



**Mermãs
Digitais**



**INSTITUTO FEDERAL
MARANHÃO**
Campus Imperatriz

Introdução à Computação

Mermãs Digitais Desenvolvendo Web



SUMÁRIO

UNIDADE

01

Introdução à Computação

Capítulo 1: Contexto histórico

- Evolução dos computadores
- Introdução à computação e suas aplicações

Capítulo 2: Hardware e Software

- O que é hardware e software?
- Qual a diferença entre eles?
- Entendendo hardware
- Entendendo software
- Como hardware e software se relacionam?

Capítulo 3: Dispositivos de E/S

- O que são?
- Qual a diferença entre eles?
- Exemplos.

Capítulo 4: Sistemas operacionais

- O que são sistemas operacionais?
- Windows
- Linux
- macOS
- Tipos de sistemas operacionais

SUMÁRIO

UNIDADE

02

Redes de Computadores

Capítulo 1: Introdução a Redes de Computadores

- O que são Redes de Computadores?
- Por que conectar o mundo?
- Diferença entre internet, Ethernet e Web

Capítulo 2: Tipos de Redes de Computadores

- Redes locais (LANs)
- Redes de longa distância (WANs)
- Redes sem fio (Wi-Fi)
- Dispositivos de Rede

Capítulo 3: Protocolo HTTP

- Como os protocolos realmente funcionam?
- O que é HTTP e quais seus métodos?
- Estruturas de solicitação e de resposta
- URI e URL: Qual a diferença?

Capítulo 4: Arquitetura cliente-servidor

- O que é a arquitetura cliente-servidor?
- Conceito de cliente e de servidor
- Comunicação cliente-servidor
- Componentes da arquitetura cliente-servidor
- Aplicações

SUMÁRIO

UNIDADE

03

Segurança da Informação

Capítulo 1: Introdução a Segurança da Informação

- O que é Segurança da Informação?
- A importância da segurança online
- Questões éticas e computação

Capítulo 2: Ameaças e vulnerabilidades

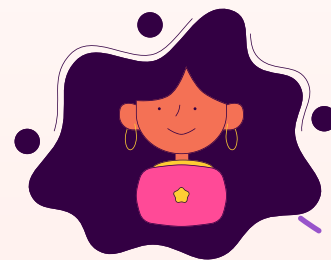
- Tipos de ameaças
- Proteção contra malwares

Capítulo 3: Como me proteger online?

- Backup de arquivos
- Cuidados com senha
- Atualizações de software
- Phishing em e-mails suspeitos
- Criptografia e autenticação em dois fatores (2FA)
- Uso responsável das redes sociais
- Compartilhamento de informações



Apresentação



Olá, mermã! **Seja bem-vinda à apostila "Introdução à Computação"**, você está prestes a embarcar em uma incrível aventura pelo mundo da computação e, acredite em mim, será uma incrível viagem tecnológica!

Esta apostila foi escrita pela equipe Mermãs Digitais para que você disponha de **um material de apoio que vá te acompanhar durante a disciplina** e, assim, possa solidificar da melhor forma possível os conhecimentos adquiridos, se tornando uma verdadeira discípula da Ada Lovelace. Então prepare-se para **mergulhar de cabeça no universo dos bits, bytes e algoritmos de uma forma super descontraída e simplificada**.

Será um prazer te acompanhar nessa jornada. O Mermãs Digitais é um projeto que tem como uma de suas missões **tornar a computação acessível e amigável para todos**. Fizemos questão de escrever esta apostila com uma linguagem acessível e descomplicada, para que qualquer pessoa, independentemente do seu nível de conhecimento, possa **se sentir à vontade explorando esse fascinante campo**.

Aqui, você vai aprender **desde o básico**, como entender o funcionamento de um computador, **até conceitos mais avançados**, como redes de computadores e cibersegurança. E o melhor de tudo é que você não precisa ser um gênio da matemática ou um geek hardcore para entender: **o Mermãs Digitais descomplica tudo para você!**

Então, mermã, prepare-se para uma jornada empolgante, repleta de descobertas e aprendizado. Pegue seu café, acomode-se em um lugar confortável e mergulhe de cabeça na "Introdução à Computação" do Mermãs Digitais. **Você está prestes a dar um salto quântico no seu entendimento do mundo digital**. Vai ser incrível!



Bora lá!

