

Unidade II

5 PROCESSO DE DESENVOLVIMENTO DE UM SITE

Neste tópico, apresentaremos os princípios da linguagem HTML, a estrutura de um documento e os marcadores para a formatação do conteúdo e faremos uma introdução à linguagem HTML5.

5.1 Criação de padrões para páginas web

Vimos, na unidade I, que a criação de padrões para a internet permitiu a ocorrência de navegação acessível para diferentes usuários, com diversos dispositivos e distintos sistemas operacionais. Tais padrões para a web são criados pelo W3C, consórcio internacional que conta com a colaboração das organizações filiadas e do público.

Nesse sentido, foram definidas algumas técnicas de programação para organizar o desenvolvimento de sites, com destaque para a linguagem de marcação de hipertexto (Hyper Text Markup Language), conhecida como linguagem HTML.



Observação

Além do HTML, temos, por exemplo, o eXtensible Markup Language (XML), o eXtensible Hyper Text Markup Language (XHTML) e o Cascadig Style Sheet (CSS).

De acordo com Macedo (2004), o uso de padrões para o desenvolvimento de sites diminui o tempo e a dificuldade no projeto e na execução da manutenção de páginas de internet. Além disso, os padrões utilizam elementos de facilitação de acessibilidade para pessoas com deficiência, o que torna a internet disponível para todos, sem discriminação.

Vale destacar que a elaboração de páginas web que seguem padrões garante maior visibilidade nas ações de busca, visto que, com isso, os mecanismos de busca obtêm mais informações sobre o conteúdo do site.

O emprego de padrões também permite que façamos uma separação entre a estrutura e a apresentação do site. Isso possibilita que a apresentação seja modificada, de maneira ágil e flexível, segundo as necessidades do usuário (MACEDO, 2004).



Saiba mais

Os princípios que regem o W3C são: *web* para todos e *web* em todas as coisas. Ou seja, na visão do W3C, a *web* é destinada a usuários e a autores e apresenta dados e serviços confiáveis. Por exemplo: grandes empresas, pequenas agências de publicidade e o público em geral podem participar do desenvolvimento do W3C.

Para saber mais sobre o W3C, visite o *site*:

Disponível em: <https://www.w3c.br/>. Acesso em: 1 dez. 2020.

5.2 Linguagem HTML

A linguagem usada na criação de documentos para a *web* é a linguagem de marcação de hipertexto (Hyper Text Markup Language), mais comumente chamada de HTML.

Com o uso da linguagem HTML, o desenvolvedor consegue fazer a especificação de atributos para determinado texto, como fonte, tamanho e cor, e criar hipertextos, marcações que definem um vínculo entre o texto e outro documento. Aqui, usamos o conceito do hipertexto relativo ao estabelecimento de vínculos entre diversos documentos, normalmente conhecidos como páginas, criados a partir de marcações específicas.

Precisamos reforçar que o HTML não pode ser considerado uma linguagem de programação propriamente dita. De modo estrito, o HTML pode ser classificado como uma linguagem de formatação de textos ou de definição da estrutura de um documento, pois nele não temos a compilação de um programa executável autônomo, de extensão .exe, tal qual acontece nas linguagens de programação tradicionais, como no C++, no Java e no Pascal. Em vez disso, no HTML há apenas um arquivo em formato de texto, normalmente com a extensão .htm ou .html, que é lido e interpretado por um navegador. Esse código é responsável por exibir na tela aquilo que foi codificado no documento HTML.



Observação

A linguagem HTML não permite a geração de aplicações executáveis, mas somente de documentos que podem ser visualizados em um navegador ou *browser*.

5.2.1 Características da linguagem HTML

A seguir, listamos algumas características da linguagem HTML:

- A linguagem HTML não apresenta estruturas de controle e de repetição.
- Na linguagem HTML, não é possível fazer a criação de procedimentos ou funções nem a chamada de rotinas internas do sistema operacional.
- Na linguagem HTML, há independência de plataforma, tanto em termos de *hardware* quanto em termos de *software*. Isso possibilita que qualquer tipo de computador leia e interprete o conteúdo de um documento HTML. Nesse sentido, vale destacar que o HTML foi desenvolvido para ser usado na *web*, e não em um equipamento específico que opere com determinado sistema operacional.
- A linguagem HTML não é monopólio de uma pessoa, de uma empresa ou de um órgão governamental.
- Os arquivos resultantes do HTML são pequenos, vinculados entre si por meio dos *hiperlinks* que são definidos na estrutura dos documentos. O tamanho reduzido viabiliza a transmissão com velocidade aceitável, mesmo em meios de comunicação de baixa velocidade, como na conexão discada.
- O HTML não necessita de um editor especial, visto que podemos utilizar o bloco de notas, o WordPad ou qualquer outro programa de edição de texto capaz de gravar arquivos em um padrão de texto sem formatação, conhecido como texto puro.

Com o passar do tempo, surgiram outras linguagens que funcionam em conjunto com o HTML. Tais linguagens apresentam finalidades específicas e dispõem de recursos diferenciados. Vejamos três exemplos:

- As linguagens JavaScript e VBScript são indicadas quando desejamos fazer o tratamento de eventos gerados pelos navegadores, como o clique em um botão de formulário. Nesse caso, o código será implementado no servidor, o qual irá gerar uma página dinâmica que será exibida no navegador do cliente.
- A linguagem PHP é indicada quando desejamos fazer o desenvolvimento de *sites* que acessam e manipulam bancos de dados e de páginas dinâmicas.
- A linguagem Java, que não tem relação com a linguagem JavaScript, é indicada quando desejamos fazer a criação de interfaces gráficas para uso interno nas páginas, como nos teclados virtuais.

5.2.2 Estrutura do documento HTML

Na linguagem HTML, em vez de usarmos as instruções das linguagens convencionais, utilizamos elementos denominados *tags*, ou marcadores, empregados para ativar ou desativar (ligar ou desligar) uma formatação a ser aplicada a um texto.



Observação

O HTML faz parte de uma classe de linguagens de programação chamada de linguagens de marcação, ou Tag Languages. Nessa classe, escrevemos os comandos na forma de marcações denominadas *tags*. Em geral, as *tags* são usadas aos pares e delimitam o texto que será formatado.

Um documento HTML é dividido em seções, e cada seção deve conter um tipo específico de informação. Temos um marcador para definir cada seção do documento.

A estrutura básica de um documento HTML é formada pelos componentes citados a seguir:

- Início do documento.
- Cabeçalho.
- Título.
- Corpo do documento.
- Fim do documento.

Se traduzirmos a estrutura anterior para a linguagem HTML, ficamos com o que se mostra a seguir e o que se ilustra na figura.

```
<HTML>  
  <HEAD>  
    <TITLE>  
    </TITLE>  
  </HEAD>  
<BODY>  
</BODY>  
</HTML>
```

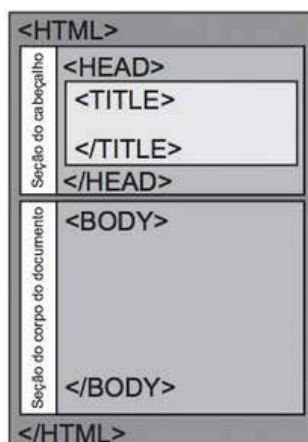


Figura 25 – Estrutura básica de um documento HTML

Alternativamente, podemos fazer a estrutura indicada a seguir.

```
<HTML>
  <HEAD>
    <TITLE>
      Exemplo de estrutura básica
    </TITLE>
  </HEAD>
  <BODY>
    Bem-vindo(a) ao ambiente web!
  </BODY>
</HTML>
```

Os marcadores (*tags*) são os elementos do HTML equivalentes aos comandos das linguagens convencionais e que possibilitam a formatação do texto. Um marcador deve ser apresentado entre os sinais "<" e ">". A maioria dos marcadores funciona como uma espécie de chave "liga e desliga". Logo, verificamos que um marcador é empregado para indicar o início da formatação e outro para informar o fim dela. Na indicação do fim da formatação, utilizamos uma barra ("/") antes do nome do marcador.

O HTML não faz distinção entre caracteres maiúsculos e minúsculos, ou seja, não é *case sensitive*. Assim, as escritas <BODY>, <Body> e <body> correspondem à mesma *tag*.



Saiba mais

Para saber mais sobre os comandos do HTML, leia o texto sugerido a seguir:

TCDF. *HTML: comandos*. 2017. Disponível em: <https://bit.ly/3vNQmE8>. Acesso em: 11 jan. 2021.

No HTML, usamos parágrafos para agrupar conteúdos relacionados, que podem ser de diferentes tipos, como imagens, vídeos e campos de um formulário. A *tag* HTML <p> representa um parágrafo. Devemos usar esse tipo de *tag* para fazer a quebra do texto em um novo parágrafo, visto que o HTML não reconhece o comando "ENTER" como o fim de uma linha ou de um parágrafo.

Como exemplo do que estamos estudando, usaremos o programa Notepad++ como editor dos códigos HTML.



Saiba mais

O programa Notepad++ pode ser baixado gratuitamente no *site* a seguir:

Disponível em: <https://notepad-plus-plus.org/>. Acesso em: 26 nov. 2020.

Depois de realizar o *download* do Notepad++, efetue a sua instalação.

A figura a seguir apresenta a interface desse *software*.

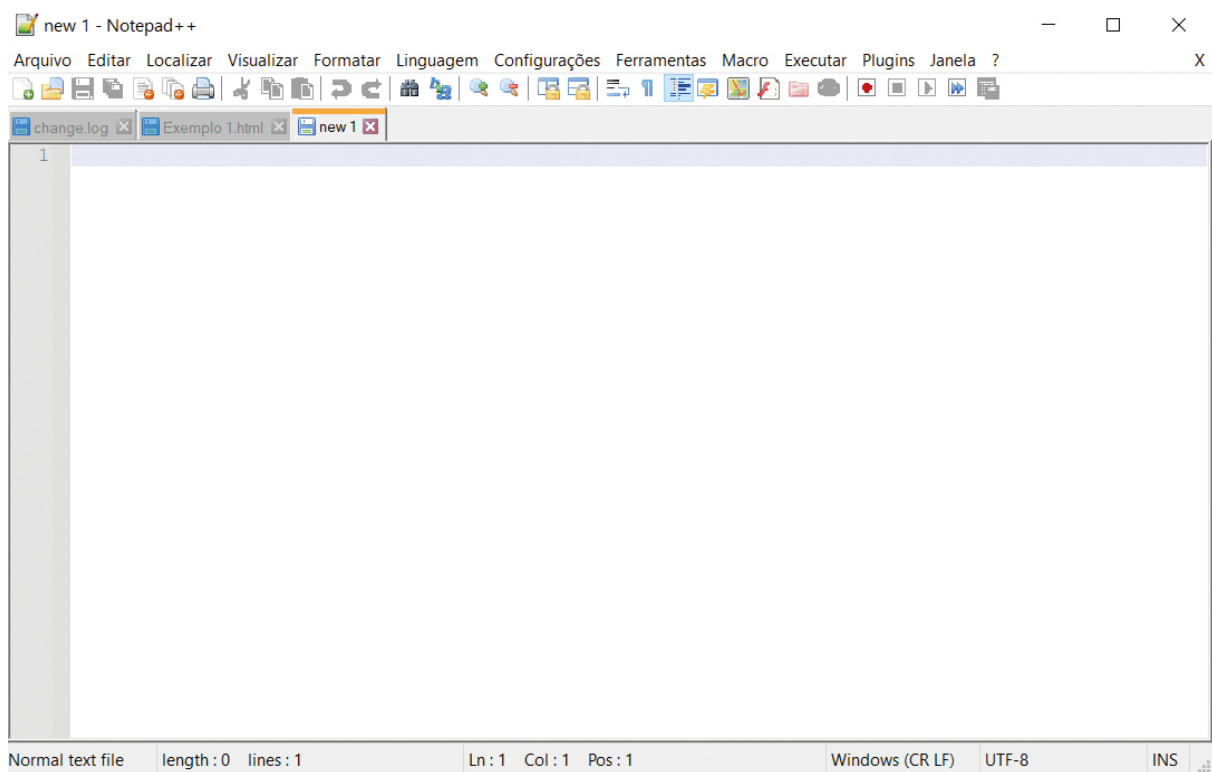


Figura 26 – Interface do Notepad++

Observação

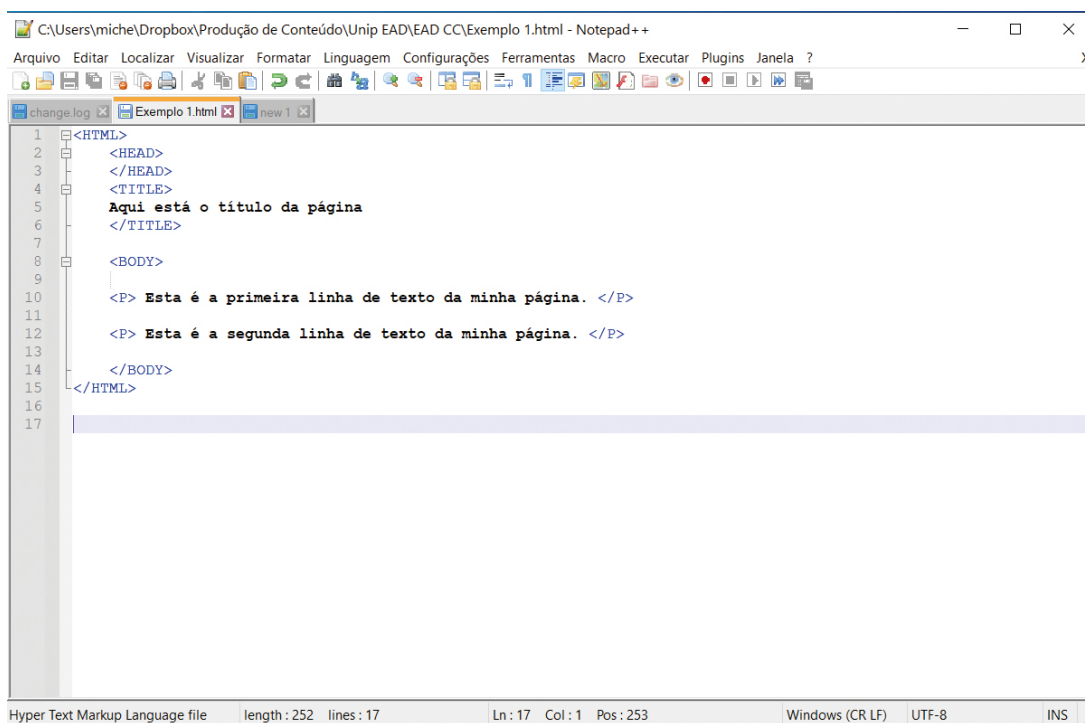
No menu "Linguagem" do Notepad++, é possível selecionar a linguagem HTML, entre outras.

Daremos um exemplo bem simples para mostrar, de modo didático, o uso dos marcadores. Execute o NotePad++ e digite o texto indicado a seguir e ilustrado na figura.

```
<HTML>

    <HEAD>
    </HEAD>
    <TITLE>
    Aqui está o título da página
    </TITLE>

    <BODY>
    <P> Esta é a primeira linha de texto da minha página. </P>
    <P> Esta é a segunda linha de texto da minha página. </P>
    </BODY>
</HTML>
```



```
1 <HTML>
2   <HEAD>
3   </HEAD>
4   <TITLE>
5   Aqui está o título da página
6   </TITLE>
7
8   <BODY>
9
10  <P> Esta é a primeira linha de texto da minha página. </P>
11
12  <P> Esta é a segunda linha de texto da minha página. </P>
13
14  </BODY>
15 </HTML>
16
17
```

Hyper Text Markup Language file length : 252 lines : 17 Ln : 17 Col : 1 Pos : 253 Windows (CR LF) UTF-8 INS

Figura 27 – Código HTML escrito no Notepad++

O arquivo HTML do exemplo foi gravado como "Exemplo1.html" e, posteriormente, aberto como um navegador. O navegador deve apresentar as duas linhas de texto. A figura a seguir exibe o documento aberto no Microsoft Edge.

