**Tópicos de Ambiente Web**

**ARPANET**: a primeira rede de computadores por comutação de pacotes e uma das percursoras da internet atual, possibilitou que diversos centros de computadores e diversos grupos de pesquisa de universidades fizessem compartilhamentos de informações on-line.

**MILNET**: uma rede independente para usos militares específicos.

A rede do ARPANET foi renomeada: passou a ser chamada de ARPA-INTERNET e foi destinada à pesquisa nas universidades.

- Início da década de 1960: a ideia da internet começou a tomar forma nas concepções dos cientistas da computação.

- Final da década de 1960: constituição de uma rede de comunicações por meio de computadores.

- Década de 1970: formação de comunidades dispersas de computação reunindo cientistas da computação.

- Década de 1990: presenciamos o marco do nascimento da internet para os empresários e para a sociedade em geral.

Um navegador de internet (ou browser) é um programa que possibilita o nosso acesso aos sites ou links, visto que é ele quem faz a comunicação com os servidores, e processa os dados e as informações.

Década de 1990: Tim Berners-Lee desenvolvem um sistema de hipertexto conhecido como www (World Wide Web), a rede mundial.

Em 1994, a Netscape Communications, oriunda da Mosaic Communications, disponibilizou o Netscape Navigator, reconhecido como o primeiro navegador comercial.

O Protocolo de Controle de Transporte, ou Transport Control Protocol (TCP) é um dos principais protocolos e opera na camada de transporte, acrescentando funcionalidades, como a garantia da confiabilidade do fluxo de dados na transmissão.

O Protocolo de Internet ou Internet Protocol (IP), opera na camada de rede e possibilita a comunicação.

**Web 1.0:**

Forneceu as páginas web dos anos iniciais da internet.

Não ofertava a possibilidade de interação com o usuário e apresentavam conteúdos estáticos e, muitas vezes, desatualizados.

**Web 2.0:**

Chamada de web colaborativa, porque os usuários tinham a possibilidade de colaborar na criação de conteúdos, deixando de ser meros consumidores.

Surgimento dos blogs com a opção de inserção de comentários, dos sites interativos e das diversas redes sociais, em que os usuários compartilham textos, fotos, áudios e vídeos.

**Web 3.0:**

Chamada de web inteligente, onde a informação tem um elevado grau de organização, de modo que tanto humanos quanto robôs e computadores podem usá-la.

Surge a Inteligência Artificial, e a Internet das Coisas ou Internet of Things (IoT).

**Web Sêmantica:**

As informações são classificadas de modo padronizado, com a intenção de que o acesso a elas seja facilitado.

Pode ser encarada como uma das responsáveis pela melhoria da qualidade das informações obtidas na internet e pela otimização do posicionamento de sites.

**e-commerce:**

**B2B** (Business to Business): “de empresa para a empresa”. Empresas B2B vendem para as empresas, como ocorre, por exemplo, no mercado de automóveis, em que diversos fornecedores vendem componentes para as montadoras.

**B2C** (Business to Consumer): “de empresa para o consumidor”. Empresas B2C vendem para o consumidor final, como ocorre, por exemplo, na Amazon, na Netflix e no Submarino.

**B2E** (Business to Employee): “de empresa para o funcionário”. Empresas B2E vendem para os seus funcionários, como ocorre, por exemplo, com as empresas que incentivam os seus funcionários a consumirem o que elas produzem pelo oferecimento de descontos atraentes.

**B2G** (Business to Government): “de empresa para o governo”. Empresas B2G vendem para o governo (em geral, essa venda ocorre por processos de licitação com concorrência pública).

**C2C** (Consumer to Consumer): “de consumidor para o consumidor”. Na categoria C2C, consumidores vendem, diretamente, para outros consumidores, como ocorre, por exemplo, no Mercado Livre e no eBay.

**Características:**

Ubiquidade.

Alcance global.

Padrões universais.

