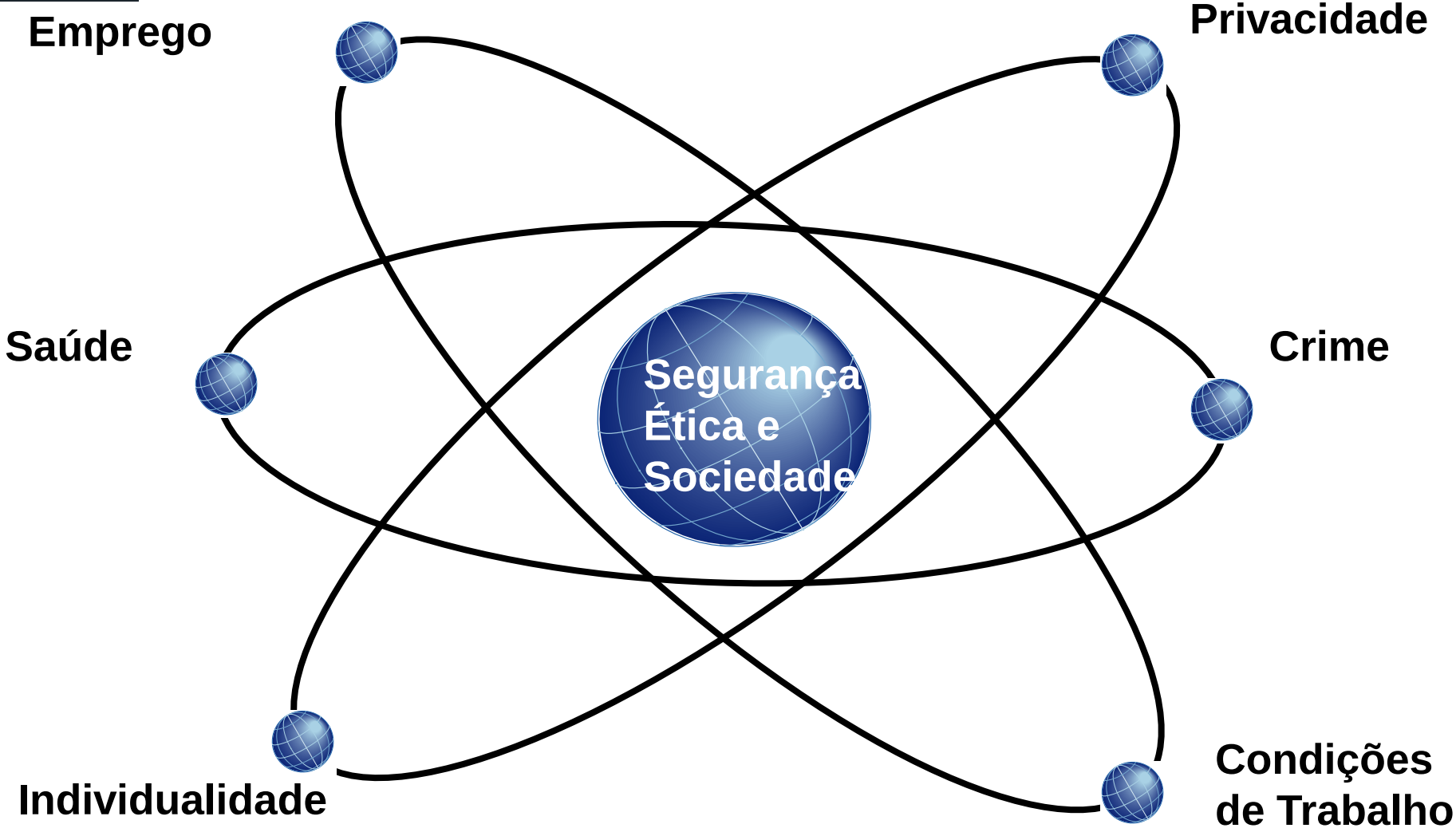
ÉTICA E SEGURANÇA EM TI

ÍNDICE

Princípios da Ética Tecnológica

Princípios da Ética Tecnológica
• **Proporcionalidade.** O bem realizado pela tecnologia deve exceder o dano ou o risco. Além disso, não deve haver nenhuma alternativa que realize os mesmos benefícios ou comparáveis com menos dano ou risco.
• **Consentimento Informado.** Aqueles afetados pela tecnologia deveriam compreender e aceitar os riscos.
• **Justiça.** Os benefícios e as responsabilidades da tecnologia devem ser distribuídos corretamente. Aqueles que se beneficiam deveriam suportar a divisão justa dos riscos, e aqueles que não se beneficiam não deveriam sofrer um aumento significativo no risco.
• **Riscos Minimizados.** Mesmo se considerada aceitável pelas outras três diretrizes, a tecnologia deve ser implementada de modo a evitar todos os riscos desnecessários.

