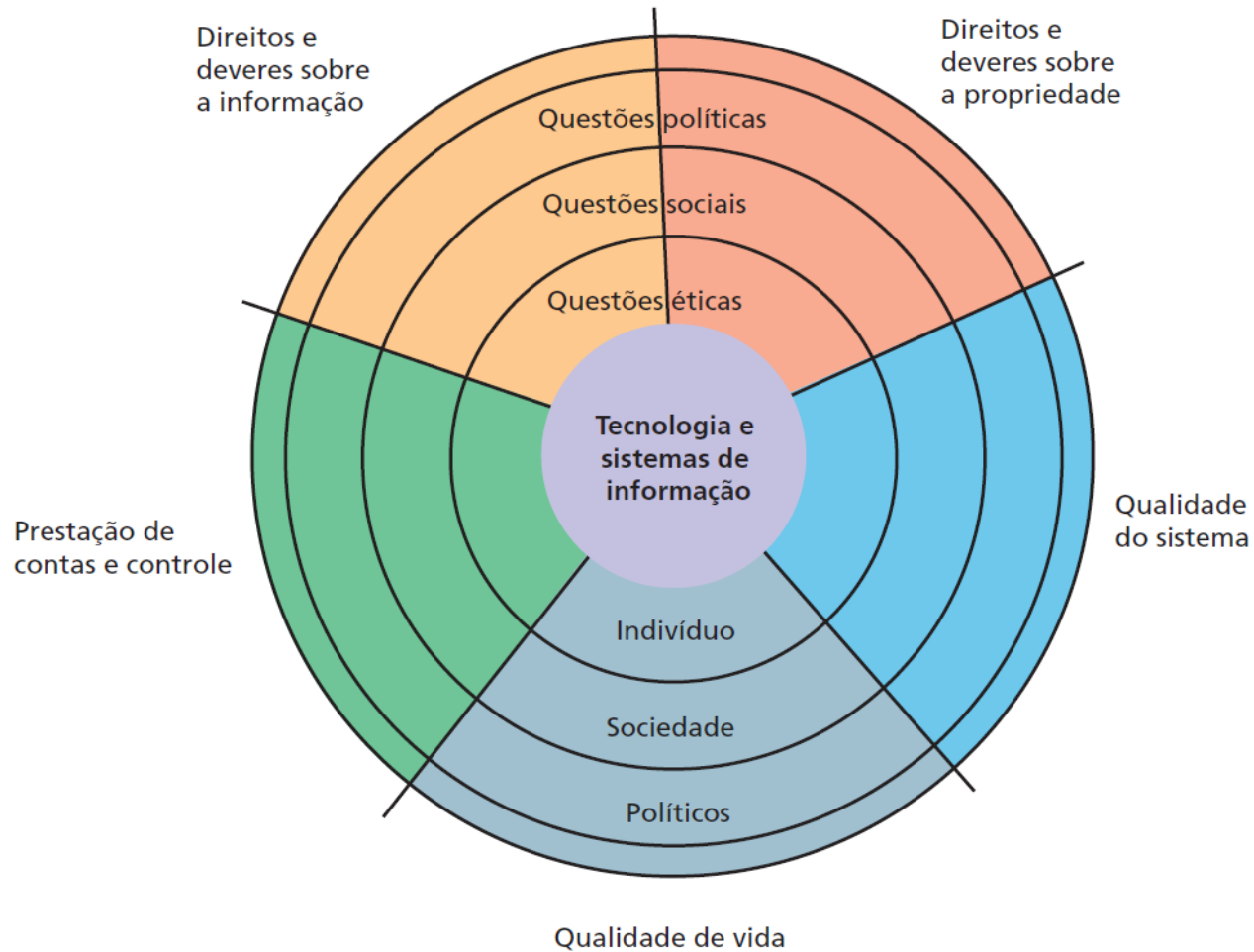
Alguns mandamentos do código da ACM

- Esforçar-se para concluir com a mais alta qualidade todos os processos e produtos do trabalho profissional.
- Adquirir e manter competência profissional.
- Conhecer e respeitar as leis existentes relativas ao trabalho profissional
- Honrar contratos e responsabilidades assumidas.