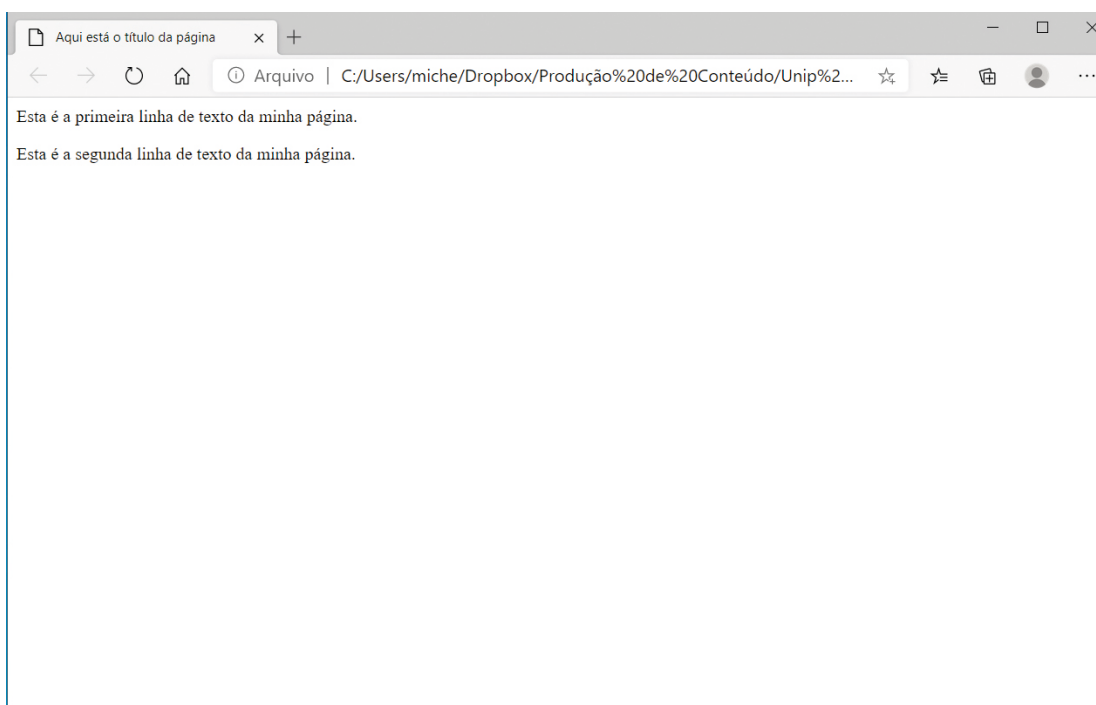


Figura 28 – Página HTML aberta no Microsoft Edge

5.2.3 Cabeçalhos e títulos

Na linguagem HTML, precisamos ter atenção especial aos títulos e aos cabeçalhos que podem ser adicionados às páginas web, pois eles possibilitam que o usuário saiba em que ponto do *site* ele se encontra ou sobre qual assunto a página trata. Adicionalmente, tais elementos auxiliam as ferramentas de busca e a otimização da pesquisa, ou Search Engine Optimazation (SEO).

No HTML, há um marcador especial que configura o texto para a apresentação em um formato de título. Esse marcador configura o tamanho da fonte e o estilo negrito do texto. Os tamanhos da fonte são dados por seis níveis, indicados por nível 1, nível 2, nível 3, nível 4, nível 5 e nível 6, conforme podemos ver no código HTML a seguir. Quanto maior o número do nível, menor o tamanho do caractere do texto.

```
<HTML>
<HEAD>
<TITLE>
Exemplo de Configuração de títulos
</TITLE>
</HEAD>
  <BODY>
    <p>A seguir temos os seis níveis de títulos/cabeçalhos </p>
    <H1>Titulo formatado com nível 1 </H1>
    <H2>Titulo formatado com nível 2 </H2>
    <H3>Titulo formatado com nível 3 </H3>
    <H4>Titulo formatado com nível 4 </H4>
    <H5>Titulo formatado com nível 5 </H5>
    <H6>Titulo formatado com nível 6 </H6>
  </BODY>
</HTML>
```

A figura a seguir apresenta o resultado obtido quando a página é visualizada em um navegador.



Figura 29 – Página HTML visualizada em um navegador

Podemos fazer a centralização do texto no documento, o que é particularmente útil no caso de títulos. Para isso, usamos os marcadores `<CENTER>` e `</CENTER>`.



Saiba mais

Para saber mais sobre os elementos do HTML, visite o *site*:

Disponível em: <https://html.spec.whatwg.org>. Acesso em: 11 jan. 2021.

5.2.4 HTML5

O HTML5 é a quinta versão da linguagem HTML e apresenta melhores funcionalidades e características de semântica e de acessibilidade do que as versões anteriores.

Segundo Teruel (2014), no HTML5, temos:

- Novos recursos baseados em HTML, CSS, DOM e JavaScript.
- Redução da necessidade de *plugins* externos; por exemplo, para o uso do Flash.
- Permissão da utilização de elementos (*tags*) para substituir diversos *scripts*.
- Melhor manipulação de erros.
- Independência do dispositivo, ou seja, as mesmas marcações são utilizadas e renderizadas em diferentes tipos de dispositivo.

Vimos que uma das vantagens oferecidas pelo HTML5 é a possibilidade de redução (ou eliminação) de *plugins* necessários aos navegadores para que conteúdos de multimídia possam ser apresentados. Os novos recursos presentes no HTML5 permitem que criemos desenhos 2D e animações completas diretamente no código da linguagem. Adicionalmente, existem *tags* específicas para a execução de vídeos e áudios.

No HTML5, o cabeçalho da página pode ser definido com a nova *tag* `<HEADER>`, e uma área de rodapé pode ser criada com `<FOOTER>`.

Há, também, o componente canvas no HTML5, que possibilita a construção de elementos gráficos na página *web* com o uso de comandos simples. Assim, podemos desenhar, com facilidade, círculos, linhas, retângulos e outras formas geométricas mais complexas.

Para execução de áudios, o HTML5 dispõe da *tag* <AUDIO>. Para execução de vídeos, essa versão apresenta a *tag* <VIDEO>. Com esses recursos, podemos especificar alguns parâmetros, como a execução automática ou a repetição infinita.

No HTML5, há novas interfaces de programação de aplicativos, ou Application Programming Interfaces (APIs), que possibilitam a manipulação de conteúdos *off-line*, a consulta da geolocalização, o acesso a bancos de dados, a validação de formulários, a realização de comunicação bidirecional com o servidor, a execução de *scripts* em paralelo, a edição de arquivos de áudio e de vídeo, a criação de gráficos e desenhos, entre outros. Por exemplo: a API Web SQL Database permite a manipulação de bancos de dados do lado do cliente usando SQL via JavaScript (TERUEL, 2014).



Saiba mais

Para saber mais sobre o HTML5, leia os textos indicados a seguir:

ALVES, W. P. *Desenvolvimento e design de sites*. São Paulo: Érica, 2014.

TERUEL, C. E. *HTML 5: guia prático*. 2. ed. São Paulo: Saraiva, 2014.

5.3 Tipos de navegação

Neste tópico, apresentaremos os principais tipos de navegação e os principais tipos de páginas *web*. Veremos que existe uma correlação entre o tipo de navegação e o tipo de *site* adequados para determinado desenvolvimento.

5.3.1 Categorias de navegação

De acordo com Kalbach (2009), existem três tipos principais de navegação:

- Navegação estrutural.
- Navegação associativa.
- Navegação utilitária.

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* (KALBACH, 2009).

Na navegação associativa, temos o estabelecimento de vínculos entre páginas com assuntos e conteúdos similares, independentemente da localização dessas páginas no *site*. Nesse caso, os *links* costumam passar através das fronteiras estruturais do *site* (KALBACH, 2009).

Na navegação local (em nível de página), o usuário trafega em uma única categoria. Comumente, a navegação local trabalha de maneira conjunta com um sistema de navegação principal, configurando-se como uma extensão da navegação principal.

A figura a seguir apresenta as disposições mais frequentes da navegação principal e da navegação local, que são L invertido, horizontal e vertical embutido.

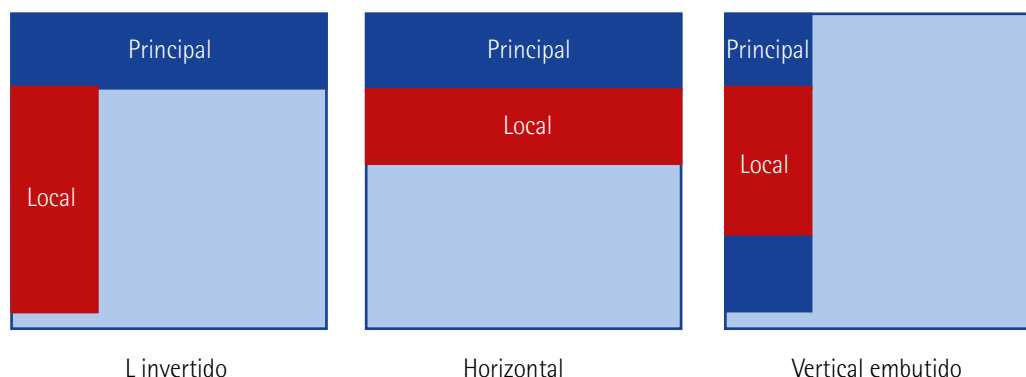


Figura 31 – Disposições frequentes das navegações principal e local

5.3.3 Navegação associativa

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 (KALBACH, 2009).

A navegação associativa pode ser realizada por meio de (KALBACH, 2009):

- Navegação contextual.
- Navegação de rodapés.

A navegação contextual é realizada nas proximidades do conteúdo de uma página web. Nesse caso, cria-se uma conexão direta entre o significado de um texto específico e as páginas relacionadas a ele.

As duas formas típicas de navegação contextual em um *site* são:

- Navegação embutida.
- Navegação por *links* relacionados.

Na navegação embutida, os *links* estão colocados no próprio texto. Na navegação por *links* relacionados, os *links* estão colocados no fim do texto ou ao lado do conteúdo. A figura a seguir apresenta esses tipos de navegação contextual.

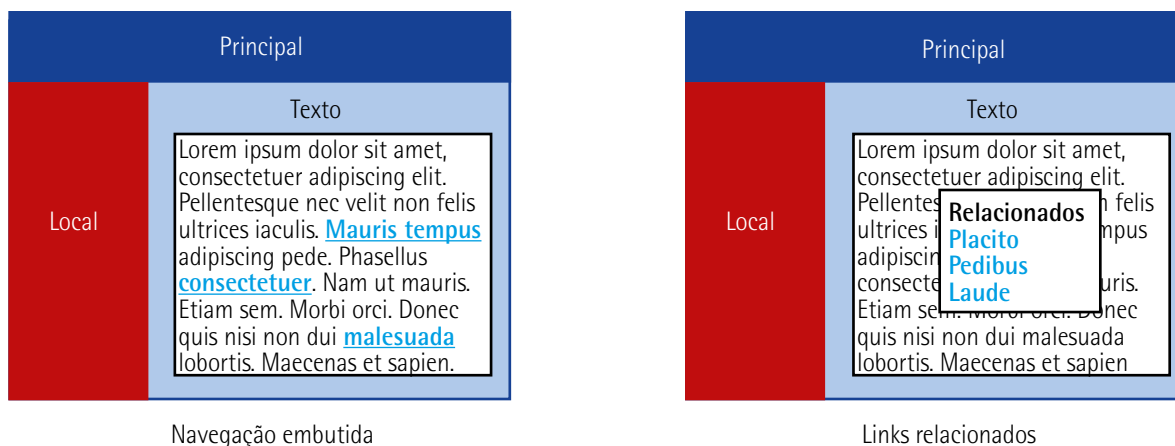


Figura 32 – Tipos de navegação contextual

Vale dizer que temos, também, os *links* rápidos, que oferecem acesso a conteúdos relevantes ou a áreas do *site* não representadas em uma navegação principal. A diferença fundamental entre a navegação por *links* rápidos e a navegação contextual é que os *links* rápidos são contextuais para o *site* inteiro, e não para dada página, como ocorre na navegação principal.

Os *links* rápidos estão frequentemente localizados no topo ou nos lados de uma página. Quando são colocados em páginas seguintes à página principal, os *links* rápidos podem ser transformados em um menu *drop-down* ou em um menu dinâmico (KALBACH, 2009).



Observação

Os menus dinâmicos oferecem acesso rápido às opções de navegação e precisam da interação do visitante para que possam ser exibidos.

Os menus *drop-down* são empregados na seleção HTML com opções. Nesse caso, após o usuário selecionar uma opção, há o seu direcionamento para uma nova página *web*.

A navegação de rodapés é feita na seção final de uma página *web* e é comumente representada por *links* textuais. Esse tipo de navegação é realizado quando desejamos obter informações suplementares, que não estão estritamente relacionadas ao conteúdo do *site*, como termos e condições de uso, informações de *copyright* e créditos do *site* (KALBACH, 2009).

5.3.4 Navegação utilitária

A navegação utilitária engloba ferramentas e funcionalidades que contribuem para a melhor utilização do *site* por parte dos usuários. Essas páginas geralmente não são encontradas na hierarquia do menu principal do *site*. Por exemplo, *links* para um formulário de busca ou para páginas de ajuda não estão presentes nos sistemas de navegação (KALBACH, 2009).

Uma das maneiras de efetuarmos a navegação utilitária pode ser pelo uso das caixas de ferramentas, que unificam as opções de um *site* considerando as funções realizadas. Outro modo de procedermos à navegação utilitária é pelo emprego dos seletores de idiomas em *sites* que apresentam opção de múltiplas línguas.



Observação

Podemos dizer que não é uma boa prática a utilização de imagens das bandeiras dos países para indicar a troca da língua de um *site*, pois um mesmo idioma pode ser falado em diversos países. O português, por exemplo, é língua oficial em oito países. Além disso, há países com mais de uma língua oficial.

Temos também de considerar que podem existir páginas muito extensas. Nessa situação, para evitar que o usuário perca muito tempo realizando a rolagem da página, podem ser adicionados *links* para páginas internas, que permitem pular de uma seção da página para outra. Muitas vezes, vemos, no fim da página, um *link* para voltar ao topo da página, o que é considerado uma navegação interna.

5.4 Tipos de páginas web

Dissemos que há uma correlação entre o tipo de navegação em um *site* e o tipo de página *web* a ser escolhido. Cada página no *site* deve ter uma razão de existir, e isso precisa ficar claro para os visitantes do *site* (KALBACH, 2009).

Podemos agrupar as páginas *web* nas seguintes categorias (KALBACH, 2009):

- Páginas navegacionais.
- Páginas de conteúdo.
- Páginas funcionais.

As páginas navegacionais visam fazer o direcionamento dos visitantes ao conteúdo procurado. A página principal (*home page*), as galerias e as páginas de aterrisagem (*landing pages*) são exemplos de páginas navegacionais.



Observação

As páginas de aterrisagem apresentam um panorama das principais categorias de um *site*. Analogamente à *home page*, que fornece uma visão completa do *site*, as páginas de aterrisagem consolidam o conteúdo de certa divisão do *site*.

As 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. As páginas de conteúdo representam valor fundamental na *web* (KALBACH, 2009).

As páginas funcionais possibilitam que os internautas realizem ações como 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 cadastros. Assim, páginas de busca, aplicações do *site* e formulários de submissão são alguns exemplos de páginas funcionais (KALBACH, 2009).



Observação

As aplicações *web* correspondem a um conjunto de páginas que apresentam funcionalidades e características interativas (KALBACH, 2009).

6 PUBLICAÇÃO DE UM SITE

6.1 Exemplo de ferramenta para elaboração de sites: WordPress

O WordPress é uma plataforma do ambiente *web* destinada à publicação e à gestão de conteúdos. Trata-se da Content Management System (CMS) mais difundida no planeta e é usada por mais de dezenas de milhões de *sites* e por empresas de vários portes.

Por meio do WordPress, é possível publicar conteúdos na internet de forma rápida e relativamente simples, com grau interessante de customização, e trabalhar de forma colaborativa com todos os administradores do *site*.

Vale destacar que o WordPress é uma plataforma de código aberto (*open source*) e que fornece suporte em mais de cinquenta idiomas. Segundo informações do *site* W3Tech, seis em cada dez *sites* com sistemas de gerenciamento de conteúdo utilizam WordPress.

Algumas das vantagens oferecidas por essa plataforma são o fato de se tratar de um sistema flexível, estável, administrável e que conta com uma grande comunidade de desenvolvedores que contribuem ativamente para o seu desenvolvimento contínuo e sua evolução.

Visto que o WordPress é uma das plataformas mais maduras e já testadas da internet, temos nível elevado de garantia de ocorrência de otimizações constantes, que lhe asseguram estabilidade e velocidade. Também precisamos mencionar a sua flexibilidade, resultado da utilização de *plugins* que estendem as funcionalidades do WordPress. Por exemplo, os *plugins* usados simplificam a inclusão de formulários de contato no *site*, o que pode transformá-lo em um *e-commerce*, um fórum ou uma rede social.

Pelo fato de o WordPress ser *open source* e livre de direitos comerciais, há uma extensa e variada comunidade de *designers* e desenvolvedores que fazem complementações e implementam melhorias na plataforma (muitas vezes, de forma gratuita).

Em função da elevada popularidade atingida pelo WordPress, uma grande quantidade de serviços de hospedagem de *sites* (ou *hostings*) já oferece um processo de instalação automatizado dessa plataforma, o que garante que os conteúdos sejam publicados em questão de minutos.

Há uma área administrativa no WordPress em que é possível gerenciar os usuários de determinado *site* WordPress, os níveis de acesso realizado, os conteúdos, os *plugins* e os *templates*.



Observação

Um *template*, que pode ser traduzido como modelo em português, é uma estrutura já pronta para uso, mas que pode ser personalizada para assumir determinada identidade visual. Trata-se do que podemos chamar de tema.

Temos duas versões de WordPress:

- A versão gratuita, conhecida como wordpress.org (ou versão da comunidade).
- A versão paga, conhecida como wordpress.com.

A versão gratuita permite sua instalação no servidor do usuário, dispõe de recursos de customização, oferece a possibilidade de criação de novas funcionalidades e novos *templates*, por exemplo.

A versão paga é contratada diretamente no site www.wordpress.com. Essa versão oferece serviços de hospedagem e de manutenção e fornece suporte da própria equipe desenvolvedora do WordPress. Trata-se de uma ferramenta prática e de fácil manipulação mesmo para quem não detenha conhecimentos aprofundados nas áreas de computação e de tecnologia.

Nas figuras a seguir, temos capturas de tela do *site* de Christiane Mazur Doi, professora titular da UNIP, feitas no WordPress.