UNIDADE 01

introdução à computação





Capítulo 1



Olá, mermã exploradora do mundo da computação! Vamos começar nossa jornada pela Introdução à Computação, explorando **a história por trás do universo tecnológico.**



Contexto Histórico

A palavra computador surge do latim **computatore** que significa **algo capaz de realizar cálculos**. Assim, nossa história começa muito antes dos computadores que conhecemos atualmente — na verdade, os primeiros dispositivos de cálculo foram inventados há séculos: o primeiro passo foi a invenção do ábaco, uma espécie de calculadora que surgiu há mais de 2.000 anos!

No século XIX, com a Revolução Industrial, vieram diversos avanços tecnológicos. Nesse contexto, **Charles Babbage**, um inventor britânico, projetou uma máquina de cálculo mecânica chamada **Máquina Analítica**, assim, seus projetos foram grandes inspirações que vieram a servir de base para os computadores modernos.

A partir do século XX, houveram avanços incríveis na computação. Durante a **Segunda Guerra Mundial**, os cientistas desenvolveram máquinas como o **Colossus** e o **ENIAC**, os primeiros computadores eletrônicos programáveis que ocupavam salas gigantescas. Eles foram usados para fins militares, como decifrar códigos inimigos.

Nesse contexto de guerra, surgiram os primeiros computadores, que usavam **válvulas** e **cartões perfurados** para realizar cálculos. Eram enormes, consumiam muita energia e grandes investimentos. Na década de **1950**, os **transistores** substituíram as válvulas, tornando os computadores menores e mais confiáveis. Por isso, foram criadas linguagens de programação. Em **1960**, chegaram os **circuitos integrados**, que permitiram a criação de computadores menores, mais poderosos e mais acessíveis.

Na década de **1970**, os **microprocessadores** foram desenvolvidos, levando à criação dos computadores pessoais. Isso revolucionou a computação, tornando-a **acessível** a todos. Nesse período, empresas como Apple e IBM lançaram os primeiros computadores a serem usados em casa, o que abriu as portas para a era digital em que vivemos hoje.

Atualmente, **estamos na quinta geração de computadores**, com avanços incríveis em inteligência artificial, aprendizado de máquina e computação em nuvem, que estão moldando nosso mundo de maneiras surpreendentes!

Gerações de Computadores

As gerações de computadores são uma maneira de categorizar e classificar o **desenvolvimento da tecnologia** de computadores ao longo do tempo. As gerações de computadores são divididas em **cinco principais**:

Geração	Período
1ª geração	1946 - 1954
2ª geração	1955 - 1964
3ª geração	1964 - 1977
4ª geração	1977 - 1991
5ª geração	1991 - agora

Primeira Geração (1940-1956): A primeira geração de computadores era caracterizada pelo uso de válvulas, parecidas com lâmpadas, para processamento de dados. O exemplo mais notável dessa época é o ENIAC (Electronic Numerical Integrator and Computer), que era enorme, consumia muita energia e tinha uma capacidade de processamento limitada. Programar essas máquinas era uma tarefa extremamente trabalhosa, usando linguagem de máquina.

Segunda Geração (1956–1963): Essa geração foi marcada pela transição das válvulas eletrônicas para transistores. Isso permitiu a criação de computadores menores, mais rápidos e mais eficientes em termos de consumo de energia. Nessa época, foi desenvolvida a linguagem Assembly, tornando a programação um pouco mais acessível.

Terceira Geração (1964–1971): Nesta geração, os circuitos integrados (chips) foram adotados, o que trouxe diminuição significativa no tamanho dos computadores e aumento de poder computacional. Os super computadores e minicomputadores ganharam espaço nesse período.

Quarta Geração (1971–1980): Agora com microprocessadores, chips únicos que continham a unidade central de processamento (CPU), houve o nascimento dos computadores pessoais (PCs), como o IBM PC. Além disso, surgiram linguagens de programação de alto nível, como C e Pascal.

Quinta Geração (1980–presente): Geração que atualmente vivemos, é marcada pela evolução contínua da tecnologia. Isso permitiu o desenvolvimento de computadores cada vez menores, como os smartphones. Além disso, os computadores pessoais e a Internet revolucionaram a maneira como as pessoas usam a tecnologia da informação.



Aplicações da Computação

Agora que entendemos a história e a evolução dos computadores, é hora de explorar ainda mais a **computação**. A área da Ciência da Computação permeia quase todos os aspectos da nossa vida moderna. Hoje, a computação não é apenas uma ferramenta, é a essência da inovação. Ela molda o nosso mundo de maneiras surpreendentes, desde a forma como nos comunicamos através de redes sociais até como revolucionamos indústrias inteiras com análise de dados avançada.