Dimensões Éticas e Profissionais



Dimensões Éticas e Profissionais

A TI levanta sérios problemas éticos e sociais em termos de seu impacto no emprego, individualidade, condições de trabalho, privacidade, saúde e crimes em informática.

EMPREGO:

Perda do Emprego por automação e substituição do computador por trabalhos manuais.

CONDIÇÕES DE TRABALHO:

Monitoramento do trabalho
Qualidade das condições de trabalho que fazem uso pesado da TI

INDIVIDUALIDADE:

Perda de personalidade,
Organização e inflexibilidade de alguns Sistemas de Empresariais.

SAÚDE:

Uso intenso do computador por longos períodos.

PRIVACIDADE:

Acessar e coletar dados pessoais sem sem autorização, calúnias por computador.

CRIMES EM TI:

Hacking, Virus, worms, furtos, uso não autorizado do trabalho alheiro, pirataria.

Responsabilidade Ética nos Negócios

Os gerentes e especialistas em TI podem ajudar a resolver o uso impróprio da TI assumindo suas responsabilidades éticas para o uso ergométrico, uso benéfico e gerenciamento de TI esclarecido para a Sociedade.

Exemplos: Responsalidade Social, que esboçam a responsabilidade da gerência e dos empregados em TI para a empresa e para a sociedade em questão.

Gerenciamento da Segurança

Ferramentas e políticas de segurança podem assegura a precisão, a integridade e a segurança dos recursos de informação de uma empresa, minimizando erros, fraudes e perdas em suas atividades.

Exemplos como a Criptografia de dados, firewalls, monitoramento de e-mails, softwares de anti-virus, códigos de segurança, segurança biométrica, medidas de recuperação de desastres e auditorias são algumas providências para controlar imprevistos indesejáveis.

Crime com o uso do Computador

Acesso Indevido (Hacking)

Ciberrroubo

Vírus de Computador

Uso não autorizado em Serviço

Pirataria

Táticas Usuais de Hacking

- Negação de Serviço
- Scans
- Programas de Sniffer
- Spoofing
- Cavalos de Tróia
- Back Doors
- Applets prejudiciais
- Discagem de Guerra (War Dialing)
- Bombas Lógicas
- Buffer Overflow
- Quebrador de Senhas
- Engenharia Social
- Mergulho no Depósito de Lixo