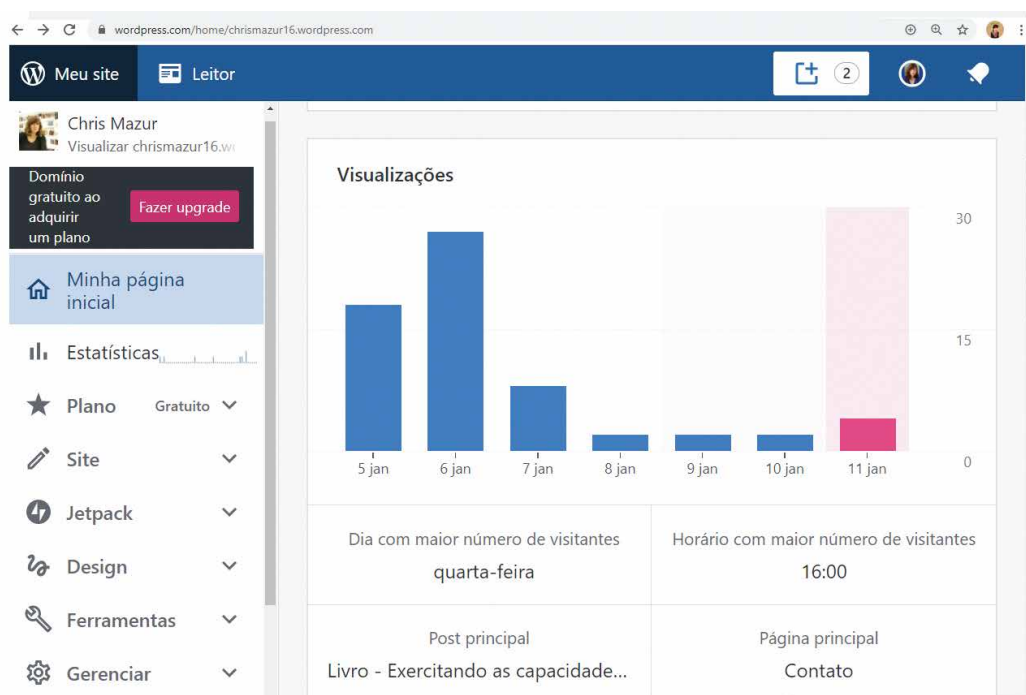


Figura 33 – Captura de tela (parte 1): WordPress de endereço <https://chrismazur16.wordpress.com>

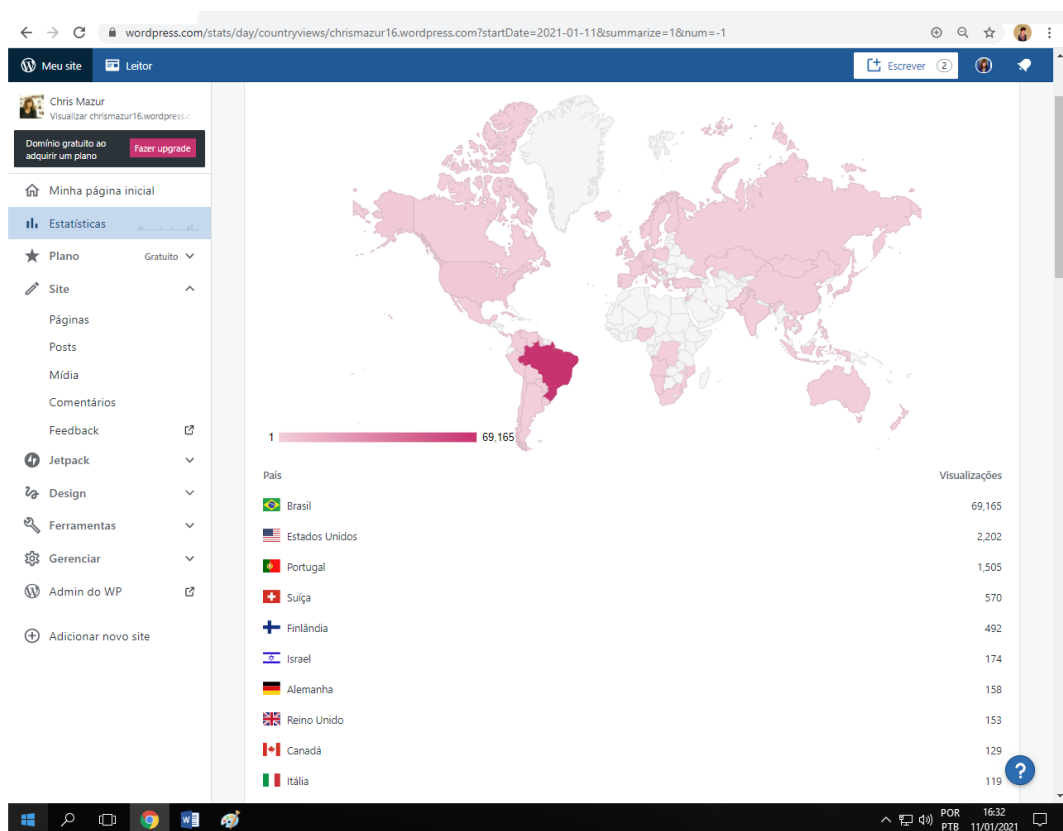


Figura 34 – Captura de tela (parte 2): WordPress de endereço <https://chrismazur16.wordpress.com>

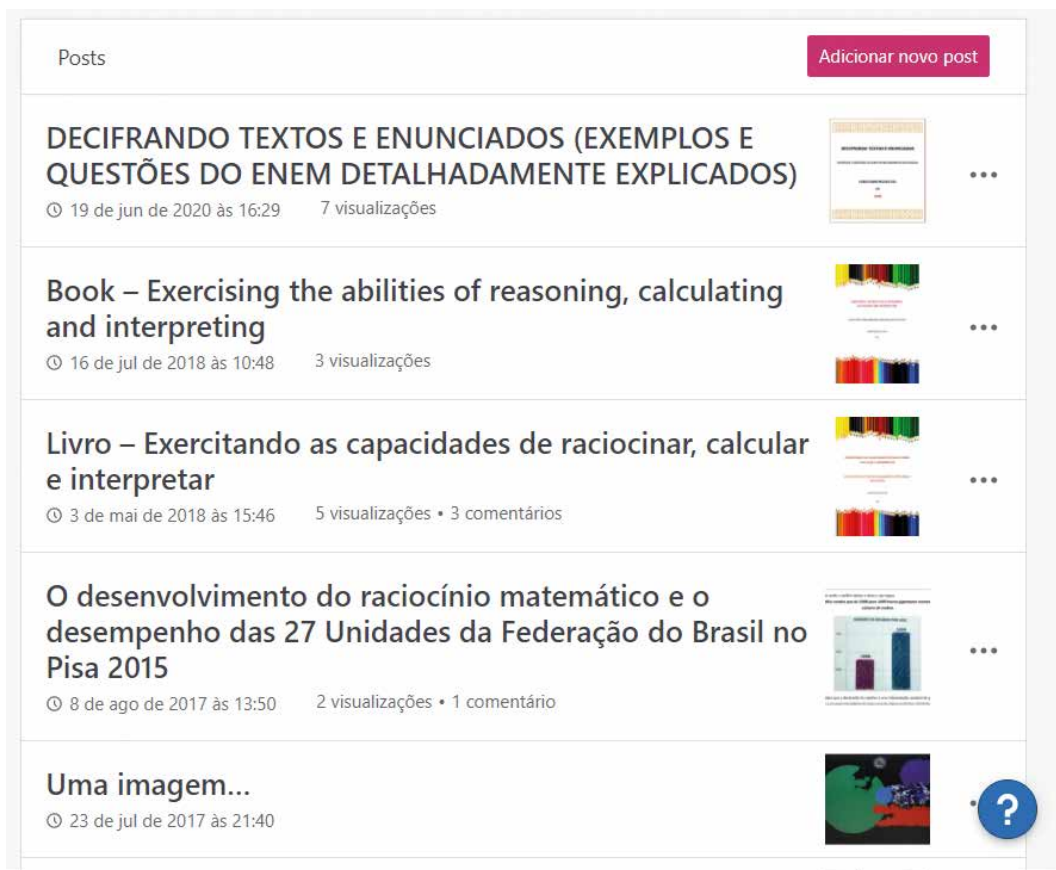


Figura 35 – Captura de tela (parte 3): WordPress de endereço <https://chrismazur16.wordpress.com>

6.2 Links e navegação web

De acordo com Kalbach (2009), podemos conceituar a navegação web das três maneiras apresentadas a seguir:

- A navegação web é a forma como as pessoas mudam de página para outra página na internet.
- A navegação web refere-se a todos os *links*, rótulos e componentes que geram acesso a páginas da internet e que auxiliam as pessoas a orientar-se durante a interação com um *website*.
- A navegação web diz respeito ao processo de busca focado em objetivos específicos e na localização de informação.

Os *links* consistem em textos ou elementos gráficos presentes em uma página web e que conectam essa página a outra página ou a uma localização diferente da mesma página. Assim, os *links* mostram a relevância de uma página pela sua associação com outra.

O clique do usuário em uma página web é uma decisão por ele tomada: cada clique exige que o usuário examine uma nova página e tome a decisão de clicar ou não em algum objeto do documento.

No caso de *sites* de venda de produtos e de serviços, é especialmente interessante que as páginas sejam o mais agradável possível de serem navegadas e que tenham *links* fartos e eficientes para que o consumidor tome a decisão de compra.

6.3 Sites informativos e sites interativos

Segundo Bell (2000), os *sites* existentes na *web* apresentam duas finalidades principais: informar e interagir. Assim, com base nessa concepção, temos:

- *Sites* informativos.
- *Sites* interativos.

Nos *sites* informativos, há a necessidade de que 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. Logo, o valor de um *site* informativo reside na sua habilidade de apresentar a informação desejada para seus usuários de modo categorizado e com fácil acesso.

Nos *sites* interativos, existe a demanda por grande capacidade de processamento de dados e por programação avançada, com o objetivo de que as aplicações funcionem de maneira eficaz. Além disso, o valor de um *site* interativo está, também, nas características da sua interface.

6.4 Fases do processo de criação de sites

Após a reunião inicial com o cliente, o desenvolvedor de *sites* que use o processo em cascata (*waterfall*) pode seguir, com a possibilidade de variações e inclusões, as fases indicadas a seguir.

- **Fase 1:** elaboração do *briefing*, termo que pode ser livremente traduzido como resumo em português. Trata-se do documento que contém informações sobre as necessidades a serem atendidas pelo projeto. Podemos dizer que o *briefing* é uma espécie de questionário que contém perguntas sobre a missão institucional, o histórico da organização, as características dos produtos e dos serviços da empresa, o perfil do público-alvo, as condições da concorrência etc.
- **Fase 2:** envio do orçamento ao cliente.
- **Fase 3:** aprovação do orçamento pelo cliente.
- **Fase 4:** elaboração do esboço do *site*, etapa em que pode ser feito o que chamamos de *wireframe*, um protótipo da página *web*.
- **Fase 5:** envio do esboço do *site* ao cliente.
- **Fase 6:** aprovação do esboço do *site* pelo cliente.

- **Fase 7:** desenvolvimento do *design* ou *layout* do *site* objetivando a criação de menus e de páginas em conformidade com as especificações do cliente. Todos os itens da estrutura do *site* e suas explicações devem ser devidamente documentados.
- **Fase 8:** desenvolvimento efetivo do *site*, incluindo a escrita dos códigos tanto de *back end* (parte não disponível ao usuário, mas essencial para o funcionamento do *site*) quanto de *front end* (parte visível na tela para o usuário, que inclui textos, imagens, animações, áudios e vídeos).
- **Fase 9:** realização de testes de validação e de Search Engine Optimization (SEO), traduzido literalmente como "otimização para os motores de busca". O SEO refere-se a uma série de técnicas que influenciam os algoritmos dos buscadores para determinar o posicionamento de uma página *web* para dada palavra-chave pesquisada.
- **Fase 10:** definição das ferramentas usadas para a administração e a divulgação do *site* e das estratégias de *marketing*.
- **Fase 11:** aprovação final do *site* pelo cliente.

Após o lançamento do *site*, realizam-se a manutenção e a implementação de melhorias contínuas. Esse tipo de processo de criação de *sites* está sujeito ao risco de ocorrência de atrasos.

6.5 Design de navegação: amplitude e profundidade

Segundo Kalbach (2009), todo *site* apresenta:

- Amplitude, que se refere ao número de itens de menu existentes em uma página.
- Profundidade, que se refere ao número de níveis hierárquicos existentes na estrutura.

Deve existir um balanço entre amplitude e profundidade, pois há um compromisso entre ambos (KALBACH, 2009):

- Quanto mais itens de navegação de uma vez (maior amplitude) houver, menos níveis de hierarquia (menor profundidade) haverá.
- Quanto menos itens de navegação (menor amplitude) houver, mais níveis de hierarquia (maior profundidade) haverá.

A figura a seguir ilustra um mesmo número de páginas organizado de formas diferentes com base na amplitude e na profundidade.

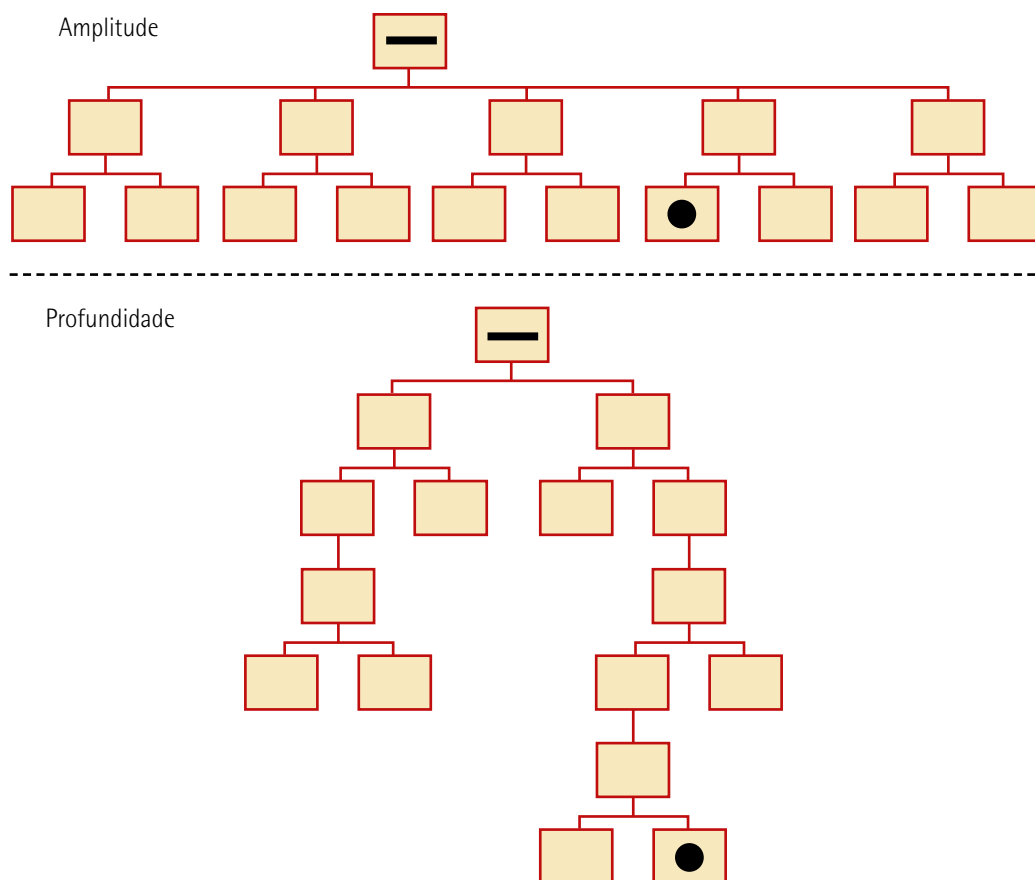


Figura 36 – Formas de organizar um *site* com base na amplitude e na profundidade

6.6 Características desejáveis para um *site*

Entre as características mais desejáveis que um *site* deve apresentar, estão a 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. Isso é conhecido como usabilidade. Nesse sentido, vale destacar que, em geral, o tempo médio de permanência em uma página *web* é da ordem de segundos e que não há treinamentos nem são feitas leituras de manuais por um usuário antes de ele acessar determinado *site*.

O *design* da interface precisa ser atraente e consistente e trazer conforto ao usuário. Assim, preferencialmente, para otimizar a navegação, preconiza-se que, em todas as páginas do *site*, haja padronização dos rótulos e do *layout* e manutenção dos *links* nas mesmas posições da tela.

Muitas vezes, é necessário fornecer *feedback* aos visitantes que navegam em um *site*, para que eles sejam comunicados a respeito do sucesso de suas ações, por exemplo. Assim, a presença de tutoriais, vídeos instrutivos, textos e rótulos é importante para que os usuários recebam informações.

A clareza visual do *site* é determinante para que o visitante seja motivado a nele permanecer e seja orientado a como nele navegar. Logo, a existência de elementos visuais atraentes e o uso de cores, fontes e *layouts* adequados são decisivos para o sucesso do *site*.

Além disso, 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 de páginas que abrem rapidamente.

Particularmente para o caso de *sites* que praticam o comércio eletrônico, uma funcionalidade interessante é a chamada trilha de navegação (*breadcrumb*), que permite que o usuário saiba em que página está e entenda como voltar para menus anteriores.

Em relação a *sites* que solicitam o preenchimento de campos de formulários ou a digitação de dados pessoais ou empresariais, deve-se considerar que as informações precisam ser solicitadas com clareza. Além disso, deve-se garantir o sigilo e a segurança das informações fornecidas pelos usuários.