A computação torna nossas casas mais inteligentes, nossos carros mais eficientes e até mesmo nos ajuda a entender melhor nosso próprio corpo com a bioinformática. A Computação representa a fascinante capacidade humana de criar, resolver problemas e explorar o desconhecido, tudo isso graças à tecnologia. A computação está em todos os lugares e você, mermã, tem a **oportunidade de explorar e moldar esse mundo sensacional!**



Capítulo 2



Mermã, neste capítulo vamos entender sobre os conceitos de **hardware e software**, além de conhecer os componentes que formam um computador básico. Você também vai conhecer como os softwares estão relacionados à computação.



Hardware e software: o que são?

Hardware refere-se a **tudo que pode ser tocado** num dispositivo de computação. Isso inclui todas as peças, desde o gabinete do computador até os circuitos eletrônicos internos, como placas, cabos e dispositivos de entrada/saída, como teclados, monitores e mouses.

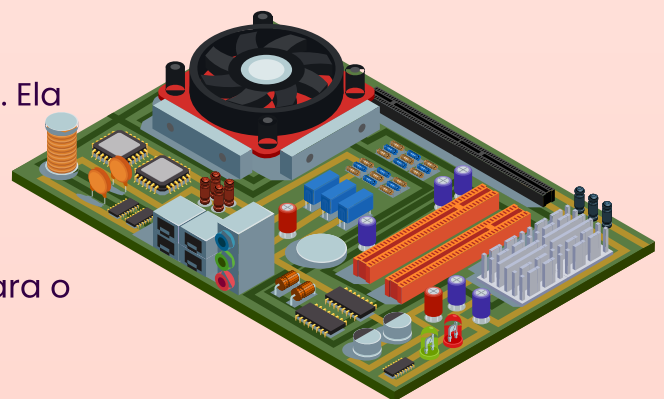
Software, por outro lado, é o **conjunto de programas** que dão vida ao hardware. São os aplicativos, sistemas operacionais e código que permitem que o hardware execute tarefas específicas e realize as operações que você deseja.

A principal diferença entre hardware e software é que o hardware pode ser tocado, é físico, enquanto o software não pode, é lógico. Pensemos no hardware como o corpo de um dispositivo e no software como a mente que dá comandos para que o corpo execute ações.

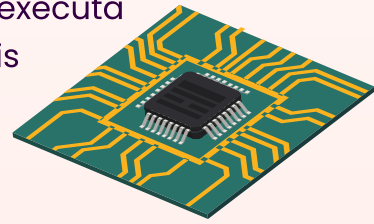


Entendendo o hardware

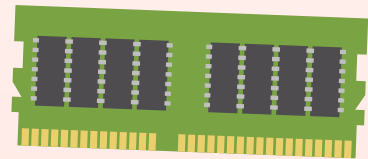
Placa mãe: É como a "cabeça" do computador. Ela é uma placa de circuito que conecta todos os componentes principais do sistema, como a CPU, a memória RAM, as placas de vídeo e os dispositivos de armazenamento. É essencial para o funcionamento do computador.



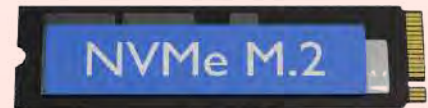
Processador: A CPU, ou Central Processing Unit (Unidade Central de Processamento), é o cérebro real do computador. Ela executa todas as operações de cálculo e controle. Quanto mais rápida e poderosa a CPU, mais rapidamente o computador pode executar tarefas.



Memória: A memória de um computador, como a RAM Random Access Memory (Memória de Acesso Randômico), é onde os dados são temporariamente armazenados enquanto o computador está ligado. Quanto mais RAM, mais eficientemente o computador pode executar múltiplas tarefas e armazenar dados temporários.



Dispositivo de armazenamento: O disco rígido (Hard Disk, ou Solid State Drive – SSD, unidade de estado sólido) é o espaço de armazenamento permanente do computador, onde os dados são gravados e armazenados. É como a memória de longo prazo do dispositivo, onde você guarda seus arquivos, programas e o sistema operacional.



Entendendo o software

Sistemas operacionais: Os sistemas operacionais, como o Windows, macOS e Linux, são programas que gerenciam todos os recursos de hardware do computador e fornecem uma interface para que os usuários interajam com o dispositivo. Eles são essenciais para a execução de aplicativos e a realização de tarefas. Veremos mais sobre eles no capítulo 4 desta unidade.

Aplicativos e utilitários: Os aplicativos são programas de software que realizam tarefas específicas, como navegadores da web, editores de texto, jogos e muito mais. Os utilitários são programas que auxiliam na manutenção e na otimização do sistema, como antivírus e ferramentas de limpeza de disco, aplicativos de música ou imagem.