Desafios no Emprego

Redução das Oportunidades de Emprego

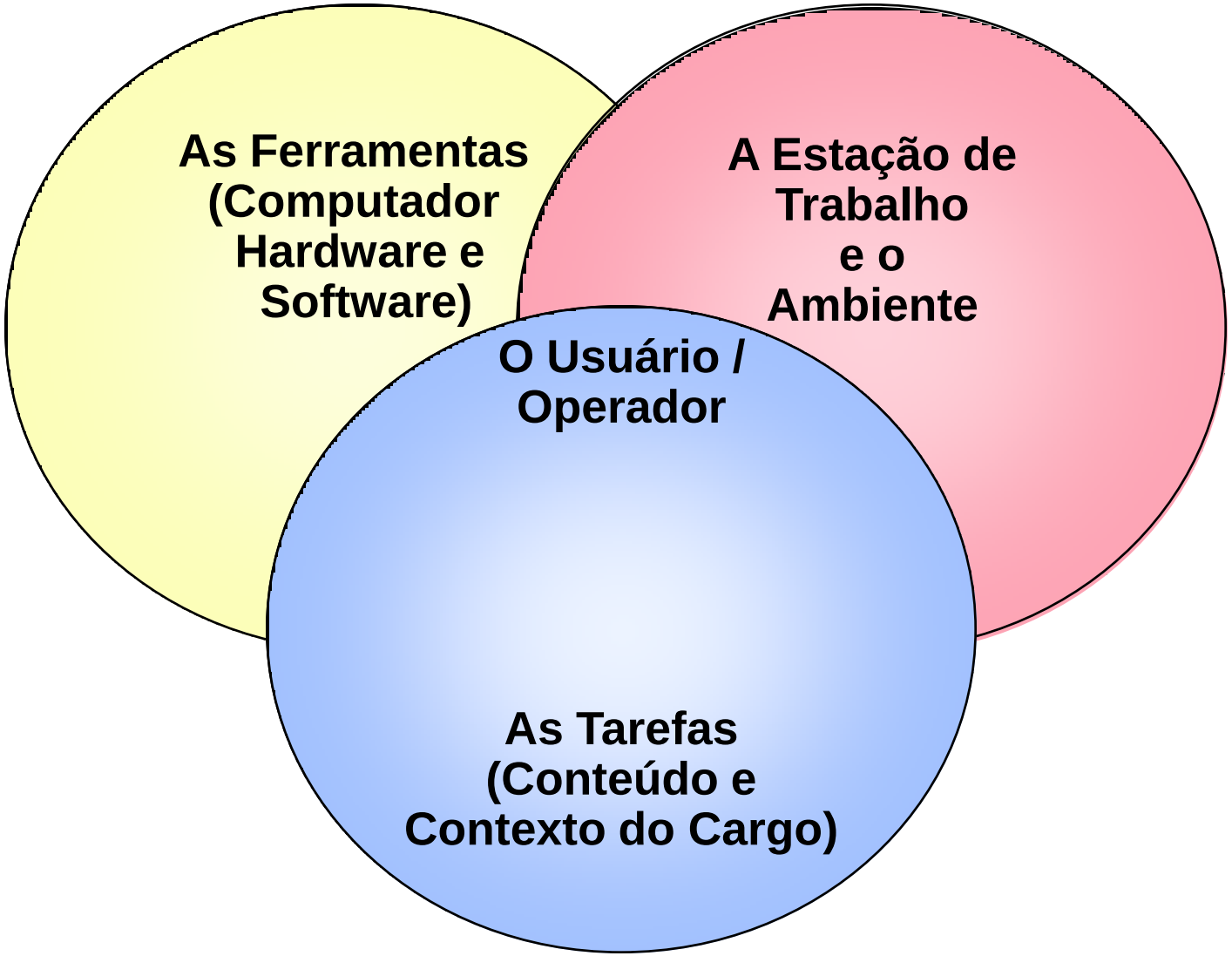
Perda da Individualidade

Condições de Trabalho

Monitoramento por Computador

Problemas de Saúde

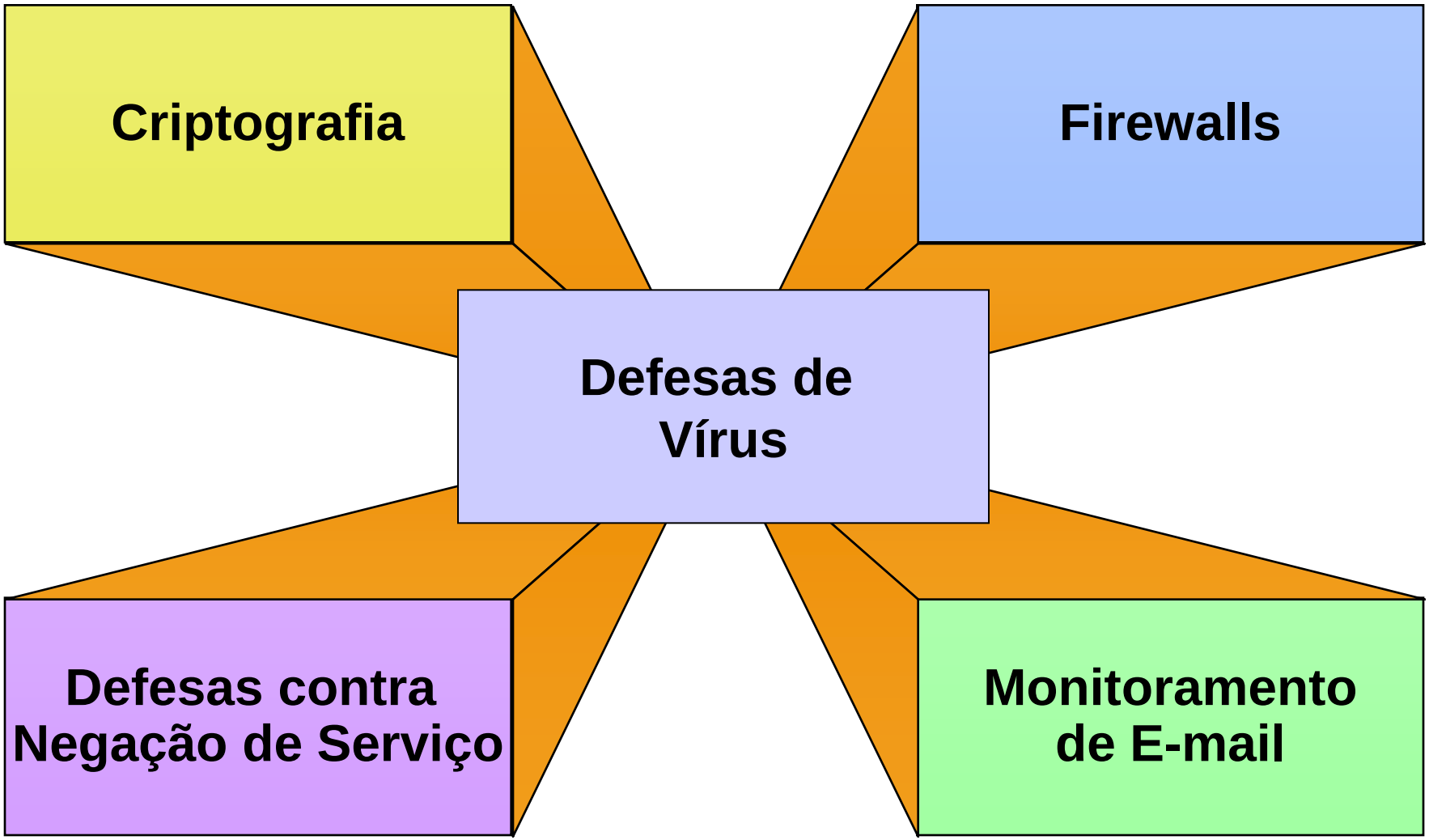
Fatores Ergonômicos no Local de Trabalho