6.7 Publicação de páginas web e sites

Silva (2016) propôs um tutorial para publicação de páginas web e *sites*, conforme descrito a seguir.

Primeiramente, deve-se elaborar o *site* de forma que as várias páginas em arquivos HTML sejam agrupadas de modo coerente, lógico e articulado. Escolhas adequadas em termos de estrutura, identidade visual, tamanho de fonte e paleta de cores auxiliam na autêntica expressão do conteúdo do projeto.

O *site* deve ser padronizado no sentido de ter sua identidade visual exibida em um *template*, que será utilizado como modelo para suas páginas web. As páginas, produzidas com estrutura definida, são inseridas em tabelas no arquivo HTML.

Durante a elaboração das páginas web, os arquivos precisam ser inseridos em um mesmo diretório, que será, posteriormente, publicado no servidor.

Depois que todas as páginas web forem produzidas, deve-se elaborar um menu contendo expressões claras, curtas e diretas. Tal menu deve ser reproduzido em todas as páginas do *site* a fim de estabelecer vínculos (*hiperlinks*) entre elas. Dessa forma, a navegação no *site* poderá ser fluida e permitirá que o visitante volte facilmente a determinada página que lhe despertou interesse.

A introdução de botões do tipo "Retornar ao Topo" é uma iniciativa interessante no caso de páginas que se estendam além da tela do usuário.

Na página inicial do *site*, recomenda-se que o menu ocupe posição de destaque e seja facilmente acessível.

Quando a construção do *site* é finalizada, deve-se registrar um nome de domínio, ou seja, uma URL, acrônimo de Uniform Resource Locator. Por exemplo, o domínio da empresa fictícia Grande Empresa na web pode ser www.grandeempresa.com.br, se tal nome estiver disponível para utilização. No Brasil, para registrar um *site*, deve-se acessar o *site* www.registro.br, responsável pela regulamentação dos endereços de internet no nosso país.

Concluído o registro do domínio, deve-se hospedar o *site* em um servidor para que ele tenha seu acesso disponibilizado aos usuários. Há vários tipos de serviços de hospedagem, pelos quais são cobrados variados valores de mensalidade.

Alguns desses tipos de hospedagem de *sites* são:

- Hospedagem compartilhada.
- Hospedagem de servidor privado virtual.
- Hospedagem na nuvem (*cloud*).

Na hospedagem compartilhada, todos os *sites* hospedados no mesmo servidor compartilham todos os recursos, como memória, capacidade de processamento e espaço em disco. Trata-se de uma opção indicada para empresas pequenas e *blogs* pessoais, que demanda baixo gasto e reduzida necessidade de conhecimento técnico. Além disso, a incumbência da manutenção e da administração do servidor fica a cargo da empresa de hospedagem. Entretanto, há ausência de controle sobre as configurações do servidor.

Na hospedagem de servidor privado virtual, ou Virtual Private Server (VPS), embora exista o compartilhamento do servidor com outros usuários, há o emprego da técnica de virtualização, em que se aloca para determinado usuário uma partição no servidor com recursos privados de capacidade de processamento, espaço em disco e tamanho da memória. Trata-se de uma opção indicada para empresas de médio porte, que proporciona um espaço exclusivo para o *site*, de modo que o tráfego em um *site* não afeta o desempenho de outro. Contudo, é uma solução mais custosa do que a hospedagem compartilhada, e, para gerenciar o servidor, é necessário conhecimento técnico.

Na hospedagem na nuvem (*cloud*), oferece-se ao *site* um *cluster* de servidores, sendo que os arquivos e os recursos envolvidos são replicados em cada servidor. Isso aumenta a confiabilidade, pois, se um dos servidores *cloud* está ocupado ou indisponível, o tráfego é direcionado automaticamente para outro servidor do *cluster*, o que diminui o tempo de inatividade ou indisponibilidade. Além disso, falhas em um servidor não afetam o desempenho do *site*. No entanto, os custos podem ser elevados, pois dependem dos recursos utilizados.

7 SEGURANÇA NA WEB

De acordo com o Instituto Nacional de Padronização e Tecnologia dos EUA, o termo "segurança computacional" pode ser definido como a proteção oferecida a um sistema de informações automatizado a fim de que sejam atingidos os objetivos relativos à preservação da integridade, da disponibilidade e da confidencialidade dos recursos do sistema de informações, o que inclui *hardware*, *software*, *firmware*, informações e dados (NIST, 1995).

Analisando somente do ponto de vista da internet, Cisco (2020) afirma que a segurança cibernética é o esforço contínuo para proteger esses sistemas em rede e todos os dados de usos não autorizados ou prejudiciais.

7.1 Conceitos de segurança na web

Vamos, neste tópico, discorrer a respeito de conceitos utilizados na segurança na web. Começemos com o conceito de vulnerabilidade.

A definição de vulnerabilidade relaciona-se aos termos definidos a seguir (STALLINGS, 2008):

- **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 alterações ou 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.



Lembrete

Os três principais pilares para a segurança web são: confidencialidade, integridade e disponibilidade; em inglês, *confidentiality*, *integrity* e *availability*, respectivamente. Na língua inglesa, esses conceitos formam o acrônimo CIA.

A figura a seguir mostra um esquema da definição de vulnerabilidade.

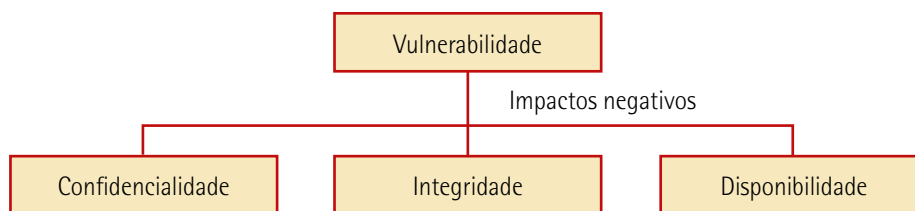


Figura 37 – Esquema da definição de vulnerabilidade

Dos conceitos estudados, depreendemos que (STALLINGS, 2008):

- A perda da confidencialidade causa a divulgação não autorizada de informações.
- A perda da integridade acarreta a modificação ou a destruição não autorizada de informações.

- A perda da disponibilidade gera o impedimento ao acesso ou ao uso de informações.

Os serviços de segurança são oferecidos por uma camada de protocolo de comunicação de sistemas abertos e visam garantir a segurança adequada dos sistemas e das operações de transferências de dados. Esses serviços têm o objetivo de implementar políticas de segurança por meio da instalação de mecanismos de segurança e podem ser classificados nas categorias a seguir (STALLINGS, 2008):

- autenticação;
- controle de acesso;
- confidencialidade dos dados;
- integridade dos dados;
- irretratabilidade.

A espionagem industrial, a falsificação de identidade, o roubo de saldos em dinheiro e a posse indevida de informações de valor (ou ainda sua possível modificação) são exemplos de ações que podem causar danos, cuja prevenção justifica esforços e investimentos consideráveis por parte de empresas de quaisquer portes.

Violações da segurança do sistema ou sua má utilização podem ser classificadas em intencionais (maliciosas) ou acidentais (SILBERSCHATZ; GALVIN; GAGNE, 2015). No entanto, as últimas são normalmente identificadas e/ou evitadas pelos mecanismos clássicos de proteção presentes em qualquer sistema operacional contemporâneo.

Para falar sobre segurança, aqui usamos os termos descritos a seguir (SILBERSCHATZ; GALVIN; GAGNE, 2015).

- **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 a descoberta de uma vulnerabilidade.
- **Ataque:** trata-se da tentativa de violação da segurança de um sistema computacional.

A lista a seguir mostra alguns tipos de violações acidentais e maliciosas da segurança (SILBERSCHATZ; GALVIN; GAGNE, 2015):

- **Violação de sigilo:** refere-se à duplicação não autorizada de informações. Esse é o tipo mais comum de violação e destina-se à obtenção de informações sigilosas, usualmente com finalidades políticas, estratégicas, financeiras ou de competitividade.

- **Violação de integridade:** refere-se a uma classe de violação em que os dados são modificados de forma não intencional e/ou não autorizada. Esse tipo de violação pode ocorrer por meio do sequestro de dados (em que o atacante visa receber um resgate) ou pode ser efetuado apenas para causar dano aos legítimos donos das informações.
- **Violação de disponibilidade:** refere-se a uma classe de violação em que os dados não são modificados, mas, sim, destruídos. Em geral, os invasores que praticam a violação de disponibilidade visam aumentar o *status* dos invasores perante seus pares, defender alguma causa ou demonstrar uma vulnerabilidade (usualmente, pela aplicação de um método ilegal de grande visibilidade).
- **Furto de serviço:** refere-se a uma classe de violação em que o objetivo do invasor é se aproveitar de algum recurso computacional de forma não autorizada.
- **Recusa de serviço:** refere-se a uma classe de violação em que o invasor visa impedir que um sistema continue operando normalmente e oferecendo sua funcionalidade. Um exemplo clássico de recusa de serviço refere-se aos chamados ataques DoS, ou Denial of Service. Outra versão desse mesmo tipo de ataque é chamada de DDoS, ou Distributed Denial of Service. Esse tipo de ataque é tipicamente feito por meio de diversas máquinas comprometidas externas ao sistema que se quer bloquear, que súbita e concomitantemente passam a inundar a rede com pedidos de conexão que acabam por impedir o funcionamento normal da máquina.



Saiba mais

Para saber mais sobre o ataque de DDoS, leia:

O QUE são ataques de DDoS? *Kaspersky*, 2021.

Disponível em: <https://bit.ly/2R1KjwQ>. Acesso em: 9 set. 2020.

O mais comum dos ataques a parques computacionais é a personificação, em que um participante de uma comunicação finge ser alguém que não é, ou seja, finge ser outra pessoa ou outra máquina. Por meio da personificação, o agressor viola a autenticação da identidade e pode, assim, obter acessos que, normalmente, não receberia (SILBERSCHATZ; GALVIN; GAGNE, 2015).

Um ataque bastante frequente é aquele que envolve a interceptação e a gravação de uma transmissão de dados. Posteriormente, o invasor faz com que essa gravação seja executada de novo, com o objetivo de tentar repetir o resultado da transmissão original. Por esse motivo, tal ataque é chamado de reexecução. De modo alternativo, o atacante pode tentar manipular os dados gravados, a fim de alterar o comportamento original (SILBERSCHATZ; GALVIN; GAGNE, 2015).

Outra forma de ataque que utiliza as telecomunicações digitais é o chamado ataque do intermediário. Lembremos que, em comunicações, dizemos que o emissor é o dispositivo que envia

uma mensagem, enquanto o receptor é o dispositivo que recebe. Em uma rede de computadores, todos os computadores podem ter esses dois papéis, mas vamos imaginar um cenário simplificado, supondo um retrato da comunicação em dado instante, com uma máquina enviando dados e outra recebendo. Na estratégia do ataque do intermediário, o atacante coloca-se no meio dessa comunicação, fingindo ser um emissor para a máquina que está recebendo e um receptor para a máquina que está enviando. Nesse caso, o invasor pode, inclusive, modificar a comunicação, normalmente com alguma finalidade maliciosa.

Conforme Silberschatz, Galvin e Gagne (2015), existem quatro níveis de medidas necessárias para assegurar um parque computacional:

- Medidas de natureza física.
- Medidas de natureza humana.
- Medidas do sistema operacional.
- Medidas da rede.

No caso das medidas de natureza física, a preocupação fundamental está na integridade dos equipamentos e dos locais em que eles estão instalados. Nessa situação, precisamos observar que de nada adianta ter um sistema computacional extremamente seguro (do ponto de vista de *software*) se qualquer pessoa pode acessar fisicamente a máquina na qual o sistema executa. É por isso que os *datacenters* de grandes empresas devem funcionar em um ambiente cuidadosamente controlado, no qual haja apenas a permissão da entrada de pessoas autorizadas.

Uma vez superados os aspectos físicos de acesso às máquinas, temos as questões humanas. Do ponto de vista da segurança, queremos que somente os usuários autorizados sejam capazes de utilizar um sistema. O problema é que esses usuários, por motivos psicológicos, por exemplo, podem permitir que outras pessoas utilizem o sistema no seu lugar. Mesmo que um sistema force o usuário a ter uma senha complexa, nada impede que ele escreva essa senha em um papel e deixe-a sobre a sua mesa, em um lugar no qual qualquer pessoa possa vê-la. Usuários podem também ser enganados por pessoas que se façam passar por administradores de sistemas ou por altos executivos. Dessa forma, as questões humanas oferecem uma série de desafios adicionais no quesito da segurança.

O sistema operacional também deve ser projetado para ser seguro. Além disso, ele precisa ser implementado de forma segura. Adicionalmente, tanto a manutenção do sistema operacional quanto a instalação de atualizações visam garantir que, uma vez que vulnerabilidades ou problemas sejam encontrados, eles sejam corrigidos o mais rapidamente possível. Atacantes profissionais especializam-se em buscar vulnerabilidades nos sistemas operacionais mais comuns, tentando explorar potenciais falhas e brechas de segurança.

Finalmente, a rede de computadores deve ser segura: muitos problemas de segurança são oriundos de ataques e invasões de redes de computadores. A comunicação via rede também é um problema,

especialmente quando pensamos em redes públicas. O uso de algoritmos de criptografia forte na comunicação é feito para assegurar a integridade e o sigilo das comunicações. O monitoramento das redes é fundamental para garantir a segurança de um parque de máquinas.

É interessante observar que esses quatro aspectos, ou níveis, são complementares. Falhas na segurança em um desses aspectos afetam todos os demais. Por exemplo, falhas humanas, que ocasionem a permissão do acesso de pessoas não autorizadas, podem burlar completamente o esquema de proteção de uma rede. É fundamental que seja adotada uma visão integrada para trabalhar com a segurança de computadores (SILBERSCHATZ; GALVIN; GAGNE, 2015).



Saiba mais

O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a internet no Brasil, sendo sustentado pelo NIC.br, do Comitê Gestor da internet no Brasil. Esse grupo é responsável pelo tratamento a incidentes de segurança em computadores que estão em redes ligadas à internet no país.

No *site* da CERT.br, está disponível uma cartilha de segurança para internet, um documento com recomendações e dicas para o usuário de internet aumentar sua segurança. Leia para conhecer:

CERT.BR. *Cartilha de segurança para internet, versão 4.0*. São Paulo: Comitê Gestor da internet no Brasil, 2012. Disponível em: <https://bit.ly/2RA5TZc>. Acesso em: 6 dez. 2020.

7.1.1 Hackers e criminosos virtuais

Podemos entender os criminosos virtuais como indivíduos ou grupos de indivíduos que buscam explorar vulnerabilidades para ganho pessoal ou financeiro. Esses invasores estão interessados em informações diversas, como números de cartões de crédito e detalhes dos projetos de produtos.

O grupo dos *hackers* corresponde a um grupo de invasores que entra em computadores ou redes para obter acesso e, normalmente, tem amplo conhecimento de redes e programação. Dependendo da intenção da invasão, esses invasores são classificados como:

- Chapéu branco (*white hat*).
- Chapéu cinza (*grey hat*).
- Chapéu preto (*black hat*).

Os invasores *white hat* acessam redes ou sistemas de computadores com o consentimento de seus proprietários, visando à descoberta de fraquezas e vulnerabilidades, com o objetivo de melhorar a segurança. Essas invasões são feitas com prévia autorização, e todos os resultados são relatados ao proprietário para que a rede seja ajustada antes que alguém faça, de fato, algo prejudicial (BASTA; BASTA; BROWN, 2014).

Os invasores "do mal" (*black hat*) aproveitam qualquer vulnerabilidade para obter ganho pessoal, ganho financeiro, ganho político, fama etc. Esse tipo de *hacker* tenta entrar nos sistemas para fazer algo prejudicial, como roubar segredos comerciais, números de cartão de crédito, listas de clientes e de funcionários. Trabalha sem a sanção de organizações oficiais ou extraoficiais (BASTA; BASTA; BROWN, 2014).

Os invasores suspeitos (*grey hat*) situam-se entre os invasores "do bem" (*white hat*) e os invasores "do mal" (*black hat*). Quando esse tipo de *hacker* encontra uma vulnerabilidade em um sistema, ele pode relatar a vulnerabilidade aos proprietários do sistema se essa ação coincidir com sua agenda. Alguns *hackers grey hat* publicam os fatos sobre a vulnerabilidade na internet para que outros invasores possam explorá-la.

O quadro a seguir apresenta a variedade de motivações dos *hackers/crackers* de chapéu branco e de chapéu preto.

Quadro 2 – Motivações dos *hackers/crackers* de chapéu branco e de chapéu preto

Tipo de <i>hacker</i>	<i>Hackers</i> de chapéu branco	<i>Hackers</i> de chapéu cinza	<i>Hackers</i> de chapéu preto
Motivação e objetivos	Aprender assuntos novos; proteger a rede sob sua responsabilidade contra invasão ou danos; manter o <i>status quo</i> ; trabalhar com a sanção das organizações oficiais	Fama, crédito por resolver desafios na área de redes; <i>hackers</i> -ativistas realizam ativismos através da alteração de <i>sites</i> e redes de malfeitores, tais como empresas envolvidas em crimes ambientais ou temas sociais polêmicos	Pagamentos em dinheiro, ofensas; podem roubar segredos comerciais, listas de clientes, números de cartões de crédito; objetivam informações para obter lucro; trabalham sem a sanção de organizações oficiais ou extraoficiais

Fonte: Basta, Basta e Brown (2014, p. 3).