Alguns mandamentos do código da ACM

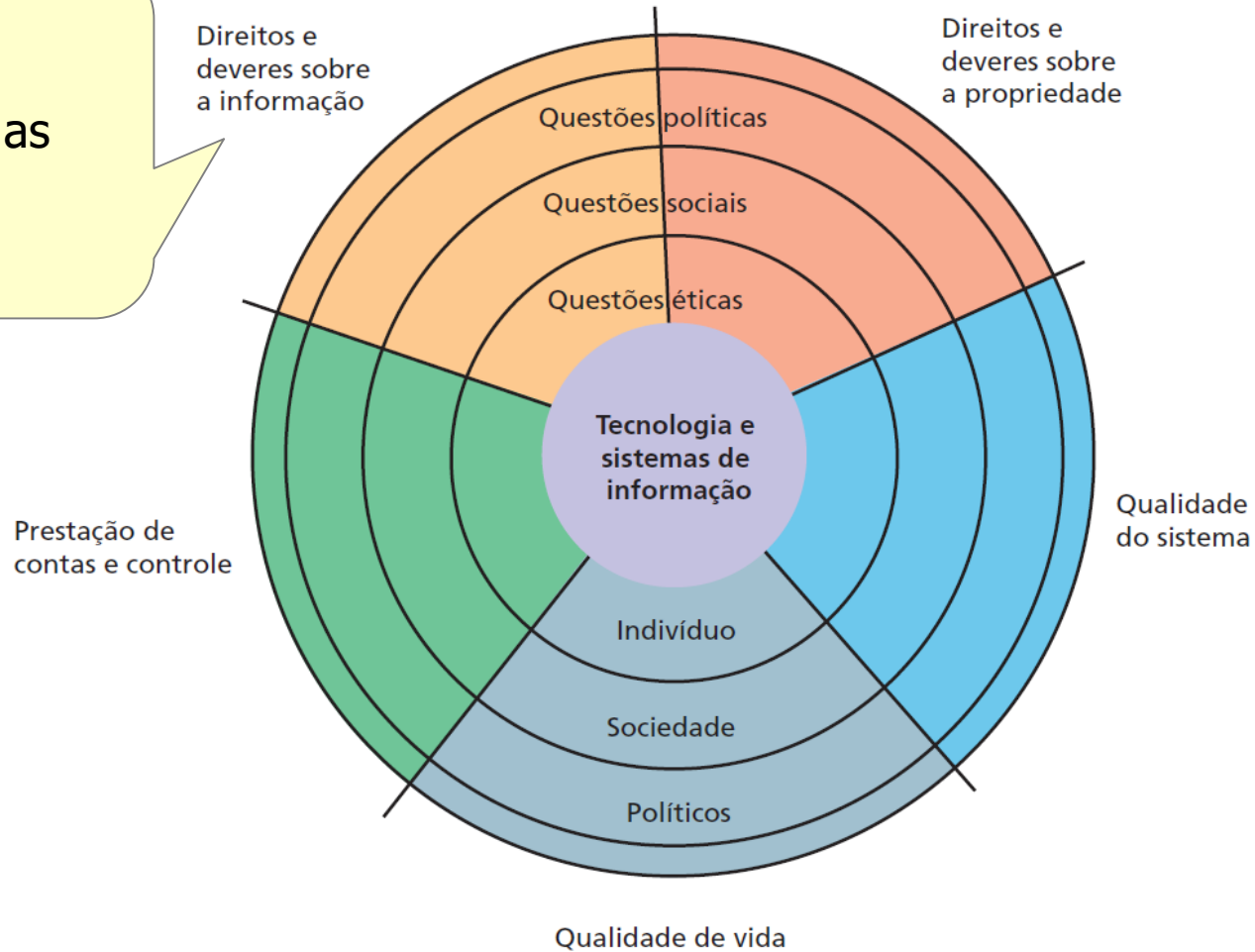
- Acessar recursos computacionais e de comunicação somente quando autorizado.
- Respeitar a privacidade de terceiros
- Honrar a confidencialidade
- Respeitar os direitos de propriedade