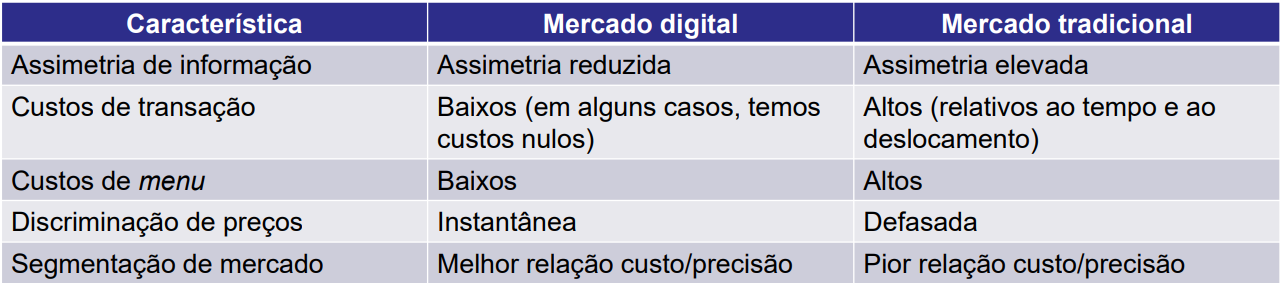
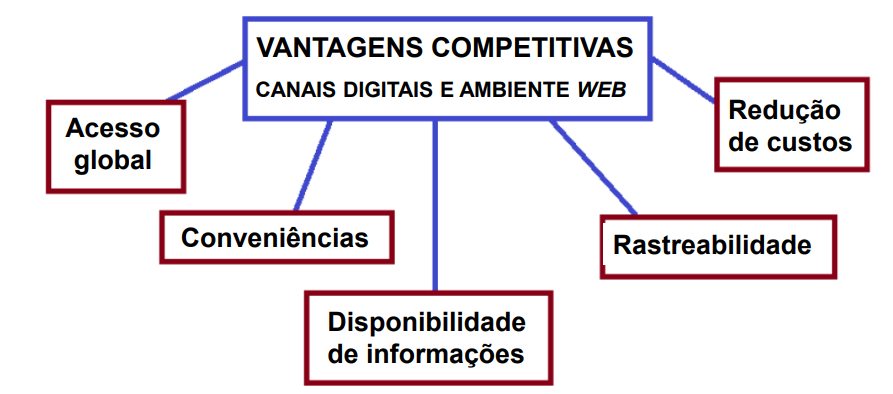
Riqueza da informação.

Interatividade.

Densidade da informação.

Personalização/customização.

Tecnologia social.



**Benefícios**:

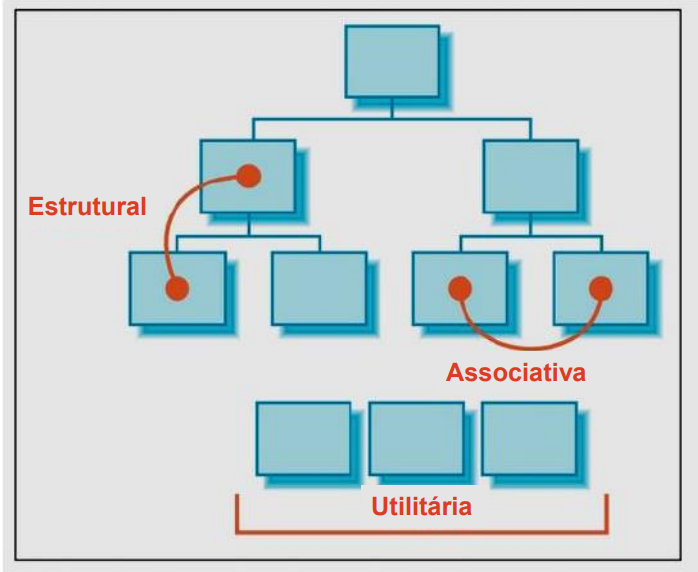
Acesso a informações estratégicas de modo veloz.

Controle e gestão total das operações realizadas, e em processamento.

Identificação de falhas e desvios nos processos.

Apuração rápida dos resultados de desempenho de vendas e de entregas.

**Tipos de Navegação:**



Na **navegação estrutural**, uma página web está ligada a outra página de acordo com a hierarquia do site.

Nesse caso, se estivermos em uma página qualquer, é possível irmos para a página acima ou para a página abaixo dela, na hierarquia do site.

Por meio da **navegação associativa**, permite-se que um usuário que esteja lendo a respeito de um tópico também possa acessar outros assuntos a ele relacionados, o que é um aspecto fundamental para a realização de marcações de hipertextos

A **navegação associativa** pode ser embutida (links colocados no próprio texto) e navegação por links relacionados (links colocados no fim do texto ou ao lado do conteúdo) ou por meio de informações no rodapé.

A **navegação utilitária** engloba ferramentas e funcionalidades que contribuem para a melhor utilização do site por parte dos usuários.