Capítulo 3



Quanto conhecimento até o momento, né, mermã? Agora vamos entender os **dispositivos de entrada e saída**, chamados de dispositivos E/S. Eles são como 'pontes mágicas' que **conectam o usuário ao computador**. Esses dispositivos são fundamentais para que as informações fluam no sistema, por isso, dominar esse conteúdo nos ajudará a transformar ideias nessa jornada. Vamos lá?!



Dispositivos de Entrada e Saída

Imagine os **dispositivos de entrada e saída** como os 'olhos', 'ouvidos' e 'boca' dos computadores: eles são como os **sentidos especiais** que permitem que os **computadores se comuniquem com o mundo exterior**. Os dispositivos de entrada são como 'ouvidos atentos' que captam informações do usuário, como comandos, dados ou interações. Em contrapartida, os dispositivos de saída agem como 'bocas falantes', apresentando os resultados das operações realizadas pelos computadores para o usuário.

Existem **duas categorias** principais de dispositivos de entrada e saída:

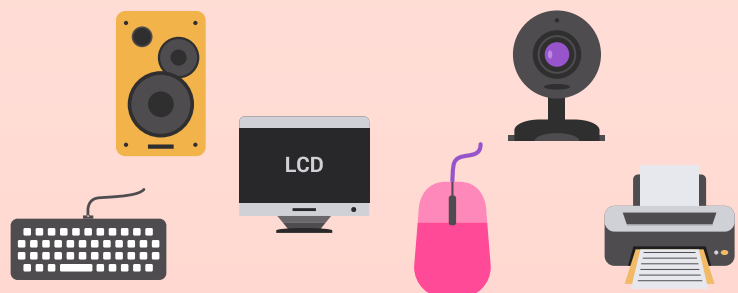
- Dispositivos de Comunicação com o Usuário
- Dispositivos de Comunicação Interna do Computador



Dispositivos de Comunicação com o Usuário

Essa categoria engloba dispositivos como:

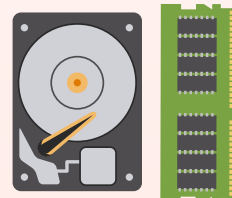
- Teclados
- Monitores
- Mouses
- Impressoras
- Caixas de Som
- Microfones
- Câmeras
- Touchpads e Sensores de Movimento



Dispositivos de Comunicação Interna do Computador

Essa categoria se concentra na **comunicação entre o processador e os componentes internos do computador**. Alguns dispositivos importantes nessa categoria incluem:

- **Controladores de Disco:** Gerenciam a comunicação entre a CPU e dispositivos de armazenamento, como discos rígidos e unidades flash;
- **Controladores de Memória:** Gerenciam o acesso à memória do sistema, incluindo a RAM.



Exemplos de Dispositivos E/S

Aqui estão alguns exemplos de dispositivos de entrada e saída:

Dispositivos de Entrada:

- **Teclados:** Usados para inserir texto e comandos;
- **Mouses:** Oferecem controle direcional e seleção;
- **Microfones:** Captam áudio e entrada de voz;
- **Câmeras:** Capturam imagens e vídeos;
- **Touchpads e Sensores de Movimento:** Permitem interações gestuais.

Dispositivos de Saída:

- **Monitores:** Exibem informações e saídas visuais;
- **Impressoras:** Geram saídas impressas em papel;
- **Fones de Ouvido:** Reprodução de áudio;
- **Caixas de Som:** Reproduzem áudio para o usuário;
- **Projetor:** Exibição de imagens em tela grande.

Essa é a **base sobre os dispositivos E/S**. Eles são verdadeiros facilitadores de um mundo de possibilidades, desde a produção de documentos e obras de arte digital até a exploração de vastos conjuntos de dados, capacitando-nos a executar tarefas com eficiência, proporcionando **um mosaico fascinante de realizações tecnológicas**. A interação harmoniosa entre o humano e o digital é, indiscutivelmente, um dos pilares mais notáveis da era moderna, **tornando a computação altamente funcional**.



Capítulo 4



Neste último capítulo da unidade, vamos navegar no **fascinante mundo dos sistemas operacionais**, onde a magia da computação ganha vida! Assim, exploraremos como os sistemas operacionais controlam os aspectos dos seus dispositivos eletrônicos. **Vamos juntos embarcar nas ideias e maravilhas dos sistemas operacionais!**



Sistemas Operacionais

Um sistema operacional (SO) é o **software central** que gerencia um computador, **atuando como um intermediário entre os componentes físicos**, como processador e memória, **e os programas** que os usuários desejam executar. Podemos imaginar um SO como um maestro de uma grande orquestra, gerenciando toda a música que acontece. O maestro (SO) desempenha um papel vital: garantir que os músicos (programas) e os instrumentos (componentes físicos do computador) estejam sincronizados perfeitamente.