A acepção *hacker* é um tema controverso. Frequentemente, a imprensa e o público em geral empregam o termo para designar qualquer acusado de utilizar a tecnologia para fazer fraudes de cartão de crédito, ações de terrorismo, roubos de identidade e atos de vandalismo. Contudo, as comunidades de computação costumam atribuir a expressão *hacker* a um profissional especialista ou um programador de vasto conhecimento técnico, que tem satisfação em explorar sistemas computacionais e aprender mais sobre eles (KIM; SOLOMON, 2014).

No mundo da segurança, entende-se *hacker* como alguém que tenta invadir ou explorar um sistema. Ainda assim, há tipos diferentes de *hackers*, como vimos.

Temos grupos de *hackers* organizados, formados por empresas de criminosos virtuais, hacktivistas, terroristas e até *hackers* patrocinados por Estados. Os criminosos virtuais geralmente são grupos

profissionais, focados em obter controle, poder e riqueza. Trata-se, em geral, de criminosos altamente sofisticados e com elevada capacidade de organização que podem, inclusive, fornecer o crime digital como um serviço a outros criminosos. Os hacktivistas fazem declarações políticas para sensibilizar as pessoas para questões que são importantes para eles. Os invasores patrocinados por Estados reúnem informações ou cometem sabotagem em nome de um governo. Esses invasores geralmente são bem treinados e bem remunerados, e seus ataques são concentrados em objetivos específicos e benéficos para os governos que representam.

Outra categoria é a dos invasores amadores, também chamados de *hackers* inexperientes. Esse grupo é composto por invasores com limitada ou nenhuma qualificação profissional e que, frequentemente, usam ferramentas básicas, disponíveis na internet, para efetuar seus ataques. Apesar disso, os resultados dos seus ataques ainda podem ser devastadores.

Há, também, os *crackers*. Trata-se de um grupo que apresenta habilidades computacionais bastante sofisticadas, interessado em obter, de modo específico, ganhos financeiros. Esses tipos de atacantes configuram sérias ameaças aos recursos de informação e às redes, pois estão relacionados a fraudes, roubos e destruição de dados e bloqueios de acesso, entre outras atividades com intenções maldosas.

Os criminosos virtuais podem estar:

- dentro da empresa (*insiders*);
- fora da empresa (*outsiders*).

Vale destacar que os *insiders* podem ser funcionários insatisfeitos com a empresa, além de pessoas contratadas por empresas terceirizadas.

Um usuário interno, como um funcionário ou um parceiro de contrato, pode, de forma acidental ou intencional, fazer o que segue:

- Tratar erroneamente os dados confidenciais.
- Ameaçar as operações de servidores internos ou de dispositivos de infraestrutura de rede.
- Facilitar ataques externos conectando mídias USB infectadas no sistema de computador corporativo.
- Instalar acidentalmente um *malware* para a rede por *e-mail* ou por *sites* mal-intencionados.

As ameaças internas chegam a apresentar potencial de gerar maior dano que as ameaças externas, pois os usuários internos têm acesso direto ao edifício e aos seus dispositivos de infraestrutura, por exemplo. Os funcionários também podem ter conhecimento sobre a rede corporativa, seus recursos e seus dados confidenciais, além de saber a respeito dos diferentes níveis de usuários ou dos privilégios administrativos.

Ameaças externas de amadores ou de invasores habilidosos podem explorar vulnerabilidades na rede ou em dispositivos de computação ou usar a engenharia social para obter acesso ao sistema de uma empresa.

7.2 Brechas de segurança

Ainda que uma empresa adote medidas efetivas para proteger sua rede de computadores, há a chance de que atacantes experientes consigam acessar os recursos dessa rede. Isso porque existe o que chamamos de brecha de segurança, que pode ser definida como qualquer evento que tenha como consequência violações nos princípios de segurança, ou seja, violações na disponibilidade, na integridade e na confiabilidade de um sistema (KIM; SOLOMON, 2014).

Entre as várias atividades que podem originar brechas de segurança, temos as seguintes:

- Ataque de negação de serviço (DoS).
- Ataque de negação de serviço distribuída (DDoS).
- Modificações acidentais em dados.
- Espionagem telefônica (*wiretapping*).
- Comportamento inaceitável de navegador *web*.

7.2.1 Ataque de negação de serviço (DoS)

Um ataque de negação de serviço, ou DoS, tem como resultado a falta de acesso de usuários legítimos a dado recurso do sistema.

Um ataque de DoS é uma tentativa coordenada feita com a intenção de que um serviço tenha sua execução negada. Para isso, diversas tarefas não produtivas são executadas, o que torna o sistema indisponível para a realização de operações legítimas. No entanto, ao detectarmos um ataque de DoS, podemos impedir a sua continuidade de forma relativamente fácil.

Os primeiros ataques de negação de serviço foram realizados por *hackers* com o intuito de provar que a segurança de um *site* não era eficaz o bastante para que nunca pudesse ser quebrada. Como o DoS, podem acontecer ataques de cunho político e ataques de extorsão, em que se cobram valores dos *sites* por proteção.

Atualmente, não são apenas *hackers* especializados que realizam invasões. Dadas as facilidades que usuários comuns têm para obter ferramentas de ataque automáticas disponíveis na internet, tais usuários, mesmo apresentando conhecimentos elementares da área de segurança, podem se transformar em atacantes. Os próprios países, usando as máquinas de Estado, recursos financeiros e inteligência, têm condições de desenvolver ferramentas próprias com elevado potencial de sucesso em invasões.

Existem dois tipos principais de DoS, conhecidos por:

- "quantidade exorbitante de tráfego";
- "pacotes formatados maliciosamente".

No caso do tipo "quantidade exorbitante de tráfego", o invasor envia enorme quantidade de dados a tal velocidade que a rede, o servidor ou a aplicação não consegue suportar. Assim, ocorre diminuição na taxa de transmissão (resposta) ou surge uma falha em um dispositivo ou serviço.

No caso do tipo "pacotes formatados maliciosamente", o atacante envia um pacote formatado de forma maliciosa para um *host* ou um aplicativo, e o receptor não consegue contê-lo. Por exemplo, um aplicativo não pode identificar os pacotes que contêm erros ou os pacotes formatados incorretamente encaminhados pelo invasor. Isso causa lentidão ou falha na execução do dispositivo receptor.

Uma das melhores proteções contra os ataques de negação de serviço é a utilização de sistemas de prevenção de intrusos, ou Intrusion Detection Systems (IDS), que podem detectar ataques de DoS, alertar sua ocorrência quando estiver em progresso e, com isso, impedir o sucesso do ataque. Caso não exista essa defesa, os ataques de negação de serviço rapidamente dominam os servidores e outros *hardwares* da rede, o que reduz a vazão de dados úteis a patamares que chegam a forçar uma parada total do sistema.

Frequentemente, os ataques de DoS têm como alvo os pontos fracos na arquitetura geral de um sistema, que utiliza protocolos comuns da internet, como o TCP, o IP e o protocolo de controle de mensagem na internet, ou Internet Control Message Protocol (ICMP).

Um ataque de DoS direcionado contra um dos protocolos citados pode paralisar um ou mais servidores ou elementos de rede, inserir um volume gigantesco de pacotes inúteis na rede ou oferecer informações incorretas aos servidores. Esse tipo de ação é conhecido como inundação de pacotes ou ataque de inundação.

Em suma, no ataque de DoS do tipo inundação, são enviadas elevadas quantidades de solicitações inúteis para as máquinas com o intuito de arrasar o processador, a memória e os dispositivos de rede do computador.

Uma das técnicas mais populares de inundação de pacotes é chamada de inundação de SYN, ou SYN *flood*. O SYN é um *bit* de controle do protocolo TCP utilizado para a sincronização dos números de sequência dos pacotes. Nessa técnica, o atacante transmite grande número de pacotes, que solicitam conexões com o computador da vítima. Cada solicitação é registrada pela vítima, e é reservado um local para haver a conexão em uma tabela da memória, com o envio de uma confirmação para o agressor. O atacante não responde à confirmação: com isso, a tabela de conexões do computador atacado é preenchida, e esse computador fica aguardando a confirmação pendente. Quando a tabela de conexões é totalmente preenchida, um usuário legítimo não consegue mais conectar-se ao computador atacado,

que fica indisponível até o momento que as solicitações de conexões são canceladas por atingir o tempo limite sem resposta, isto é, até a ocorrência de *time out*.

Outra técnica de inundação de pacotes é denominada *smurfing*. Nela, o atacante, conhecido como *smurf*, utiliza a difusão direcionada para provocar a inundação do tráfego da rede.

Há outro tipo de ataque de DoS, denominado ataque lógico, em que falhas de *software* são usadas para comprometer o desempenho do servidor remoto. Uma forma de proteção contra esse tipo de ataque é a instalação das correções mais recentes ou de *patches* para manutenção do *software* atualizado, principalmente no que se refere ao sistema operacional.

7.2.2 Ataque de negação de serviço distribuída (DDoS)

O ataque de negação de serviço distribuída, ou DoS, ocorre com o emprego de muitos recursos computacionais. Nesse caso, os computadores são sobrecarregados com solicitações falsas, o que impede seu acesso por usuários legítimos.

Ataques desse tipo visam extinguir os recursos e causar indisponibilidades no objeto atacado. Com isso, os usuários que dependem desses recursos são impactados, visto que não conseguem realizar as operações pretendidas.

Ao final do ataque, os serviços que ficaram indisponíveis voltam a operar normalmente. Por exemplo, um ataque de negação de serviço distribuída pode ser feito da seguinte maneira: um invasor cria uma rede de *hosts* infectados, denominada *botnet*, composta por zumbis (os zumbis são os *hosts* infectados). O invasor usa um sistema de controle para monitorar os zumbis. Os computadores zumbis examinam e infectam constantemente mais *hosts*, o que cria números crescentes de zumbis. Quando está pronto para o ataque, o *hacker* instrui os sistemas controladores para fazer com que o *botnet* de zumbis execute um ataque de DDoS.

Vale notar que os principais alvos para ataques de DDoS são grandes empresas e universidades.

7.2.3 Ataque do tipo "porta dos fundos" (*backdoors*)

Vários desenvolvedores de *software* incluem no seu escopo de produção métodos de acesso ocultos aos programas denominados "porta dos fundos", ou *backdoors*. Por meio desses acessos, é possível entrar no sistema sem enfrentar muitos controles de segurança.

Se esses acessos permanecessem ocultos aos demais usuários, isso não representaria uma brecha de segurança. Entretanto, nem sempre as "portas dos fundos" permanecem ocultas: se um ataque descobrir sua existência, pode utilizá-las para driblar os outros dispositivos de segurança.

Na figura a seguir, temos um esquema de um ataque do tipo "porta dos fundos" (*backdoor*).

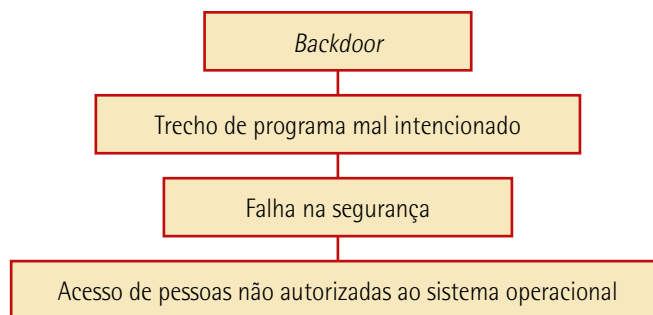


Figura 38 – Esquema de um ataque do tipo "porta dos fundos" (*backdoor*)



Lembrete

Uma porta aberta representa um serviço disponível, que pode ser conectado e, conseqüentemente, atacado por um criminoso virtual.

7.2.4 Ataque de espionagem telefônica (*wiretapping*)

Temos diversos modos de realizar um grampo telefônico em linhas de telefonia fixa e em linhas de comunicação de dados. Nesse sentido, a espionagem telefônica, ou *wiretapping*, pode ser classificada como:

- **Ativa:** quando o atacante realiza modificação no sinal da linha.
- **Passiva:** quando o atacante simplesmente tem acesso ao conteúdo do sinal da linha, mas não pode alterá-lo.

Na espionagem ativa, temos a espionagem telefônica com entrada em *piggyback*, na qual o atacante pode interceptar e modificar a mensagem original de forma a interromper a linha de comunicações. Com isso, o criminoso consegue rotear a mensagem para outro computador, que atua como hospedeiro.

Tradicionalmente, o termo *wiretapping* está associado a comunicações por voz. Para a interceptação de dados, é mais frequente o termo *sniffing*, ou farejador, que também é aplicado às interceptações de transmissão sem fio.

7.2.5 Ataque de navegação *web* inaceitável

Nos ataques de navegação *web* inaceitável, temos a utilização do navegador de forma não permitida pela política de determinada organização.

A política de uso aceitável, ou Acceptable Use Policy (AUP), é um documento que estipula os limites aos quais um usuário deve obedecer e as práticas que ele pode usar para ter acesso à rede corporativa ou à internet. Antes de ter acesso à rede em empresas e escolas, por exemplo, o usuário deve ler e aceitar essa política.

Um uso não aceitável de navegação *web* acontece quando, por exemplo, funcionários de uma empresa buscam arquivos ou diretórios em *sites* que exibem conteúdos inadequados.

8 AMEAÇAS NO AMBIENTE WEB

8.1 Tipos de ataques no ambiente web

Neste tópico, trataremos de alguns dos tipos de ataques mais comuns no ambiente *web*, apresentados a seguir.

- Falsificação de *e-mail*.
- Ataque de força bruta.
- Desfiguração de página (*defacement*).
- *Plugins*.
- Envenenamento de SEO.
- Engenharia social.
- Fraude de antecipação de recursos (*advance fee fraud*).
- Representação (*scam*) e farsas ou boatos (*hoax*).
- *Phishing*.
- *Pharming*, *smishing*, *vishing* e *whaling*.
- *Shoulder surfing*.

8.1.1 Falsificação de *e-mail*

Na técnica de falsificação de *e-mail*, ou *e-mail spoofing*, são feitas alterações nos campos do cabeçalho de um *e-mail* com a intenção de iludir o usuário com uma informação incorreta do remetente.

Por uma deficiência do protocolo do serviço de *e-mail* Simple Mail Transfer Protocol (SMTP), podem ser falsificados os seguintes campos:

- **"From"**: remetente da mensagem.
- **"Reply-To"**: endereço de resposta.
- **"Return Path"**: endereço para reportar erros no envio da mensagem.

Os atacantes utilizam endereços de *e-mail* coletados de computadores que foram contaminados e tentam fazer com que seus destinatários acreditem que partiram de pessoas conhecidas e confiáveis.

É relativamente comum recebermos *e-mails* de desconhecidos solicitando um clique no *link* disponibilizado na mensagem ou a execução de um programa anexado. Isso pode ocasionar um ataque do tipo falsificação de *e-mail*.

8.1.2 Ataque de força bruta

No ataque de força bruta, ou *brute force*, um atacante tenta acertar, por tentativa e erro, um nome de usuário e sua senha. Para isso, o criminoso executa diversos processos e obtém acesso a *sites*, computadores e serviços no nome do usuário lesado, com os mesmos privilégios desse usuário.

Essas tentativas de acerto são realizadas por meio de ferramentas automáticas, que visam tornar o ataque mais efetivo.

Adicionalmente, um ataque de força bruta pode iniciar um ataque de negação de serviço, dependendo da forma como é realizado, pois há sobrecarga no *site* resultante da grande quantidade de tentativas para acessá-lo em um período de tempo reduzido.

8.1.3 Desfiguração de página (*defacement*)

Na técnica de desfiguração de página, ou *defacement*, há a alteração de conteúdo de uma página *web* de um *site*. O atacante é chamado de *defacer* e explora:

- Erros e imprecisões da aplicação *web*.
- Vulnerabilidades do servidor.
- Fragilidades da linguagem de programação ou dos pacotes usados para desenvolver a aplicação.

Desse modo, o criminoso:

- Invade o servidor em que a aplicação está instalada.
- Altera diretamente os arquivos que formam o *site*.
- Furta senhas de acesso à interface *web* utilizada para administração remota.

As violações de segurança podem afetar os navegadores da *web* ou os *browsers* de forma a:

- Exibir anúncios de *pop-up*.
- Coletar informações pessoais identificáveis e sensíveis.
- Instalar *adwares*, vírus ou *spyware*.

8.1.4 Plugins

Os *plugins* Flash e Shockwave da Adobe permitem a criação de animações gráficas e desenhos que podem aprimorar de modo significativo o visual de uma página da *web*. Os *plugins* exibem o conteúdo desenvolvido usando o *software* apropriado.

Os *plugins* já tiveram um registro de segurança considerável. À medida que o conteúdo baseado em Flash cresceu e se tornou mais popular, os criminosos examinaram os *plugins* e os *softwares* Flash com mais detalhes, determinaram suas principais vulnerabilidades e exploraram o Flash Player.

A minuciosa exploração do Flash Player por parte de *hackers* pode causar uma falha no sistema ou permitir que um criminoso assuma o controle do sistema afetado. Espera-se que ocorra aumento nas perdas de dados à medida que os criminosos continuam analisando as vulnerabilidades dos *plugins* e dos protocolos mais populares.

8.1.5 Envenenamento de SEO

Os mecanismos de busca, como o Google, classificam as páginas encontradas e apresentam resultados relevantes com base nas consultas de pesquisas dos usuários.

De acordo com a relevância do conteúdo do *site*, ele pode aparecer em posição mais alta ou mais baixa na lista ordenada de resultados da pesquisa. O SEO, ou otimização de mecanismos de busca, é um conjunto de técnicas usadas para melhorar a classificação do *site* por um mecanismo de pesquisa.