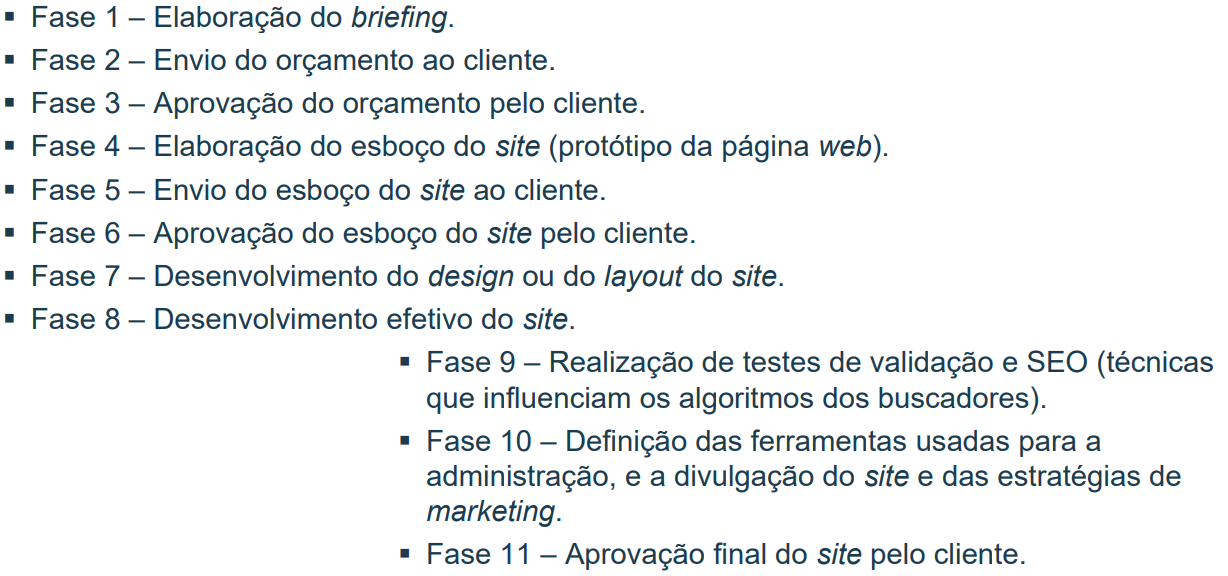
**Páginas navegacionais:** fazem o direcionamento dos visitantes ao conteúdo procurado. Exemplos: página principal, as galerias e as páginas de aterrissagem.

**Páginas de conteúdo:** contêm os motivos que levam as pessoas a visitarem o site e apresentam, por exemplo: artigos, textos, notícias, blogs, informações sobre determinada empresa, vídeos, fotos, dados a respeito dos serviços oferecidos e características dos produtos vendidos.

**Páginas funcionais:** possibilitam que os internautas realizem ações como, por exemplo: a execução de buscas, a realização de compras on-line, a verificação de mensagens de e-mails, a consulta de saldos bancários e o preenchimento de cadastro.

**Sites informativos:** são caracterizados por apresentarem uma informação desejada para os seus usuários de modo categorizado e com fácil acesso. Por isso, há a necessidade de que uma elevada quantidade de conteúdo seja organizada na forma de documentos, a fim de que se facilite a navegação dos usuários, no sentido de eles encontrarem aquilo que estão procurando.

**Sites interativos:** são caracterizados por oferecerem interfaces funcionais de aplicações. Por isso, há a demanda por grande capacidade de processamento de dados e por uma programação avançada.



**Características desejaveis para um site:**

Facilidade de utilização (ou de aprendizagem) por parte do usuário e a funcionalidade, de modo que o visitante possa encontrar rapidamente a informação que procura.

O design da interface precisa ser atraente e consistente, e trazer conforto ao usuário.

Fornecer um feedback aos visitantes que navegam em um site, para que eles sejam comunicados a respeito do sucesso de suas ações.

A clareza visual do site é determinante para que o visitante seja motivado a nele permanecer e seja orientado a como nele navegar.

A velocidade com que o site “carrega” é um fator a ser considerado, diante da frequente falta de disponibilidade de tempo das pessoas e da concorrência.

**Vulnerabilidade**:

**Confidencialidade**: refere-se à manutenção das restrições que foram autorizadas sobre o acesso na divulgação de informações e respeito à privacidade das informações dos indivíduos.

**Integridade**: representa a capacidade de prevenção contra as alterações, ou as destruições impróprias ou não autorizadas de informações.

**Disponibilidade**: a informação deve estar disponível para o usuário. A disponibilidade representa a garantia do acesso e da utilização da informação, de maneira rápida e confiável, em qualquer momento desejado pelo usuário.

**Atacante** (ou invasor): trata-se de quem tenta (ou consegue) violar a segurança de um sistema computacional intencionalmente.