Um sistema operacional **executa uma série de funções técnicas essenciais para o funcionamento do computador**, incluindo controle de acesso aos recursos de hardware, gerenciamento de memória para a execução simultânea de vários programas e fornecimento de uma interface para a interação do usuário. O SO também lida com o **gerenciamento de processos**, assegurando que os programas sejam executados e interrompidos corretamente, além de controlar a comunicação com dispositivos periféricos, como impressoras e discos rígidos. Outras funções incluem organização e acesso a dados armazenados, segurança contra ameaças como vírus e facilitação da comunicação em redes de computadores.

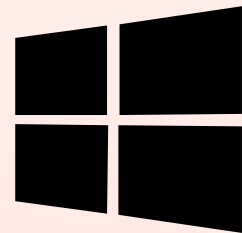
Normalmente, as empresas de computadores **não criam** seus próprios sistemas operacionais devido à **complexidade** envolvida. Em vez disso, **contam com especialistas** como a Microsoft, Apple e a comunidade de código aberto



para fornecer sistemas confiáveis, como Windows, macOS e Linux, essenciais para a eficácia dos computadores. Cada um desses sistemas tem características técnicas únicas, mas todos **desempenham um papel crucial na operação eficiente dos computadores.**

Windows

Vamos agora conhecer mais do **sistema operacional mais popular do mundo**: o Windows! Desenvolvido pela **Microsoft Corporation**, é um sistema operacional que desempenhou um papel fundamental na história da computação pessoal e empresarial.



O Windows teve seu **início em 1985** com o lançamento do **Windows 1.0**. No entanto, foi o **Windows 95** que trouxe uma interface gráfica revolucionária, o menu Iniciar e a multitarefa, tornando-o um marco na computação pessoal. Desde então, várias versões notáveis, como o Windows XP, Windows 7, Windows 10 e o Windows 11, **influenciaram a computação moderna**. As principais versões do Windows são:

Windows 95 (1995)

- Foi um enorme sucesso
- Marcou a transição do MS-DOS para uma interface gráfica mais avançada
- Introduziu o menu iniciar, a barra de tarefas e o sistema de plug and play
- Foi o primeiro SO Windows a obter um amplo reconhecimento e uso.

Windows XP (2001)

- Um dos sistemas operacionais mais queridos da Microsoft
- Introduziu uma interface mais estável e moderna
- Ofereceu recursos de segurança mais aprimorados
- Continuou sendo usado por muitos usuários, mesmo após o lançamento de versões posteriores.

Windows 7 (2009)

- Foi elogiado por sua usabilidade e estabilidade
- Apresentou melhorias na interface do usuário, como a barra de tarefas aprimorada e o Aero Glass
- Tornou-se um dos SOs mais populares da Microsoft.

Windows 10 (2015)

- Unificou os elementos do Windows 7 e do Windows 8
- Windows Update passa a contar com atualizações cumulativas
- Trouxe recursos como a assistente virtual Cortana e a loja Microsoft.

Uma das características marcantes dos sistemas Windows é sua **interface gráfica intuitiva**. Ao longo de sua evolução, o Windows aprimorou constantemente sua interface para **tornar a experiência do usuário mais amigável e eficiente**.

Ao longo de todas as versões, o Windows incorporou recursos de facilitação, como **atalhos de teclado, pesquisa rápida e assistentes virtuais**, como a Cortana. A personalização sempre foi uma parte fundamental da interface do Windows, permitindo que os usuários ajustem a aparência e o layout **de acordo com suas preferências**.

Outro ponto importante de se destacar do Windows é a **segurança do sistema**, prioridade fundamental para a Microsoft ao projetar e manter seus sistemas operacionais. Alguns dos principais aspectos relacionados à segurança no Windows são:

Windows Defender: O Windows Defender é um antivírus e antispyware integrado ao Windows 10 e versões posteriores. Ele oferece proteção em tempo real contra ameaças de malware, como vírus, trojans e spyware. A Microsoft regularmente atualiza a base de dados de definições de vírus para garantir a detecção de ameaças mais recentes.

Firewall do Windows: O Firewall do Windows controla o tráfego de rede para e do seu computador. Ele ajuda a bloquear conexões não autorizadas e protege seu sistema contra ataques de rede. Os usuários podem personalizar as configurações do Firewall do Windows para atender às suas necessidades específicas.