Questões éticas, sociais e políticas



Questões éticas, sociais e políticas

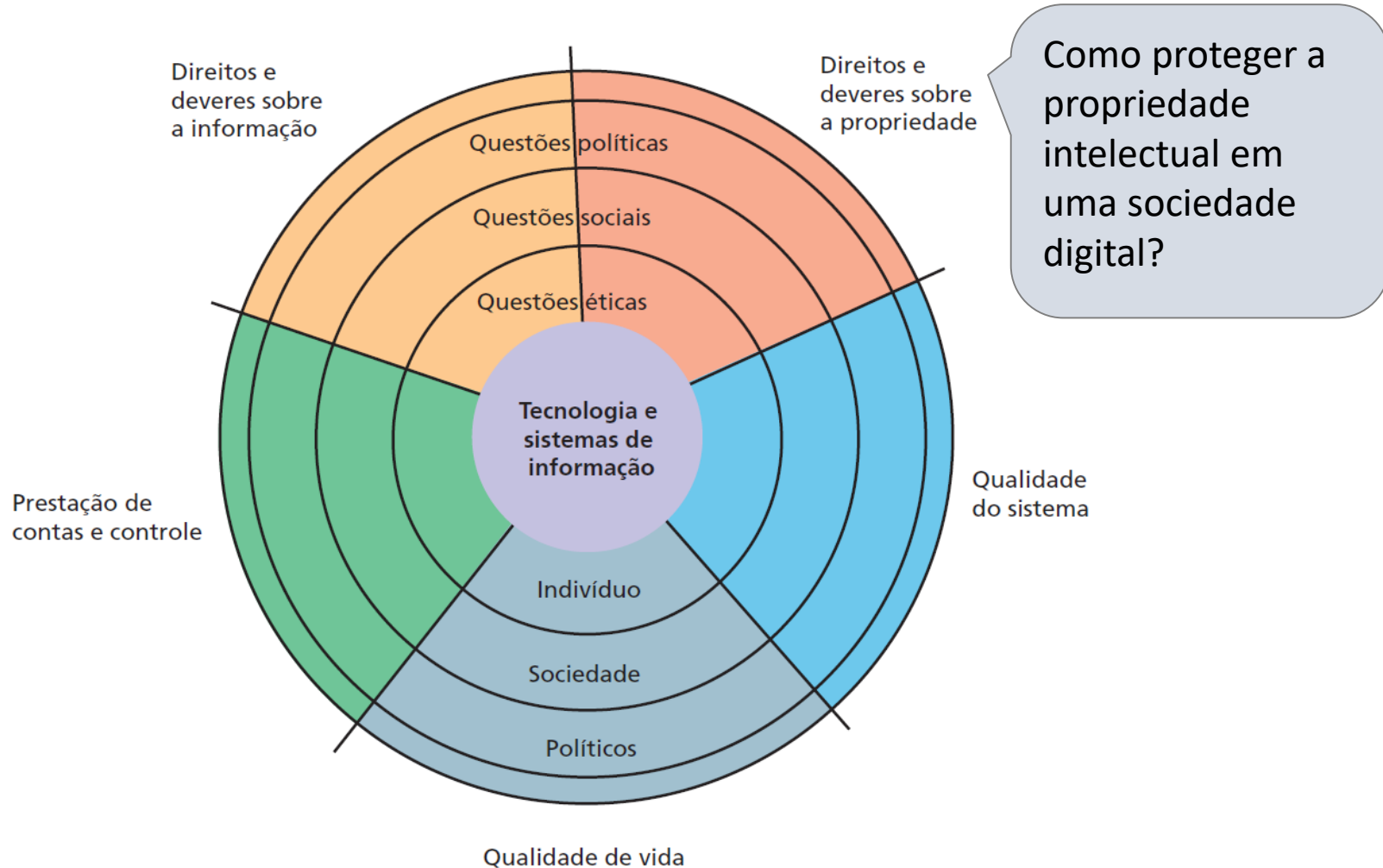
Que direito sobre a informação as empresas possuem?



Direitos sobre a Informação: Privacidade e Liberdade na Era da Internet

- Privacidade:
 - direito dos indivíduos de não serem incomodados (livres de vigilância)
- Desafios da Internet à privacidade
 - Facebook, Google - rastreamento
 - Cookies, spywares