Considerações Éticas

- Princípios Éticos
  - Proporcionalidade
  - Consentimento com Informação
  - Justiça
  - Risco Minimizado
- Padrão de Conduta
  - Agir com integridade
  - Proteger a privacidade e a confidencialidade de informação
  - Não deturpar ou reter informações
  - Não utilizar mal os recursos
  - Não explorar a fraqueza dos sistemas
  - Fixar altos padrões
  - Contribuir para a boa saúde e o bem-estar geral das pessoas

Administração de Segurança em e-Business



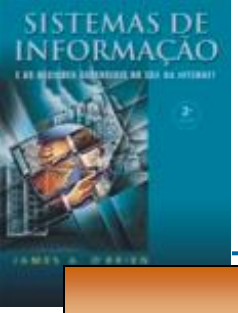
Outras Medidas de Segurança de e-Business

Códigos de Segurança

Cópias de Segurança

Monitores de Segurança

Controles Biométricos



Controles de Falha no computador

Sistemas Tolerantes a Falhas

Camada	Ameaça	Métodos Tolerantes a Falhas
Aplicações	Ambiente, falhas de hardware e software	Redundância de aplicações, pontos de verificação
Sistemas	Interrupções de energia elétrica	Isolamento do sistema Segurança de dados
Bancos de Dados	Erros de dados	Histórias das transações, cópias de segurança
Redes	Erros de transmissão	Roteamento alternativo, códigos de correção de erros
Processos	Falhas de hardware e software	Pontos de verificação
Arquivos	Erros de mídia	Reprodução de dados
Processa-dores		Nova tentativa de instrução

Recuperação de Desastres

- Quem participará?
- Quais serão as suas obrigações?
- Que hardware e software será usado?
- Que aplicações terão prioridade de execução?
- Que outras instalações poderão ser utilizadas?
- Onde os bancos de dados serão armazenados?

Auditoria e Controle de Sistemas e-Business

Controles de Entrada

Códigos de Segurança
Criptografia
Sinais de Erros

Controles de Processamento

Firewalls
Controles de Software
Controles de Hardware
Pontos de Verificação

Controles de Saída

Códigos de Segurança
Criptografia
Totais de Controle
***Feedback* do Usuário Final**

Controles de Armazenamento

Códigos de Segurança
Criptografia
Arquivos de Reserva

Resumo do Capítulo

- O papel crucial dos sistemas de e-business e e-commerce na sociedade levanta sérias questões éticas e sociais em termos de seu impacto no emprego, individualidade, condições de trabalho, privacidade, saúde e crimes com o uso do computador.
- Gerentes podem ajudar a solucionar os problemas de utilização inadequada da TI, assumindo suas responsabilidades éticas para o projeto ergonômico, uso benéfico e administração consciente das tecnologias de e-business em nossa sociedade.

Resumo do Capítulo (cont.)

- As atividades de negócios e de TI envolvem muitas considerações éticas. Princípios ético e padrões de conduta servem como diretrizes para lidar com problemas éticos nas empresas.
- Uma das mais importantes responsabilidades da administração de uma companhia é garantir a segurança e a qualidade de suas atividades de e-business.
- Ferramentas e políticas de administração de segurança podem assegurar a precisão, integridade e segurança dos sistemas e recursos de e-business.