Atualizações de Segurança: A Microsoft fornece atualizações regulares de segurança para o Windows. Essas atualizações corrigem vulnerabilidades conhecidas e melhoram a segurança do sistema.

BitLocker: O BitLocker é uma ferramenta de criptografia de disco integrada ao Windows. Ele permite que os usuários criptografem unidades de disco rígido, protegendo os dados em caso de perda ou roubo do dispositivo. O BitLocker é especialmente valioso para laptops e dispositivos móveis.

Mermã, sabia disso?



O Windows 11 trouxe importantes aprimoramentos em sua segurança, sendo um deles a utilização obrigatória de chips TPM 2.0, componentes de hardware que aumentam a segurança de dispositivos e sistemas. Ou seja, o Windows 11 está mais protegido desde o momento em que você liga o computador até o momento em que faz login. Além disso, o Windows 11 também traz melhorias na defesa contra ameaças de segurança cibernética, pois seu sistema foi projetado para ser mais resistente contra vírus, malware e outras ameaças da internet.

Cada um dos sistemas operacionais da Microsoft desempenhou um **papel crucial na história da computação pessoal e empresarial**, refletindo as **mudanças tecnológicas** e as **demandas dos usuários** ao longo dos anos. Cada nova versão trouxe inovações e aprimoramentos, moldando o cenário da tecnologia e **influenciando como interagimos com nossos dispositivos digitais**.

 Linux

Tá afim de explorar o mundo do Linux? Esse sistema operacional é um **fenômeno entre os apaixonados por tecnologia**. Esse SO se tornou um dos sistemas operacionais mais versáteis e poderosos do mundo. Nossa jornada agora vai passar pelo universo do Linux, desde suas origens humildes até as múltiplas distribuições modernas, destacando sua filosofia, funcionamento interno e como ele influenciou o cenário da computação.



A história desse sistema operacional inicia em **1991**, quando **Linus Torvalds**, um jovem estudante de ciência da computação da Universidade de Helsinki, na Finlândia, começou a trabalhar em um novo projeto de sistema operacional. Insatisfeito com as opções disponíveis na época, Linus decidiu criar algo que fosse **gratuito, flexível** e, acima de tudo, **colaborativo**. O Linux nasceu como um projeto pessoal, mas rapidamente atraiu a atenção de programadores de todo o mundo.

Nesse cenário, nasceu a **filosofia de software livre** do Linux. Sabe o que isso quer dizer? O software simplesmente tem fundamentos bem firmados, as quatro liberdades fundamentais, que são:

Liberdade de Usar: Você pode usar o software como quiser, onde quiser.

Liberdade de Estudar: Você pode olhar o código-fonte do software e entender como ele funciona.

Liberdade de Compartilhar: Você pode distribuir cópias do software para outros, de graça ou por dinheiro.

Liberdade de Modificar: Você pode alterar o software e compartilhar suas mudanças com os outros.

Embora muitas pessoas relacionem o Linux a desktops e laptops, ele tem uma presença significativa em outros domínios. O Linux é **amplamente utilizado** em servidores, supercomputadores, sistemas embarcados, dispositivos IoT (Internet das Coisas) e **até mesmo em smartphones** (por exemplo, o **Android** é baseado no kernel do Linux).

O Linux possui uma forma inteligente de cuidar dos programas que você instala: os **gerenciadores de pacotes**. Diferentes sistemas do Linux podem usar diferentes gerenciadores, mas todos têm o mesmo objetivo: **facilitar a instalação, atualização e remoção de programas, tornando tudo mais simples**.

Um dos motivos que fazem o Linux ser queridinho na computação é que ele não é apenas um sistema: **é uma família inteira de sistemas operacionais superpoderosos!** — e o melhor de tudo é que são todos gratuitos. Vamos então conhecer a vastidão das distribuições Linux, cada uma tem sua personalidade única, e você vai descobrir qual é a que mais combina com você.

Uma **distribuição** Linux, muitas vezes chamada de **distro**, é uma versão do sistema operacional Linux que inclui o **kernel do Linux**, ferramentas de sistema, bibliotecas e aplicativos. **O que diferencia** as distribuições **é como esses componentes são organizados e configurados** para criar um ambiente de computação coeso. As distribuições são personalizáveis e podem variar significativamente em termos de aparência, funcionalidade e público-alvo.

Cada uma das distribuições atende a diferentes necessidades e preferências. Algumas das distribuições mais populares incluem:



Ubuntu: Focada na facilidade de uso e na experiência do usuário, o Ubuntu é uma das distribuições mais populares para iniciantes. Ele oferece uma grande quantidade de softwares pré-instalados e é conhecido por suas versões de longo suporte (LTS).