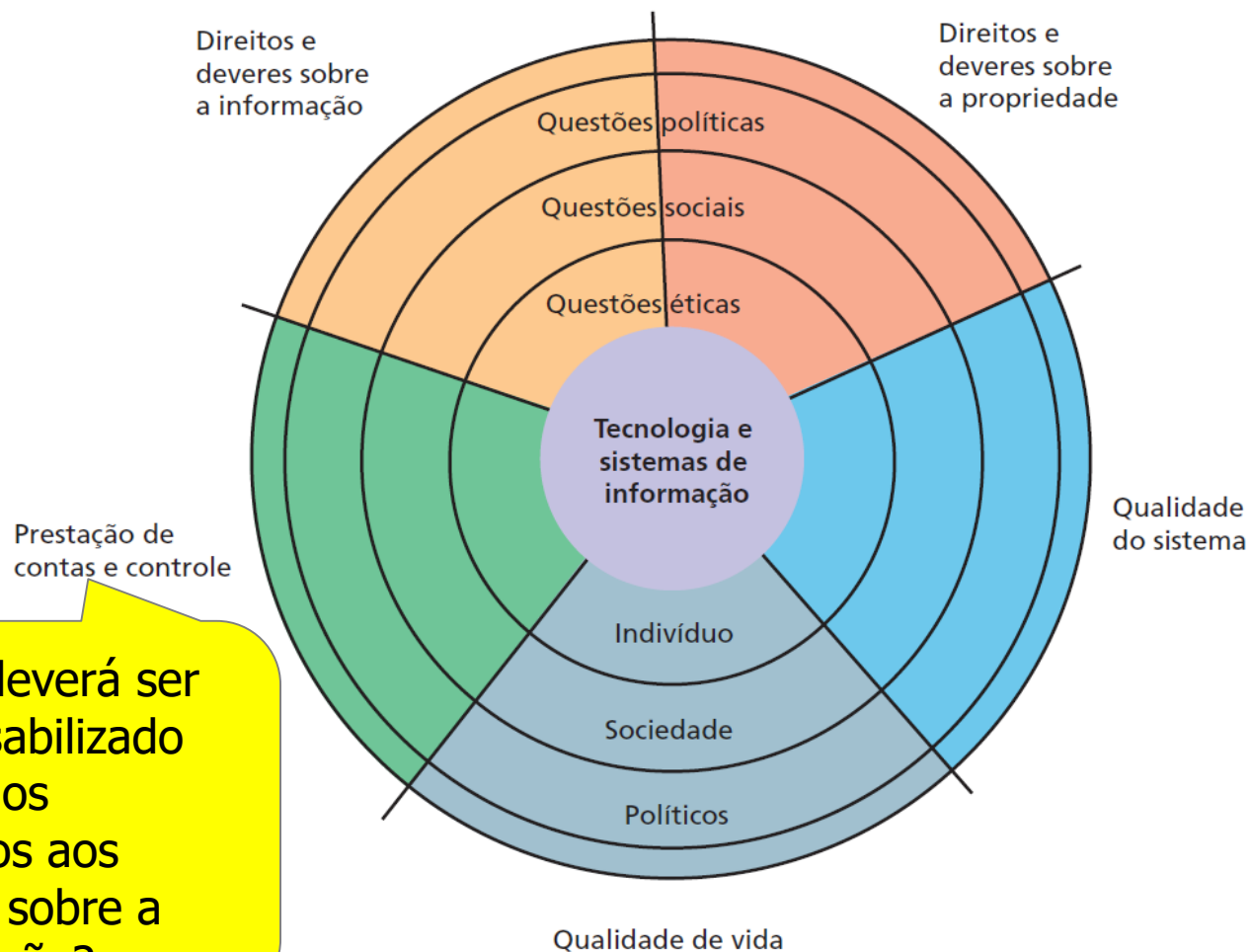
Questões éticas, sociais e políticas



Proteção à Propriedade Intelectual

- Leis do segredo comercial:
 - Software que contenham elementos ou procedimentos inusitados e exclusivos
- Direito autoral
 - Protege contra a cópia inteira de um software, mas manifestações semelhantes são permitidas
 - Ex Apple e Microsoft e janelas superpostas
- Patente
 - Programas podem ser parte de um processo patenteável (ainda não vigente)
 - Registro de software
 - Ex Apple e Samsung – iPhone e Ipads