**Ameaça**: trata-se da possibilidade de haver uma violação de segurança de um sistema computacional, como, por exemplo, a descoberta de uma vulnerabilidade.

**Ataque**: trata-se da tentativa de violação da segurança de um sistema computacional.

**Violação**:

**Violação** de sigilo: refere-se à duplicação não autorizada de informações, destinada à obtenção de informações sigilosas, com finalidades políticas, estratégicas, financeiras etc.

**Violação de integridade:** refere-se à modificação de dados, de forma não intencional e/ou não autorizada, podendo ocorrer por meio do sequestro de dados, ou pode ser efetuado apenas para causar dano aos legítimos donos das informações.

**Violação de disponibilidade**: refere-se à destruição de dados, onde os invasores praticam a violação de disponibilidade, visando aumentar o status dos invasores perante os seus pares, a defender alguma causa ou a demonstrar uma vulnerabilidade.

**Furto de serviço:** refere-se ao aproveitamento de algum recurso computacional de forma não autorizada.

**Recusa de serviço:** refere-se a uma classe de violação em que o invasor visa a impedir que um sistema continue operando normalmente e oferendo a sua funcionalidade.

**Tipos de Ataques:**

**Ataques de negação de serviço (DoS):** tentativa coordenada feita com a intenção de que um serviço tenha a sua execução negada.

**Ataques do tipo “porta dos fundos” (backdoors):** ocorrem a partir do acesso oculto a programas, denominado de “porta dos fundos”.

**Ataques de espionagem telefônica (wiretapping):** é a interceptação da comunicação de voz.

**Ataques de navegação web inaceitável:** utilização do navegador de forma não permitida pela política de determinada organização.

**Falsificação de e-mail:** são feitas alterações nos campos do cabeçalho de um e-mail com a intenção de iludir o usuário com uma informação incorreta do remetente.

**Ataque de força bruta:** o atacante tenta acertar, por tentativa e erro, um nome de usuário e a sua senha.

**Desfiguração de página (defacement):** há a alteração de conteúdo de uma página web de um site.

**Plugins**: são exploradas falhas nos plugins, que permitem que um criminoso assuma o controle do sistema afetado.

**Envenenamento de SEO (Search Engine Optimization):** aumenta o tráfego em sites maliciosos que podem hospedar malwares ou executar a engenharia social.

**Engenharia social:** ataque de acesso que tenta manipular indivíduos para realizarem ações ou divulgarem informações confidenciais.

**Fraude de antecipação de recursos (advance fee fraud):** o golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de receber algum tipo de benefício futuro.

**Representação (scam), e farsas ou boatos (hoax):** ato de fingir ser outra pessoa, com a finalidade de enganar ou de ludibriar.

**Phishing**: tipo de golpe por meio do qual um criminoso tenta obter dados pessoais e financeiros de um usuário. Exemplos: pharming (utiliza a representação de um site legítimo); smishing (utiliza mensagens de texto em celulares); vishing (utiliza a tecnologia de comunicação de voz); whaling (dedicado às vítimas de elevada hierarquia em uma empresa).

**Shoulder surfing:** forma com que os criminosos roubam informações relevante ao “olharem por cima do ombro de uma outra pessoa”, ou seja, o criminoso está bisbilhotando a vítima.

O termo “**malware**” é resultado da junção abreviada das palavras malicious e software. Exemplos: malwares infecciosos (vírus e worms); malwares não infecciosos (cavalos de Troia).

O **vírus** é um programa (ou uma parte de um programa), normalmente malicioso, que se propaga pela introdução de cópias dele mesmo.

Trata-se do malware mais conhecido e que depende da execução do programa ou do arquivo hospedeiro para se tornar ativo, e, assim, prosseguir com o processo de infecção.

O **worm** ou verme é um programa capaz de se multiplicar por uma rede, visto que envia cópias de si mesmo para os computadores interligados.

Os worms são semelhantes aos vírus, mas não se propagam pela inclusão de cópias de si mesmo em outros arquivos, mas pela execução direta das suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

O worm pode consumir muitos recursos computacionais e, com isso, diminui o desempenho de redes e a eficácia do uso de computadores, já que realiza muitas cópias de si mesmo.

É um **malware** que usa a sua aparência externa com a finalidade de enganar o usuário e fazer com que ele o execute.

**Cavalo de troia** se trata de um código malicioso que, uma vez executado, realiza as instruções de ataque com as permissões e a autoridade do usuário.

Vale destacar que esse cavalo de Troia precisa ser aceito pelo usuário, pois o programa tem de ser executado por uma pessoa.