Há empresas legítimas que se especializam na otimização de *sites* para melhor posicioná-los, mas o envenenamento de SEO usa esse mecanismo de modo desvirtuado, a fim de que um *site* mal-intencionado tenha destaque nos resultados de dada pesquisa.

O intuito do envenenamento de SEO é aumentar o tráfego em *sites* maliciosos que podem hospedar *malwares* ou executar engenharia social, tipo de ataque que veremos a seguir. Para forçar um *site* malicioso a obter uma classificação mais elevada nos resultados de pesquisa, os invasores utilizam termos de busca populares.

8.1.6 Engenharia social

A engenharia social é um ataque de acesso que tenta manipular indivíduos para realizarem ações ou divulgarem informações confidenciais. Trata-se de uma técnica por meio da qual uma pessoa visa persuadir outra pessoa a executar determinadas ações. Com frequência, os engenheiros sociais baseiam-se na vontade que as pessoas apresentam em ajudar para tirar partido de suas fraquezas (CERT.BR, 2012).

Um exemplo desse tipo de ataque é o seguinte:

- Um atacante contata um funcionário autorizado e faz questionamentos a respeito de um problema urgente, que requer o acesso imediato à rede.
- O atacante pode apelar ao orgulho do funcionário ou invocar autoridades, utilizando a citação de nomes ou apelando à cobiça do funcionário.
- O funcionário cede às pressões do atacante.

O sucesso de ataques desse tipo depende, em grande parte, da tendência das pessoas em desejar ser útil.

Na engenharia social, o elemento humano é inserido como uma brecha de segurança. Pessoas responsáveis pelo atendimento ao cliente, como recepcionistas e auxiliares administrativos com poucos conhecimentos sobre a empresa, são alvos preferenciais de ataques de engenharia social.

Na figura anterior, que ilustra um ataque do tipo "porta dos fundos" (*backdoor*), temos um exemplo de ação de engenharia social.

Vejamos, a seguir, dois tipos desse ataque.

- **Pretexting**: ocorre quando um atacante contata uma pessoa contando uma história falsa para obter acesso a dados privilegiados, como no caso em que alguém finge necessitar de dados pessoais ou financeiros para confirmar a identidade do destinatário.
- **Troca por troca (*quid pro quo*) ou *something for something***: ocorre quando um atacante solicita informações pessoais a uma entidade em troca de algum benefício, como um presente.

Os engenheiros sociais utilizam várias táticas para executar seus ataques, como as descritas a seguir.

- **Autoridade**: as pessoas são mais propensas a cooperar quando instruídas por uma autoridade. Ao receber no anexo de um *e-mail* uma notificação de um órgão do governo, como a Receita Federal e a Justiça Eleitoral, uma pessoa pode fornecer informações confidenciais.
- **Intimidação**: os criminosos podem convencer a vítima a realizar determinada ação pelo uso de mecanismos de intimidação.
- **Consenso/prova social**: muitas pessoas podem realizar uma ação se acharem que isso irá gerar a aprovação de outras pessoas. Por exemplo, há criminosos que criam *sites* contendo falsos depoimentos para promover um produto ao qual querem associar o atributo de seguro.
- **Escassez e urgência**: diversas pessoas executam, por exemplo, uma ação de compra de um produto se acreditarem que existe uma quantidade limitada de itens disponíveis ou que tais

itens ficarão com preço atrativo apenas por um tempo limitado, parecendo ser uma ótima oportunidade de negócio.

- **Familiaridade/gosto:** os criminosos criam empatia com a vítima para estabelecer um relacionamento e aproveitam-se do vínculo formado para obter informações.
- **Confiança:** os criminosos criam uma relação de confiança com a vítima. Essa tática assemelha-se à anterior, mas demanda mais tempo para ser estabelecida.

Vale ressaltar que é responsabilidade dos profissionais de segurança ensinar os outros funcionários da empresa sobre as táticas utilizadas pelos engenheiros sociais.

8.1.7 Fraude de antecipação de recursos (*advance fee fraud*)

Na fraude de antecipação de recursos, ou *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. Trata-se da prática de uma ação enganosa, impulsionada pela má-fé, realizada com a intenção de lesar alguém.

Por meio da troca de mensagens eletrônicas ou do acesso a *sites* fraudulentos, a vítima é envolvida em alguma situação fictícia e, com isso, remete informações pessoais ou realiza pagamentos adiantados.

O chamado golpe da Nigéria, ou Nigerian 4-1-9 Scam, é um tipo de fraude bastante conhecido. No nome desse golpe, a referência 4-1-9 equivale ao número do artigo do Código Penal Nigeriano que trata de estelionato, como o artigo 171 no Código Penal Brasileiro.

8.1.8 Representação (*scam*) e farsas ou boatos (*hoax*)

A representação, ou *scam*, é o ato de fingir ser outra pessoa. Por exemplo, temos os chamados *scam* de telefone, que miram contribuintes brasileiros. Nesse golpe, um criminoso, disfarçado de funcionário da Receita Federal, diz para as vítimas que elas devem dinheiro ao fisco e que precisam fazer o pagamento da dívida imediatamente, por meio de transferência bancária. O impostor ameaça a vítima, afirmando que a falta de pagamento resulta em prisão.

De modo geral, no *scam*, os criminosos também usam a representação para exercer seus ataques. Eles podem prejudicar a credibilidade das pessoas utilizando publicações em *sites* ou em redes sociais.

Uma farsa, ou um boato (*hoax*), é um ato realizado com a finalidade de enganar ou ludibriar. Uma farsa virtual pode causar tanto um problema quanto uma violação real. Exemplos desse tipo de golpe são as correntes e pirâmides financeiras.

Frequentemente, observamos que usuários repassam mensagens falsas por *e-mail* e por redes sociais quando não verificam a veracidade do conteúdo dessas mensagens.

8.1.9 Phishing

O *phishing*, *phishing-scam* ou *phishing/scam* é o tipo de golpe por meio do qual um criminoso tenta obter dados pessoais e financeiros de um usuário pelo uso combinado de meios técnicos e táticas de engenharia social. Os criminosos virtuais utilizam *e-mails*, mensagens instantâneas ou outras possibilidades das mídias sociais para coletar informações, como credenciais de *logon* ou números da conta, ao se colocar uma fachada de entidade confiável.



Observação

A palavra *phishing* tem origem em uma analogia com a palavra da língua inglesa *fishing*. Nessa palavra, criada pelos golpistas, as iscas representam as mensagens eletrônicas utilizadas para pescar senhas e dados financeiros de usuários da internet.

O *phishing* ocorre quando uma parte mal-intencionada envia um *e-mail* fraudulento disfarçado de uma fonte legítima e confiável. A intenção da mensagem é enganar o destinatário para instalar um *malware* no dispositivo dele ou compartilhar suas informações pessoais ou financeiras.

Na figura a seguir, temos um exemplo de *phishing* feito em um *e-mail* enviado, em plena pandemia do coronavírus, no qual o remetente estava falsamente marcado como a Organização Mundial de Saúde (OMS).

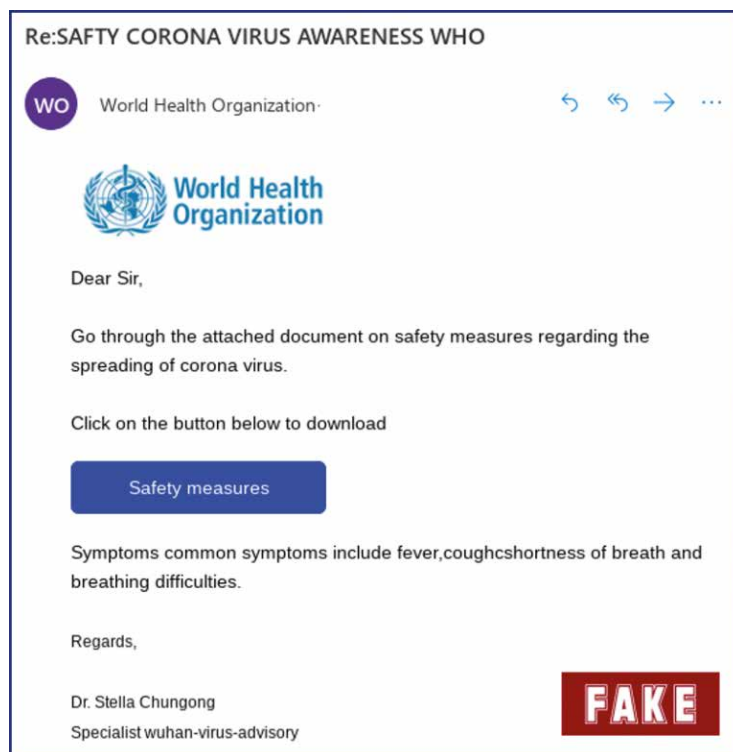


Figura 39 – Exemplo de *phishing* que se aproveita da pandemia

Outro exemplo de *phishing* é um *e-mail* falsificado que parece vir de uma loja de varejo, solicitando que o usuário clique em um *link* para receber um prêmio. O *link* pode levar o usuário para um *site* falso que pede informações pessoais ou pode instalar um vírus na máquina.

Campanhas de *phishing*, promoções fraudulentas e campanhas de desinformação estão entre as formas de ataque mais comuns. Um caso de *phishing* foi o ataque sofrido pelo Departamento de Saúde e Serviços Humanos dos EUA (HHS), do tipo DDoS, com uma campanha que tinha por objetivo espalhar o pânico durante a pandemia da covid-19.

Você, provavelmente, já deve ter recebido *e-mails* com assuntos contendo a chave de segurança da conta de um banco no qual você nunca abriu conta corrente. Esse tipo de *e-mail* contém um *link* que não direciona o usuário para o *site* do banco, mas para um *site* criado pelo fraudador (KIM; SOLOMON, 2014).



Observação

Firewalls e programas antimalware não detectam parte relevante das fraudes de *phishing*, já que não há código suspeito. Filtros de *spam* nem sempre retiram todas as mensagens de *phishing*, visto que, aparentemente, as mensagens são remetidas por fontes legítimas.

Uma variação do ataque de *phishing* é o *spear phishing*, que utiliza *e-mails* ou mensagens instantâneas para obter informações de acesso não autorizado a dados confidenciais em empresas (KIM; SOLOMON, 2014).

À primeira vista, essas mensagens parecem ser de fontes confiáveis, pois um ataque de *phishing* é altamente direcionado. Embora o *phishing* e o *spear phishing* utilizem *e-mails* para alcançar as vítimas, o *spear phishing* envia *e-mails* personalizados a uma pessoa específica. O criminoso pesquisa os interesses da vítima antes de encaminhar o *e-mail*.

Por exemplo, um criminoso descobre que a vítima está interessada em carros, procurando um modelo específico de automóvel para comprar. O criminoso entra no mesmo fórum de discussão de carros utilizado pela vítima, forja uma oferta de venda e envia um *e-mail* para o alvo. O *e-mail* contém um *link* para a visualização de fotos do automóvel. Ao clicar no *link*, a vítima instala inconscientemente o *malware* no computador.

A melhor maneira de nos proteger contra *phishings* de qualquer tipo é não oferecer informações pessoais quando solicitadas por *e-mails* ou por aplicativos de mensagens instantâneas como WhatsApp, Telegram e Messenger. Se você desconfiar de algo, acesse o endereço *web* da empresa digitando o nome dela no navegador, e não pelo clique no *link* da mensagem.



Saiba mais

O Grupo de Trabalho Anti-Phishing, ou, em inglês, Anti-Phishing Working Group (APWG), é uma associação de âmbito mundial e multissetorial que engloba empresas comerciais, governos, universidades e organizações não governamentais (ONGs) e visa eliminar fraudes e roubos de identidade decorrentes de falsificação de mensagens de *e-mail*.

Veja informações, relatórios e eventos sobre esse grupo de trabalho no *site* a seguir:

Disponível em: <https://apwg.org/>. Acesso em: 17 ago. 2020.

8.1.10 *Pharming, smishing, vishing e whaling*

Alguns subtipos de *phishing* são o *pharming*, o *smishing*, o *vishing* e o *whaling*.

O *pharming* é a representação de um *site* legítimo na tentativa de enganar os usuários para inserir as credenciais. Esse golpe leva os usuários para um *site* falso que parece ser o oficial por meio de alterações no serviço de nomes de domínio, ou Domain Name System (DNS). Assim, as vítimas inserem suas informações pessoais, pois consideram que estão conectadas a um *site* legítimo.

Tal redirecionamento pode acontecer:

- pela ação de códigos maliciosos projetados para mudar o comportamento do serviço DNS do computador;
- pela ação direta de um invasor que obtém acesso às configurações do serviço de DNS do computador ou do modem de banda larga.

O *smishing* (de *short message service phishing*) é o *phishing* que usa mensagens de texto em celulares. Os golpistas passam-se por uma fonte legítima na tentativa de obter a confiança da vítima. Por exemplo, um ataque de *smishing* pode enviar à vítima o *link* de um *site*. Quando a vítima visita esse *site*, o *malware* é instalado no seu telefone celular.

O *vishing* é o *phishing* que usa a tecnologia de comunicação de voz. Os criminosos podem falsificar as chamadas de origens legítimas usando a tecnologia de voz sobre IP, ou Voice over IP (VoIP). As vítimas também podem receber uma mensagem gravada aparentemente legítima. Os criminosos desejam obter números de cartão de crédito ou outras informações para roubar a identidade da vítima. Uma premissa importante do *vishing* é o fato de que as pessoas tendem a confiar na rede telefônica.

O *whaling* é um ataque de *phishing* que procura vítimas de elevada hierarquia em uma empresa, como executivos sêniores. Outras vítimas desse tipo de ataque são os políticos e as celebridades.



Saiba mais

Existem diversos *sites* especializados em divulgar listas de golpes aplicados na internet. Para saber mais sobre esse assunto, veja as sugestões a seguir.

Monitor de fraudes:

Disponível em: <http://www.fraudes.org/>. Acesso em: 25 abr. 2020.

E-farsas:

Disponível em: <https://www.e-farsas.com/>. Acesso em: 25 abr. 2020.

Snopes.com – Urban Legends Reference Pages:

Disponível em: <http://www.snopes.com/>. Acesso em: 25 abr. 2020.

TruthOrFiction.com:

Disponível em: <http://www.truthorfiction.com/>. Acesso em: 25 abr. 2020.

Urban Legends and Folklore:

Disponível em: <http://urbanlegends.about.com/>. Acesso em: 25 abr. 2020.

8.1.11 *Shoulder surfing*

A expressão *shoulder surfing* representa a forma como os criminosos roubam informações relevantes ao olhar por cima do ombro de outra pessoa, ou seja, o criminoso está bisbilhotando a vítima. Nesse tipo de ataque, um criminoso observa a vítima para obter PINs, senhas, códigos de acesso ou números de cartão de crédito.

Um invasor pode estar próximo de sua vítima ou pode usar binóculos ou câmeras de circuito fechado para descobrir o que quer. É com a intenção de impossibilitar essa ação que uma pessoa só pode ler uma tela de ATM em determinados ângulos. Esses tipos de proteção dificultam muito o *shoulder surfing*.

8.2 Programas maliciosos

8.2.1 Malwares

O termo *malware* é resultado da junção abreviada das palavras *malicious* e *software*.

No que se refere aos *malwares* infecciosos, vamos abordar vírus, *worms* ou vermes e "vírus" de *e-mail* e de macro.

No que se refere aos *malwares* não infecciosos, vamos abordar cavalos de Troia.

8.2.1.1 Vírus

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.

Podemos dizer que o primeiro registro formal de vírus em computadores ocorreu com o Creeper, em 1971, programado pelo pesquisador Bob Thomas. O Creeper realizava diversas cópias dele mesmo em vários computadores de uma rede e mostrava a seguinte mensagem: "*I'm the creeper, catch me if you can*". Em português, essa mensagem fica: "Eu sou o sorrateiro! Pegue-me se for capaz". Mais tarde, foi desenvolvido um programa chamado Reaper, que tinha o objetivo de encontrar o vírus Creeper e erradicar seus efeitos nos computadores infectados.

Já o Morris, criado em 1988 pelo, na época, universitário Robert Morris, foi um dos primeiros vírus disseminados *on-line*. O estudante desejava conhecer a dimensão da internet, mas produziu um *malware* que se reproduzia velozmente em redes: ele criava pastas temporárias para salvar cópias de si próprio e, com isso, fazia com que máquinas e servidores ficassem muito vagarosos. Há estimativas que sugerem que cerca de 10% dos PCs conectados à internet foram infectados pelo Morris no final da década de 1980.

No contexto em análise, podemos formular uma analogia: do mesmo modo que um vírus pode contagiar um ser humano, um vírus de computador anexa-se a algum tipo de código executável, como um programa. Quando o vírus é executado, ele tenta infectar uma grande quantidade de arquivos. O vírus é replicado nesses arquivos, realiza a tarefa maliciosa à qual se destina e repete isso até se espalhar o máximo possível.

Os antigos disquetes já foram os principais meios de propagação de vírus. Com o desuso dos disquetes, surgiram novas vias de proliferação de vírus, como o envio de *e-mails* e o uso de *pen drives*.

Há vários tipos de vírus, com distintas características e diferentes potenciais de causar danos:

- Existem vírus "sorrateiros", que permanecem ocultos aos usuários e, assim, infectam arquivos do disco rígido e executam processos sem qualquer consentimento.

- Existem vírus "dorminhocos", que permanecem inativos durante a maior parte do ano e apenas agem em datas específicas.