Questões éticas, sociais e políticas

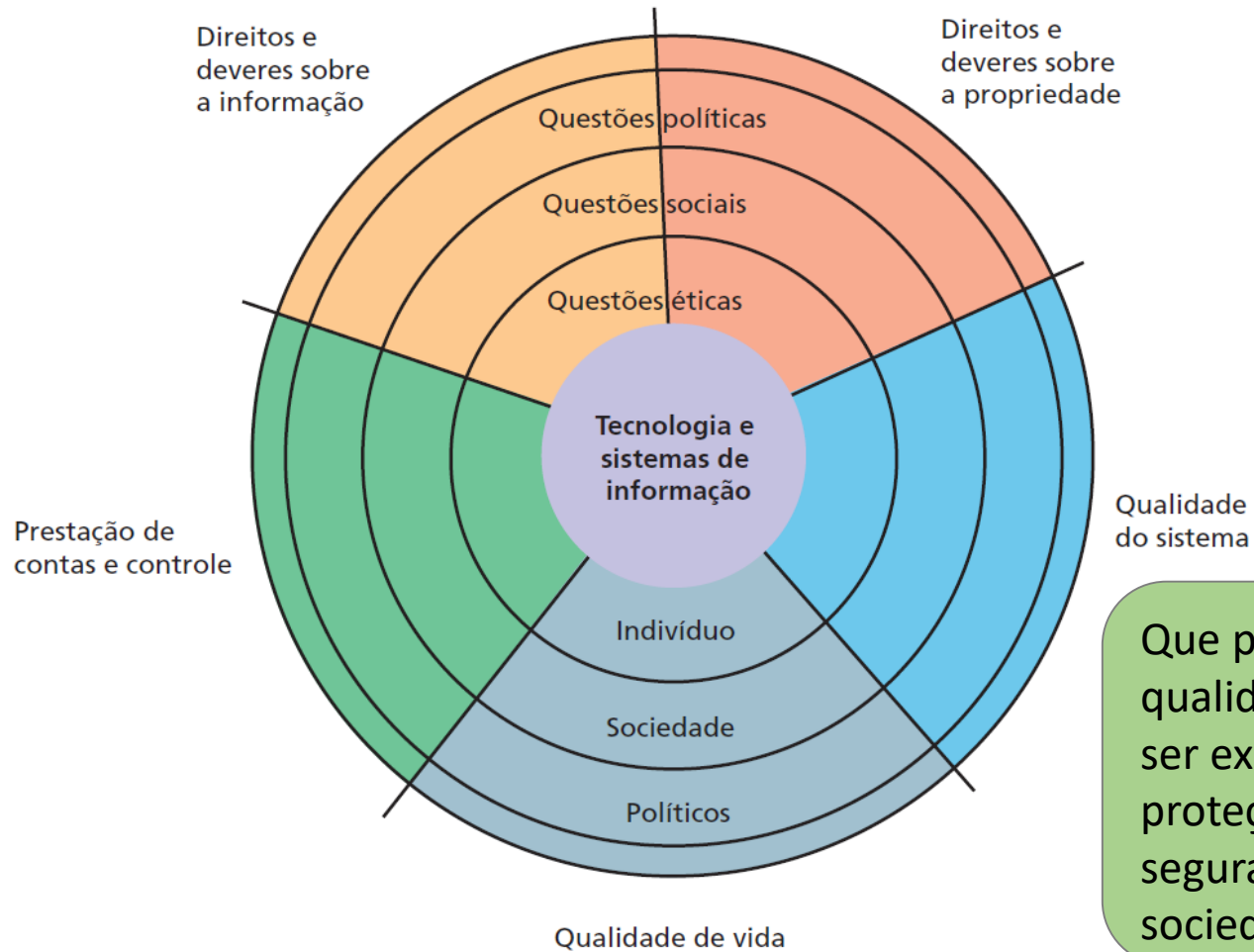


Quem deverá ser responsabilizado por danos causados aos direitos sobre a informação?

Prestação de contas, obrigação de indenizar e controle

- Quem é responsável por danos resultantes de máquinas controladas por software?
 - Ariane 5, Challenger, Máquina de Radiação, Aeroporto alemão ...
- E por sistemas autônomos?