Fedora: Essa distribuição é conhecida por ter uma abordagem inovadora e foco em software livre. É frequentemente usada por desenvolvedores e entusiastas que desejam acesso às últimas tecnologias.



Debian: Com estabilidade e compromisso com o software 100% livre, o Debian é uma base para muitas outras distribuições, além disso, é uma distro amplamente usada em servidores.

CentOS: Baseado no código-fonte do RHEL (Red Hat Enterprise Linux), o CentOS é conhecido por sua estabilidade e é usado frequentemente em servidores empresariais.



Arch Linux: Destinada a usuários avançados em busca de total domínio sobre seu sistema, essa distribuição permite que você adapte seu sistema de acordo com suas necessidades.

openSUSE: Famosa por sua ferramenta de gerenciamento de pacotes YaST, essa distro é bastante robusta, com versões para desktops e servidores.



Linux Mint: Com uma interface semelhante à do Windows, o Linux Mint é uma escolha popular para novos usuários que estão migrando do Windows, pois possui uma amigável usabilidade facilitada.

O Linux é elogiado por sua **segurança robusta**, com regras estritas que protegem arquivos e pastas contra acessos não autorizados. Além disso, suas atualizações garantem que os problemas de segurança sejam devidamente corrigidos e o seu **firewall** também não deixa a desejar: ele controla o tráfego na internet com muita eficiência! Grandes empresas confiam na estabilidade e segurança do Linux, amplamente utilizado em **servidores, firewalls, roteadores e dispositivos críticos**.

Em suma, é extremamente notório que o Linux é um sistema operacional que coloca o **controle nas mãos dos usuários**, promove a colaboração global e oferece uma ampla gama de aplicações em vários domínios. Sua filosofia de código aberto o torna uma **escolha popular para aqueles que valorizam a liberdade, a personalização e a segurança**.



O próximo sistema dessa aventura é o macOS, com seu **primeiro lançamento** sendo no ano de **1984**. No entanto, sua transformação mais significativa foi em **2001**, com o lançamento do **macOS X**, marcando a transição para uma base Unix, que trouxe estabilidade, segurança e desempenho notável ao sistema. O macOS moderno, com nomes inspirados em locais icônicos da Califórnia, continua a evoluir.



macOS

Uma das características mais **distintivas e elogiadas** deste SO é sua **interface intuitiva**. Ela dispõe de:

- **Barra de Menu Superior:** No topo da tela, há uma barra de menu que exibe informações do sistema, como a hora, a rede Wi-Fi, o nível de bateria (em laptops), e oferece acesso rápido a configurações e opções do sistema e de programas abertos.
- **Dock:** A barra de ícones na parte inferior da tela é totalmente personalizável e fornece acesso rápido aos aplicativos e pastas mais usados.
- **Gestos Multi-Touch:** Os gestos multi-touch no trackpad (ou mouse com suporte a gestos) permitem que movimentos como deslizar, pinçar, tocar e deslizar com vários dedos façam interações com a interface e os aplicativos de forma intuitiva.
- **Mission Control:** Função que oferece uma visão geral de todas as janelas e áreas de trabalho em uso.

Em resumo, a interface do macOS é conhecida por sua **elegância, simplicidade e eficiência**. Ela combina design atraente com funcionalidade intuitiva para proporcionar uma **experiência de usuário agradável e produtiva**.

As primeiras versões do macOS, **anteriormente conhecido como Mac OS X**, marcaram um **ponto de virada** na história dos sistemas operacionais da Apple. Vamos dar uma olhada nas **principais versões iniciais** e como elas moldaram o ecossistema Apple:

Mac OS X 10.0 (2001)

- Codinome: Cheetah
- Primeira versão do Mac OS X
- Marcou uma transição significativa da linha de SOs anteriores da Apple
- Apresentou uma nova interface chamada Aqua
- Incluiu o navegador "Internet Explorer" como navegador padrão.

Mac OS X 10.4 (2005)

- Codinome: Tiger
- Introduziu o sistema de busca Spotlight
- Apresentou o Dashboard
- Melhorou a integração com dispositivos móveis da Apple, como iPods.