Frequentemente, vemos vírus que se propagam por *e-mail*. Nesse caso, o usuário recebe um *e-mail* com um arquivo anexado. A mensagem recebida induz o usuário a clicar sobre o arquivo para executá-lo. Com isso, muitos arquivos do computador desse usuário são infectados. Além disso, esse vírus encaminha cópias de *e-mails* para os contatos armazenados no computador.

Também temos os chamados vírus de *script*, implementados em linguagem VBScript ou em linguagem JavaScript. O usuário pode ser infectado ao acessar uma página *web* com o *script* malicioso, ao abrir um arquivo anexo a um *e-mail* ou ao verificar uma mensagem HTML. Uma categoria específica de vírus de *script* é o vírus de macro, implantado em linguagem VBScript, que visa infectar arquivos produzidos pelo Microsoft Office.

8.2.1.2 Worms ou vermes

O *worm* ou verme é um programa capaz de se multiplicar por uma rede, visto que envia cópias de si para os computadores interligados. Os *worms* são semelhantes aos vírus, mas não se propagam pela inclusão de cópias de si mesmo em outros arquivos, e sim 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.

Um exemplo de *worm* é o conhecido como "ILOVEYOU", ou "bug do amor", que se espalhou em milhões de máquinas que rodavam com o sistema operacional Windows. O *worm* propaga-se por *e-mail*: uma pessoa enviava uma mensagem por *e-mail* com o assunto "I Love You" e com um arquivo anexo de nome LOVE-LETTER-FOR-YOU.TXT.vbs (a última extensão, .vbs, era escondida por padrão pelo Windows). Na realidade, esse anexo era um *worm* disfarçado de arquivo de texto de uma carta de amor. O arquivo era um executável que, quando aberto, realizava muitos ataques: fazia diversas cópias de si para diversos arquivos e pastas, iniciava *softwares* prejudiciais, substituía arquivos e, por fim, ocultava-se dos seus malfeitos. Esse *worm* disseminou-se de modo intenso e gerou prejuízos da ordem de milhões de dólares, pois furtava os endereços de *e-mail* do computador das vítimas e remetia mensagens para todos da lista de endereços.

O *worm* "ILOVEYOU", desenvolvido em 2000 pelo estudante universitário filipino Onel de Guzman, foi escrito em Visual Basic como parte de um trabalho da faculdade que foi rejeitado. Guzman remeteu a mensagem com o *worm* na véspera da sua formatura e, assim, chegou a infectar mais de 50 milhões de computadores.

Como curiosidade, vale dizer que, devido à falta de legislação específica para crimes digitais na ocasião que o "ILOVEYOU" foi criado, Guzman foi absolvido.

8.2.1.3 "Vírus" de e-mail e de macro

Os "vírus" de e-mail e de macro, apesar de serem chamados de "vírus", são tipos de *malwares* mais parecidos com vermes digitais do que com vírus digitais, pois se reproduzem sem a necessidade de intervenção de um usuário.

Os "vírus" de e-mail entendem os protocolos de e-mail e exploram uma vulnerabilidade no programa leitor local *default* de e-mail presente num dado computador. Por exemplo: durante muito tempo, o programa Outlook (tanto na versão Express, que era incluída no SO Windows, quanto na versão que integra o pacote Office) vinha configurado por *default* para abrir o e-mail mais recente e exibir as imagens presentes nele, o que viabilizou "vírus" que executavam quando o e-mail era aberto automaticamente. Desse ponto em diante, esses "vírus" liam a lista de contatos do usuário e enviavam cópias de si para alguns ou para todos os membros de tal lista. Como o pacote Office roda em Macintosh, também máquinas sob MacOS foram vítimas de tais ataques.

Os "vírus" de macro aproveitavam-se de vulnerabilidades para executar e se reproduzir, visto que o MS-Word e o MS-Excel, bem como o já mencionado Outlook, costumavam interpretar macros (*scripts* destinados a automatizar operações) imediatamente ao encontrá-los. Como o pacote Office tornou-se praticamente um padrão para as finalidades a que se destina, sua presença em quase todas as máquinas encontráveis contribuiu para a popularização desse tipo de *malware*.

Outra variante está nos "vírus" em Java, que são disparados automaticamente por páginas da internet que os contêm e são acessíveis por meio de endereços parecidos com os de *sites* legítimos de grande tráfego (nos quais o usuário cai quando comete um engano comum na digitação do endereço do *site* legítimo). Tais tipos de *malware* são tão perigosos e problemáticos quanto os demais, mas não infectam programas executáveis durante seu funcionamento. Logo, chamá-los de vírus é algo impróprio, mas essa nomenclatura tem uso consolidado.

8.2.1.4 Cavalo de Troia (Trojan)

Antes de falarmos sobre o *malware* conhecido como Trojan, ou cavalo de Troia, vamos lembrar um pouco da *Ilíada*, de Homero, para entendermos o porquê da escolha desse nome.

Troia era uma cidade fortificada, capital de um grande e poderoso reino. Na epopeia intitulada *Ilíada*, Homero conta a história da guerra de Troia. Vamos a essa história.

Certa vez, Páris, filho do rei de Troia, raptou Helena, rainha da pólis grega chamada de Esparta. Os gregos, revoltados com o rapto, entraram em guerra contra Troia: juntaram seus exércitos e cercaram a cidade por anos, mas as altas muralhas impediam sua invasão.

Então, o grego Ulisses teve uma ideia: ele ordenou que fosse construído um imenso cavalo de madeira oco, para que, na sua barriga, pudessem ser escondidos soldados gregos (incluindo o próprio Ulisses).

A estratégia de Ulisses foi a seguinte: os gregos deixaram o cavalo na entrada de Troia e abandonaram o cerco à cidade. Por causa dessa falsa retirada, os troianos acreditaram, erroneamente, que os gregos haviam desistido da guerra. Pensaram que o cavalo era um presente (uma espécie de oferta de paz) e, por isso, colocaram-no para dentro da cidade. Quando os troianos estavam dormindo, Ulisses e os outros guerreiros saíram da barriga do cavalo de madeira, tomaram Troia, invadiram o palácio e resgataram Helena, que foi levada de volta à Esparta.

A figura a seguir mostra uma ilustração do cavalo de Troia.



Figura 40 – Ilustração do cavalo de Troia

No contexto que estamos estudando, há um *malware* que funciona como um cavalo de Troia: é o Trojan, um *malware* que usa sua aparência externa com a finalidade de enganar o usuário e fazer com que ele o execute (KIM; SOLOMON, 2014). Trata-se 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. É evidente que ninguém instalaria um *malware* em sua máquina de modo proposital; por isso, os chamados Trojans disfarçam-se de outros *softwares* a fim de ludibriar o usuário.

Em 1974, foi lançado o primeiro cavalo de Troia, denominado Animal, que usava um jogo de charadas para agir: o computador tentava adivinhar o animal pensado pelo usuário por meio de perguntas. Esse programa se copiava em todos os diretórios nos quais o usuário podia fazer gravações.

Entre as atividades que um Trojan pode realizar, temos:

- Fazer cópias de si mesmo.
- Abrir portas de comunicação do computador.

- Baixar arquivos inutilmente.
- Ocultar informações confidenciais.



Saiba mais

Para saber mais sobre o *malware* Trojan, leia:

TECHINTER. *O que é trojan (cavalo de Troia): o pior vírus de computador.* 19 set. 2020. Disponível em: <https://bit.ly/3vMzsFC>. Acesso em: 7 maio 2021.

8.2.2 Principais tipos de *payload*

No que se refere aos principais tipos de *payload*, vamos abordar:

- *Adwares*.
- Destruidores de dados.
- *Ransomwares*.
- *Backdoors*.
- *Rootkits*.

8.2.2.1 *Adwares*

Os *adwares* são programas destinados a fazer propaganda de algum tipo de produto, especialmente (mas não só) *sites* pagos na internet e *softwares*. Em geral, eles são introduzidos nas máquinas dos usuários por meio de instaladores de programas grátis ou quando o usuário clica em certos anúncios.

Muitos *adwares* causam a abertura de janelas de navegador em intervalos aleatórios ou a abertura de janelas de navegador por baixo da janela em uso, de forma que só apareçam quando a janela que está por cima for fechada ou minimizada. Alguns também transmitem a lista de páginas acessadas pelo usuário para *sites* externos sem permissão.

Existindo no limiar da legalidade, tais programas podem parecer mais irritantes do que perigosos, mas essa percepção é incorreta, pois eles constituem quebra de segurança.

8.2.2.2 Destruidores de dados

Os destruidores de dados são programas destinados a:

- Modificar dados, como substituir o conteúdo das páginas de um *website* institucional por outro conteúdo não relacionado.
- Formatar o disco rígido (de modo rápido, mas, provavelmente, reversível).
- Sobrescrever o conteúdo do disco rígido com zeros ou com números pseudorrandômicos (de modo lento, mas irreversível).

8.2.2.3 Ransomwares

O termo *ransomwares* significa, em tradução literal, "sequestradores de dados".

Trata-se de programas que encriptam o conteúdo do disco rígido da máquina (ou, mais comumente, apenas parte deles, a saber, arquivos de texto em múltiplos formatos, inclusive .doc, .docx e .pdf, imagens em múltiplos formatos, especialmente .jpg, .jpeg, .gif e .bmp, planilhas de dados e arquivos de *e-mail*) e fazem com que, ao final do *boot*, a máquina apenas apresente a mensagem pedindo resgate, indique como pagá-lo e quais informações devem ser fornecidas junto ao pagamento para que se receba a chave de deciptação (que nem sempre é enviada se o pagamento for realizado e, quando é enviada, nem sempre funciona).

8.2.2.4 Backdoors

O termo *backdoors* significa, em tradução literal, "porta dos fundos".

Trata-se de programas que criam meios de acesso secretos a um sistema computacional que não passam pelo sistema normal de acesso seguro, o que permite que os atacantes ganhem acesso sem serem notados. Esses programas também podem personificar algum usuário lícito do sistema.

Normalmente, quando o *payload* de um ataque cria uma *backdoor*, ela fica latente até que seja usada para:

- A introdução e a distribuição inicial de um verme.
- A introdução e o disparo de um *software* destinado a causar DDoS ou algum outro tipo de *software* malicioso.
- A possibilidade de propiciar acesso que vise ao roubo ou à destruição de dados.

8.2.2.5 Rootkits

O termo *rootkits* significa, em tradução literal, algo como "conjunto de componentes para alcançar privilégio de administrador".

Quando o *payload* de um ataque é a instalação de um *rootkit*, trata-se de um ataque sofisticado.

O *rootkit* é composto por módulos projetados para serem:

- incorporados em *firmwares* (por exemplo, placas de rede ou placas gráficas) ou no BIOS (ou UEFI) da máquina;
- executados durante o *boot* do SO ou do hipervisor, ficando, depois, ocultos e latentes durante o funcionamento normal, ou injetando processos diretamente na memória, sem que o binário correspondente seja encontrável no sistema de arquivos usado pelo SO (ou porque ele reside em áreas fora do sistema de arquivos ou porque o *rootkit* os oculta ativamente).

Como os *rootkits* são constituídos por vários módulos, quando um deles é encontrado e deletado, ele é recarregado pouco depois por outro módulo, já que os módulos são criados com a função de preservar a integridade do conjunto, o que torna os *rootkits* muito difíceis de serem removidos.

Rootkits são ideais para capturar tudo que o usuário digita, possivelmente selecionar, por heurística, informações interessantes para o atacante (como dados e senha de cartões de crédito) e depois enviá-las automaticamente para um endereço de rede predeterminado. Assim, tais informações são mantidas em armazenamento até que um atacante remoto as colete.

Os *rootkits* também se destinam a destruir lentamente os dados existentes em um disco rígido, possivelmente dos menos recentemente usados para os mais recentemente usados, de forma a dificultar a detecção do ataque.



Resumo

Na unidade II, apresentamos as principais características da linguagem HTML e mostramos algumas de suas *tags*.

Abordamos o processo para criação de um *site*, que envolve desde a reunião inicial com um cliente e o preenchimento do *briefing* até a aprovação final do projeto. Também analisamos aspectos relativos à publicação de páginas *web* e *sites*.

Estudamos, de modo particular, a ferramenta WordPress, uma das plataformas para gestão e publicação de conteúdo (CMS) mais utilizadas no mundo.

Vimos que os ambientes via internet tendem a apresentar o quesito segurança como fator crítico, pois vazamentos de informações podem, por exemplo, comprometer a imagem de uma empresa e causar impactos na sua reputação.

Observamos que os custos da segurança de informação no ambiente *web* são bastante elevados, pois, além das perdas financeiras devidas a ataques a sistemas e redes, temos de considerar os gastos decorrentes de períodos de paralisação imprevistos e de pagamentos de multas.

Apresentamos os princípios da confidencialidade, da integridade e da disponibilidade e concluimos a respeito da importância deles para a eliminação de vulnerabilidades.

Mostramos as ferramentas mais utilizadas na identificação de vulnerabilidades de computadores, programas, sistemas e redes.

Finalmente, abordamos os diversos tipos de golpes praticados em ambientes *web*, como falsificação de *e-mail*, ataque de força bruta, desfiguração de página (*defacement*), *plugins*, envenenamento de SEO, engenharia social, fraude de antecipação de recursos (*advance fee fraud*), representação (*scam*), farsas ou boatos (*hoax*), *phishing*, *pharming*, *smishing*, *vishing*, *whaling* e *shoulder surfing*.



Exercícios

Questão 1. Leia o texto a seguir.

Brasil perde US\$ 10 bilhões por ano com cibercrime, diz McAfee

Estudo da empresa estima prejuízos mundiais em US\$ 608 bilhões e coloca país entre os maiores centros de atividades virtuais ilícitas

Por Felipe Machado – Publicado em 21 fev. 2018

As perdas das empresas brasileiras com crimes virtuais são de 10 bilhões de dólares por ano. A estimativa consta de relatório da empresa de segurança digital McAfee, divulgado nesta quarta-feira. O estudo também aponta também que o país é a segunda maior fonte de ataques virtuais no mundo – o que torna o uma "potência" do cibercrime, ao lado de Rússia, Coreia do Norte, Índia e Vietnã.

Se fosse o total produzido pela economia de um país, o cibercrime corresponderia ao 22º maior PIB do mundo, segundo *ranking* do Fundo Monetário Internacional (FMI). Os pesquisadores indicam que, cada vez mais, há integração entre redes de criminosos, com prestação de serviços como aluguel de máquinas para ataques e venda de programas para roubar informações

"É uma segunda economia, se equipara ao tráfico de drogas. Hoje, existem cerca 45.000 ferramentas disponíveis na '*darkweb*' [área oculta na internet, normalmente usada para atividades ilícitas] para fazer ataques virtuais. Se existe a oferta, existe a demanda", disse à VEJA Jeferson Propheta, diretor-geral da McAfee no Brasil. O crescimento das moedas virtuais, como *bitcoin*, é apontado como facilitador das atividades ilegais por permitir pagamentos anônimos.

Tanto aqui quanto lá fora, os alvos preferenciais são as instituições financeiras, afetadas por problemas como *sites* falsos, cartões clonados e *malwares* (abreviação para *software* malicioso) direcionados. Os crimes virtuais são responsáveis por 95% das perdas financeiras dessas companhias, segundo a McAfee. A leitura é de que o Brasil é um alvo preferencial desse tipo de ataque por causa do volume de transações *on-line*. Em 2016, 57% das operações ocorreram nos meios *mobile* e *internet banking*, segundo dado da Federação Brasileira dos Bancos (Febraban).

Disponível em: <https://bit.ly/3beOpKw>. Acesso em: 16 set. 2020.

Com base na leitura e nos seus conhecimentos, avalie as afirmativas.

I – As perdas das empresas brasileiras com crimes virtuais (cibercrimes), que chegam à ordem de 10 bilhões de dólares por ano, fazem com que o Brasil consolide sua posição de potência econômica mundial.

II – Um dos motivos de as perdas com crimes virtuais serem vultosas é a prevalência de comunidades mal organizadas de *hackers* do tipo *black hat*.

III – As instituições financeiras do mundo todo são especialmente lesadas em termos de perda de valores pelos crimes virtuais.

É correto o que se expõe em:

A) I, apenas.

B) II, apenas.

C) III, apenas.

D) II e III, apenas.

E) I, II e III.

Resposta correta: alternativa C.

Análise das afirmativas

I – Afirmativa incorreta.

Justificativa: segundo o texto, as perdas das empresas brasileiras com crimes virtuais (cibercrimes) chegam a 10 bilhões de dólares por ano. No entanto, isso não faz do Brasil uma potência econômica mundial. O termo “potência” no contexto da reportagem (“potência” do cibercrime) indica que o Brasil é um dos países em que mais ocorrem cibercrimes.

II – Afirmativa incorreta.

Justificativa: há comunidades bem organizadas de *hackers* do tipo *black hat* que chegam a vender cursos e tutoriais sobre a criação de *spams* e a implementação de *malware on-line*. Isso acentua a ocorrência e o sucesso dos cibercrimes.

III – Afirmativa correta.

Justificativa: no mundo, segundo o texto, as instituições financeiras são os alvos preferenciais dos cibercrimes, causadores de 95% das perdas financeiras dessas empresas.

Questão 2. Os chamados códigos maliciosos, ou *malwares*, são programas computacionais desenvolvidos com a intenção de realizar ações danosas e atividades maliciosas em um computador ou em uma rede de computadores. Esse tipo de *software* pode ser utilizado, por exemplo, para a obtenção de informações confidenciais ou para a modificação de arquivos.