Questões éticas, sociais e políticas

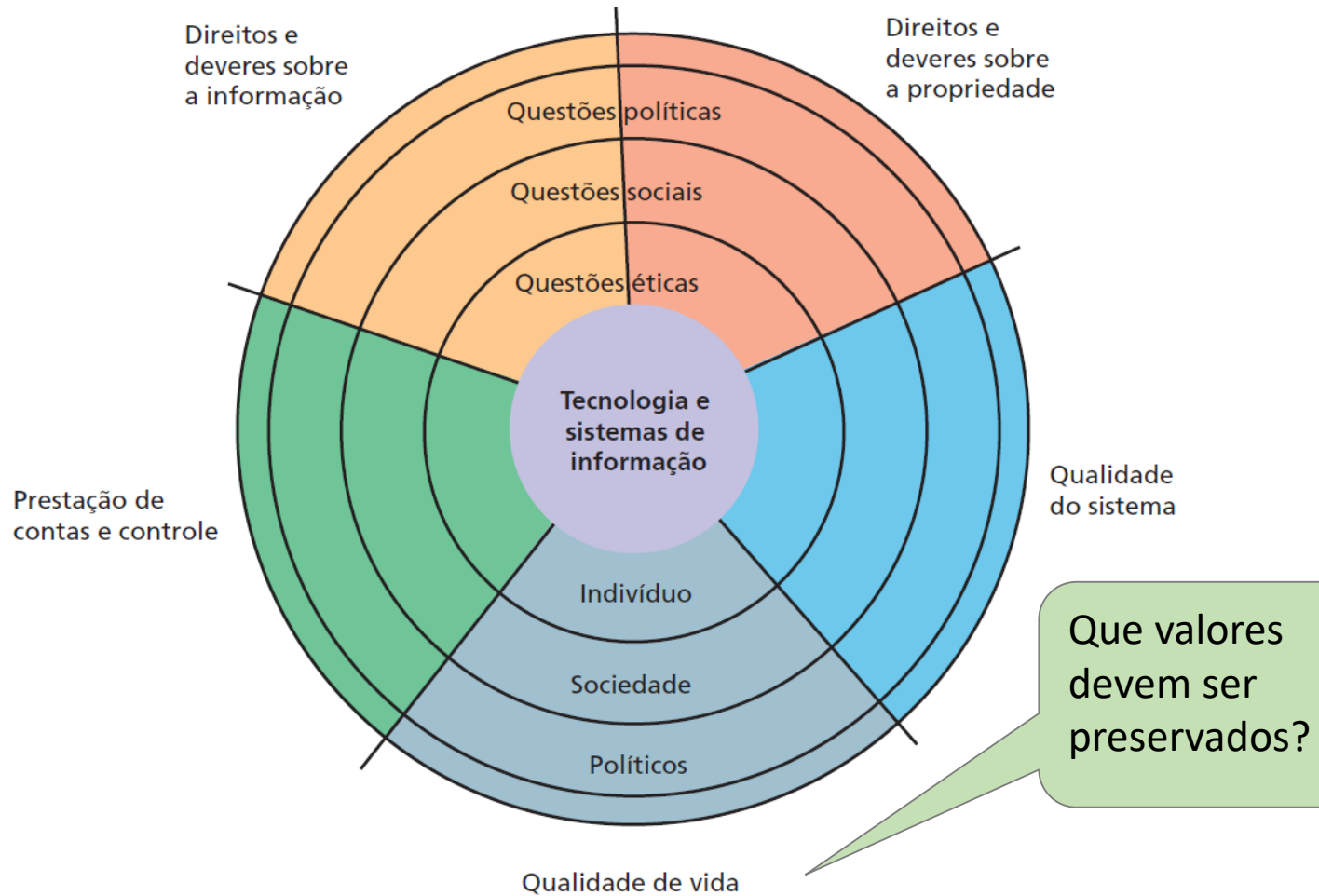


Que padrões de qualidade devem ser exigidos para proteção e segurança da sociedade?

Qualidade do Sistema

- Qualidade dos dados e erros de sistema
 - Perda de serviço (2012) – Netflix, Redes Sociais, Amazon...
 - Qualidade do serviço da nuvem: essas falhas são aceitáveis??
- Bugs e erros de software
 - *Quando o software está completamente testado?*
- Falhas no hardware ou instalações causadas por eventos naturais ou de outra ordem
- Baixa qualidade da entrada de dados

Questões éticas, sociais e políticas



Qualidade de Vida

- Custos sociais da TI e dos SIs:
 - O equilíbrio de poder: centro versus periferia
 - Fronteiras não claras entre: trabalho, família e lazer
 - Dependência e vulnerabilidade
 - Crime e abuso digital (spam)
 - Perda de emprego
 - Tecnoestresse

Um pequeno Código de Conduta para Área de Informática*

- Evitar danos a terceiros,
- Conhecer e respeitar as leis existentes, relativas ao trabalho profissional,
- Respeitar a privacidade de terceiros,
- Ser honesto e digno de confiança,
- Articular a responsabilidade social de membros de uma organização e encorajar a aceitação completa das suas responsabilidades.
- Não interferir no trabalho de computação de outra pessoa;

Um pequeno Código de Conduta para Área de Informática*

- Não interferir nos arquivos de outra pessoa;
- Não usar o computador para roubar;
- Não usar o computador para dar falso testemunho;
- Não usar software pirateado;
- Não usar recursos de computacionais de outras pessoas;
- Não se apropriar do trabalho intelectual de outra pessoa;
- Refletir sobre as consequências sociais do que escreve;
- Usar o computador de maneira que mostre consideração e respeito ao interlocutor.

Ainda sobre Código de Ética

- Código de Ética do Profissional de Informática – SBC (2013)
 - http://www.sbc.org.br/jdownloads/02.codigo_de_etica_da_sbc.pdf