Nesse sentido, um *malware* pode infectar um computador:

- I – pelo acesso a páginas *web* maliciosas, com o uso de navegadores vulneráveis;
- II – pela execução automática de mídias removíveis contaminadas, como *pen drives*;
- III – pela ação direta dos invasores, que inserem códigos maliciosos em arquivos.

É correto o que se expõe em:

- A) I, apenas.
- B) II, apenas.
- C) III, apenas.
- D) II e III, apenas.
- E) I, II e III.

Resposta correta: alternativa E.

Análise da questão

Um código malicioso, ou *malware*, pode infectar um computador quando, por exemplo:

- acessamos páginas *web* utilizando navegadores desatualizados e/ou vulneráveis;
- realizamos a execução automática de mídias removíveis contaminadas.

Além disso, o invasor pode manipular um arquivo (nesse caso, ele primeiramente invade a máquina e, depois, infecta um arquivo), ou um arquivo previamente infectado pode ser executado na máquina (provavelmente pelo próprio usuário, mas sem o seu conhecimento), comprometendo-a e possibilitando a sua invasão. No último caso, a infecção do arquivo possibilita a invasão, enquanto, no primeiro caso, a invasão gera oportunidade para a infecção do arquivo.

FIGURAS E ILUSTRAÇÕES

Figura 1

HISTORY COMPUTER. *Larry Roberts – Biography, History and Inventions*. [s.d.]. Disponível em: <https://bit.ly/3beuee2>. Acesso em: 10 maio 2021.

Figura 2

RIGUES, R. Mãe da internet faz 50 anos. Conheça a história da ARPANET. *Olhar Digital*, out. 2019. Disponível em: <https://bit.ly/2RGPq5w>. Acesso em: 23 dez. 2020.

Figura 3

NATIONAL INVENTORS HALL OF FAME. *Robert E. Kahn*. 2021. Disponível em: <https://bit.ly/33x7DoU>. Acesso em: 23 dez. 2020.

Figura 4

INTERNATIONAL SCIENCE COUNCIL. *Vinton G. Cerf*. [s.d.]. Disponível em: <https://bit.ly/2Q4leQe>. Acesso em: 23 dez. 2020.

Figura 5

3VU8ZGN. Disponível em: <https://bit.ly/3vU8ZGn>. Acesso em: 23 dez. 2020.

Figura 6

ALVES, W. P. *Desenvolvimento e design de sites*. São Paulo: Érica, 2014. p. 19.

Figura 7

33ARKV0. Disponível em: <https://bit.ly/33aRKV0>. Acesso em: 10 maio 2021.

Figura 8

3FDKVRU. Disponível em: <https://bit.ly/3fdKvRU>. Acesso em: 29 abr. 2021.

Figura 9

TERRA. *Mosaic*: há 20 anos, era lançado o 1º navegador gráfico da web. 22 abr. 2013. Disponível em: <https://bit.ly/3xW13GB>. Acesso em: 29 dez. 2020.

Figura 10

OLIVEIRA, M. Primórdios da rede: a história dos primeiros momentos da internet no Brasil. *Revista Pesquisa Fapesp*, edição 180, fev. 2011. Disponível em: <https://bit.ly/3xCeVFs>. Acesso em: 23 dez. 2020.

Figura 11

OLIVEIRA, M. Primórdios da rede: a história dos primeiros momentos da internet no Brasil. *Revista Pesquisa Fapesp*, edição 180, fev. 2011. Disponível em: <https://bit.ly/3xCeVFs>. Acesso em: 23 dez. 2020.

Figura 12

OLIVEIRA, M. Primórdios da rede: a história dos primeiros momentos da internet no Brasil. *Revista Pesquisa Fapesp*, edição 180, fev. 2011. Disponível em: <https://bit.ly/3xCeVFs>. Acesso em: 23 dez. 2020.

Figura 13

OLIVEIRA, M. Primórdios da rede: a história dos primeiros momentos da internet no Brasil. *Revista Pesquisa Fapesp*, edição 180, fev. 2011. Disponível em: <https://bit.ly/3xCeVFs>. Acesso em: 23 dez. 2020.

Figura 14

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet: uma abordagem top-down*. 6. ed. São Paulo: Pearson Education do Brasil, 2013. p. 3.

Figura 15

BREITMAN, K. K. *Web semântica: a internet do futuro*. Rio de Janeiro: LTC, 2005. p. 6.

Figura 17

UNCTAD. *Global e-Commerce hits \$25.6 trillion – latest UNCTAD estimates*. 27 abr. 2020. Disponível em: <https://bit.ly/3elkZUy>. Acesso em: 30 abr. 2021. Adaptada.

Figura 18

TI INSIDE ONLINE. *69% das grandes empresas aceleraram iniciativas digitais na pandemia*. 30 set. 2020. Disponível em: <https://bit.ly/3nCjPOh>. Acesso em: 30 abr. 2021.

Figura 19

ABCOMM. *Comércio eletrônico deve crescer 18% em 2020 e movimentar R\$ 106 bilhões*. 14 fev. 2020. Disponível em: <https://bit.ly/334NK8w>. Acesso em: 6 jan. 2021.

Figura 20

334CJ76. Disponível em: <https://bit.ly/334CJ76>. Acesso em: 10 maio 2021.

Figura 25

ALVES, W. P. *Desenvolvimento e design de sites*. São Paulo: Érica, 2014. p. 28. Adaptada.

Figura 30

KALBACH, J. *Design de navegação web: otimizando a experiência do usuário*. Porto Alegre: Bookman, 2009. p. 109.

Figura 31

KALBACH, J. *Design de navegação web: otimizando a experiência do usuário*. Porto Alegre: Bookman, 2009. p. 111.

Figura 32

KALBACH, J. *Design de navegação web: otimizando a experiência do usuário*. Porto Alegre: Bookman, 2009. p. 116.

Figura 33

WORDPRESS. *Minha página inicial*. Disponível em: <https://bit.ly/2RcaTTU>. Acesso em: 11 jan. 2021.

Figura 34

WORDPRESS. *Estatísticas*. Disponível em: <https://bit.ly/3o602XC>. Acesso em: 11 jan. 2021.

Figura 35

WORDPRESS. *Posts*. Disponível em: <https://bit.ly/3hgRX1g>. Acesso em: 11 jan. 2021.

Figura 36

KALBACH, J. *Design de navegação web: otimizando a experiência do usuário*. Porto Alegre: Bookman, 2009. p. 172.

Figura 39

SOUZA, R. COVID-19: como os criminosos estão tirando proveito da pandemia. *The Hack*, 2020. Disponível em: <https://bit.ly/3f4UdWE>. Acesso em 16 ago. 2020.

Figura 40

3ETJROC. Disponível em: <https://bit.ly/3eTjR0c>. Acesso em: 10 maio 2021.

REFERÊNCIAS

Textuais

17 MARCAS representam 85% do e-commerce brasileiro. *Mercado & Consumo*, 22 maio 2020. Disponível em: <https://bit.ly/2RfkERa>. Acesso em: 6 jan. 2021.

ABCOMM. *Comércio eletrônico deve crescer 18% em 2020 e movimentar R\$ 106 bilhões*. 14 fev. 2020. Disponível em: <https://bit.ly/334NK8w>. Acesso em: 6 jan. 2021.

ABREU, K. C. K. *História e usos da internet*. Biblioteca on-line da ciência da comunicação. 2009. Disponível em: <https://bit.ly/33Aacq0>. Acesso em: 19 nov. 2020.

ALVES, W. P. *Desenvolvimento e design de sites*. São Paulo: Érica, 2014.

ANDERSON, C. *A cauda longa: do mercado de massa para o mercado de nicho*. São Paulo: Campus, 2006.

APDSI. Glossário da Sociedade da Informação. *Web 1.0*. [s.d.]a. Disponível em: <https://bit.ly/3nMxCC1>. Acesso em: 4 maio 2021.

APDSI. Glossário da Sociedade da Informação. *Web 2.0*. [s.d.]b. Disponível em: <https://bit.ly/3uoccx1>. Acesso em: 4 maio 2021.

APDSI. Glossário da Sociedade da Informação. *Web 3.0*. [s.d.]c. Disponível em: <https://bit.ly/3xJboFA>. Acesso em: 4 maio 2021.

ARAYA, E. R. M.; VIDOTTI, S. A. B. G. *Criação, proteção e tecnologia da informação em ambientes da World Wide Web*. São Paulo: Unesp; São Paulo: Cultura Acadêmica, 2010.

BASTA, A.; BASTA, N.; BROWN, M. *Segurança de computadores e teste de invasão*. 2. ed. São Paulo: Cengage Learning, 2014.

BELL, I. *HTML, DHTML & Web Design*. São Paulo: Market Books, 2000.

BERNERS-LEE, T.; HENDLER, J.; LASSILA, O. The semantic web. *Scientific American*, v. 284, n. 5, p. 28-37, 2001. Disponível em: <https://bit.ly/3f2SLDV>. Acesso em: 7 maio 2021.

BORGES JUNIOR, M. P. *Desenvolvendo webservices*. Rio de Janeiro: Ciência Moderna, 2005.

BRASIL. Presidência da República. Casa Civil. *Lei n. 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, 2014. Disponível em: <https://bit.ly/3eOGtge>. Acesso em: 29 abr. 2021.

BREITMAN, K. K. *Web semântica: a internet do futuro*. Rio de Janeiro: LTC, 2005.

CARVALHO, L. G. *Segurança de redes*. Rio de Janeiro: Ciência Moderna, 2005.

CARVALHO, M. S. R. M. *A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança*. Rio de Janeiro: UFRJ, 2006.

CASTELLS, M. *Galáxia da internet: reflexões sobre a internet, os negócios e a sociedade*. Rio de Janeiro: Zahar, 2003.

CERT.BR. *Cartilha de segurança para internet, versão 4.0*. São Paulo: Comitê Gestor da internet no Brasil, 2012. Disponível em: <https://bit.ly/2RA5TZc>. Acesso em: 6 dez. 2020.

CHAPCHAP, G. Tendências do setor de e-commerce em 2020. *E-Commerce Brasil*, 6 dez. 2019. Disponível em: <https://bit.ly/3e6RZXl>. Acesso em: 6 jan. 2021.

CHARK, A. *Como criar sites persuasivos*. São Paulo: Pearson, 2003.

CISCO. *Introduction to Cybersecurity*. 2020. Disponível em: <https://bit.ly/33t6Tky>. Acesso em: 10 jun. 2020.

CLEBER TOLEDO. *Vendas online crescem 100% no Brasil com a pandemia*. 15 out. 2020. Adaptado de: <https://bit.ly/330C0DQ>. Acesso em: 17 out. 2020.

DOMO. *Data Never Sleeps 8.0*. [s.d.]. Disponível em: <https://bit.ly/3gR2TIP>. Acesso em: 20 nov. 2020.

E-BIT. *Webshoppers*. 42. ed. 2020. Disponível em: <https://bit.ly/3y100oD>. Acesso em: 25 nov. 2020.

GARRETT, F. Sputnik 62 anos: saiba tudo sobre o primeiro satélite artificial no espaço. *TechTudo*, out. 2019. Disponível em: <https://glo.bo/3vRpBPd>. Acesso em: 3 maio 2021.

GRUBER, T. R. A translation approach to portable ontology specifications. *Knowledge Acquisition*, v. 5, p. 199-220, 1993.

KALBACH, J. *Design de navegação web: otimizando a experiência do usuário*. Porto Alegre: Bookman, 2009.

KIM, D.; SOLOMON, M. G. *Fundamentos de segurança da informação*. Rio de Janeiro: LTC, 2014.

KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet: uma abordagem top-down*. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

LAUDON, K. C.; LAUDON, J. P. *Management information systems: managing the digital firm*. 16. ed. Nova York: Pearson, 2020.

MACEDO, M. S. *Construindo sites adotando padrões web*. Rio de Janeiro: Ciência Moderna, 2004.

MACHADO, A. Há 40 anos, surgia a Arpanet, o embrião da internet. *NIC.br*, set. 2009. Disponível em: <https://bit.ly/3tffW35>. Acesso em: 3 maio 2021.

MARTINS, R. Fidonet. *Knoow*, 2015. Disponível em: <https://bit.ly/3t5kadm>. Acesso em: 29 dez. 2020.

NEVES, M. C. B. A. *Sites de alta performance*. Curitiba: Contentus, 2020.

NIST. *An introduction to computer security: the NIST handbook*. 1995. Disponível em: <https://bit.ly/3uvahr3>. Acesso em: 26 abr. 2020.

OLIVEIRA, A. J. Sputnik entrava em órbita há 57 anos – relembre a missão. *Revista Galileu*, out. 2014. Disponível em: <https://glo.bo/338OPfq>. Acesso em: 3 maio 2021.

OLIVEIRA, M. Primórdios da rede: a história dos primeiros momentos da internet no Brasil. *Revista Pesquisa Fapesp*, edição 180, fev. 2011. Disponível em: <https://bit.ly/3xCeVFs>. Acesso em: 23 dez. 2020.

O QUE é hospedagem de *site*? Guia para iniciantes. *Hostinger*, maio 2021. Disponível em: <https://bit.ly/3xXcxJP>. Acesso em: 7 maio 2021.

O QUE são ataques de DDoS? *Kaspersky*, 2021. Disponível em: <https://bit.ly/2R1KjwQ>. Acesso em: 9 set. 2020.

RODRIGUES, C. Há 30 anos, nascia o BBS, sistema que foi o antecessor da internet. *Folha de S.Paulo*, 13 fev. 2008. Disponível em: <https://bit.ly/3vsArKZ>. Acesso em: 28 dez. 2020.

SEGUNDO, J. E. S.; CONEGLIAN, C. S.; LUCAS, E. R. O. Conceitos e tecnologias da *Web* semântica no contexto da colaboração acadêmico-científica: um estudo da plataforma Vivo. *TransInformação*, Campinas, v. 29, n. 3, p. 297-309, set./dez. 2017. Disponível em: <https://bit.ly/3tbOMdb>. Acesso em: 30 abr. 2021.

SILBERSCHATZ, A.; GALVIN, P. B.; GAGNE, G. *Fundamentos de sistemas operacionais*. 9. ed. Rio de Janeiro: LTC, 2015.

SILVA, L. G. *Tutorial: elaboração e publicação de páginas e sites web*. Curitiba: UFPR, 2016. Disponível em: <https://bit.ly/3bcFTKf>. Acesso em: 3 dez. 2020.

STALLINGS, W. *Criptografia e segurança de redes*. 4. ed. São Paulo: Pearson, 2008.

STALLMAN, R. Por que o código aberto não compartilha dos objetivos do *software* livre. *GNU*, 2020. Disponível em: <https://bit.ly/3gXqbXi>. Acesso em: 4 maio 2021.

STEIN, M. *Design de interface para sites*: desenvolvimento de uma metodologia orientadora considerando a comunicação entre clientes e usuário. Florianópolis: UFSC, 2003.

TANENBAUM, A. S.; WETHERALL, D. *Redes de computadores*. 5. ed. São Paulo: Pearson, 2011.

TANENBAUM, A. S. *Sistemas operacionais modernos*. São Paulo: Pearson, 2009.

TCDF. *HTML*: comandos. 2017. Disponível em: <https://bit.ly/3vNQmE8>. Acesso em: 11 jan. 2021.

TECHINTER. *O que é trojan (cavalo de Troia)*: o pior vírus de computador. 19 set. 2020. Disponível em: <https://bit.ly/3vMzsFC>. Acesso em: 7 maio 2021.

TECMUNDO. *A história da internet*. 24 abr. 2018. Disponível em: <https://bit.ly/3xU0soT>. Acesso em: 4 maio 2021.

TERUEL, C. E. *HTML 5: guia prático*. 2. ed. São Paulo: Saraiva, 2014.

TI INSIDE ONLINE. *69% das grandes empresas aceleraram iniciativas digitais na pandemia*. 30 set. 2020. Disponível em: <https://bit.ly/3nCjPOh>. Acesso em: 30 abr. 2021.

UNCTAD. *Global e-Commerce hits \$25.6 trillion – latest UNCTAD estimates*. 27 abr. 2020. Disponível em: <https://bit.ly/3elkZUy>. Acesso em: 30 abr. 2021.

VALLE, R.; BALDAM, R.; CAVALCANTI, M. *GED - Gerenciamento Eletrônico de Documentos*. São Paulo: Érica, 2004.

W3TECHS. *Market share trends for content management systems*. [s.d.]. Disponível em: <https://bit.ly/3hcQN6L>. Acesso em: 6 dez. 2020.

WEINSTEIN, P. C. *Ontology-based metadata: transforming the MARC Legacy*. In: ACM DIGITAL LIBRARY CONFERENCE, 3., 1998. *Proceedings* [...]. Pittsburgh, PA, USA, jun. 1998.

Sites

<https://apwg.org/>

<https://www.e-farsas.com/>

<http://www.fraudes.org/>

<https://www.incc.br/>

<https://notepad-plus-plus.org/>

<https://www.nsf.gov/>

<https://www.rnp.br/>

<https://html.spec.whatwg.org>

<http://www.snopes.com/>

<http://www.truthorfiction.com/>

<http://urbanlegends.about.com/>

<https://www.w3c.br/>

This image shows a single sheet of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



Lined writing area with horizontal lines.



Handwriting practice lines consisting of 30 horizontal lines. Each line set includes a solid top line, a dashed midline, and a solid bottom line, providing a guide for letter height and placement.



A series of horizontal lines for writing, consisting of 30 evenly spaced lines across the page.



Interativa

Informações:
www.sepi.unip.br ou 0800 010 9000