Mac OS X 10.7 (2011)

- Codinome: Lion
- Marcou a transição do "Mac OS X" para simplesmente "OS X"
- Introduziu gestos multi-touch
- Apresentou o recurso "Mission Control"

Mac OS X 10.11 (2015)

- Codinome: El Capitan
- Continuou aprimorando a estabilidade e o desempenho do sistema operacional
- Introduziu recursos, como Split View
- Melhorou a experiência de gerenciamento de janelas e a navegação no Finder.

macOS 10.14 (2018)

- Codinome: Mojave
- Trouxe o modo escuro, com a interface com tons mais escuros
- Introduziu pilhas na área de trabalho
- Reforçou a privacidade do usuário, com as permissões do sistema.

macOS 11.0 (2020)

- Codinome: Big Sur
- Redesenhou a interface, incorporando elementos do iOS
- Aprimorou o desempenho e a segurança, com atualizações regulares
- Introduziu widgets aprimorados e uma Central de Controle.

Essas primeiras versões do macOS estabeleceram os **fundamentos para a experiência Mac** que conhecemos hoje. Elas trouxeram uma interface elegante e funcional, uma base UNIX robusta e uma série de recursos inovadores que continuam a ser aprimorados nas versões subsequentes do sistema operacional da Apple.

O macOS **evoluiu consideravelmente** desde esses tempos iniciais, mas essas versões pioneiras representam um marco na transição da Apple para a era moderna dos sistemas operacionais.

Quanto à **segurança e privacidade**, o macOS dispõe de softwares como:

- **Gatekeeper:** verifica a autenticidade dos aplicativos para evitar softwares maliciosos.
- **FileVault:** criptografa os dados no disco rígido, protegendo contra roubo de dados.
- **T2 Security Chip:** em alguns modelos de Mac, garante armazenamento seguro e inicialização segura, protegendo informações sensíveis.

Assim, o macOS, combinando beleza, usabilidade e desempenho, oferece **uma experiência de computação excepcional**. Seja para tarefas cotidianas ou projetos avançados, o macOS continua sendo **uma escolha de excelência entre os entusiastas** da tecnologia em todo o mundo.

Tipos de sistemas operacionais

Existem vários tipos de sistemas operacionais, **cada um projetado para atender a necessidades específicas**. Alguns dos principais tipos de sistemas operacionais:



SOs de Desktop: Projetados para uso em computadores pessoais e laptops.



SOs de Dispositivos Móveis: Desenvolvidos para smartphones e tablets.



SOs de Servidor: Usados em servidores para hospedagem de sites, aplicativos e serviços.



SOs Embarcados: Adaptados para sistemas integrados em dispositivos, como roteadores e eletrodomésticos inteligentes.



SOs de Supercomputadores: Empregados em computadores de alto desempenho para tarefas complexas.



SOs de Rede: Encontrados em dispositivos de rede, como roteadores e switches.



SOs de Mainframes: Utilizados em sistemas mainframe para processamento de alta capacidade.



SOs de Jogos: Desenvolvidos para consoles de jogos.



SOs de Veículos Autônomos: Usados em veículos autônomos para controle e navegação.

Esses são os principais tipos de sistemas operacionais, **cada um projetado para atender a necessidades específicas** em diversas áreas e plataformas. Assim, visualizando essas peças fundamentais da tecnologia, pudemos ver como, desde suas primeiras versões até as mais avançadas, os SOs desempenharam um **papel crucial na gestão de recursos de hardware, na interação com o usuário e na segurança dos sistemas**. Descobrimos que os componentes-chave, como o kernel, memória e sistema de arquivos, mantêm nossos dispositivos funcionando de forma eficaz. Além disso, aprendemos sobre a importância dos sistemas de gerenciamento de pacotes e como eles simplificam a instalação de software. Percebemos, então, como os sistemas operacionais são a **base invisível que possibilita nossa jornada digital** e nossa conexão com o incrível mundo da tecnologia.

UNIDAD 02

redes de computadores



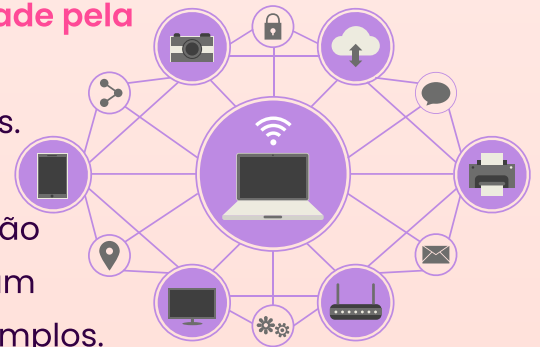


Capítulo 1



O que hoje conhecemos como uma rede de computadores teve sua origem como um projeto de defesa durante a **Segunda Guerra Mundial**, inicialmente chamado de **ARPANet**. A ideia por trás da ARPANet era assegurar que **informações sigilosas não fossem centralizadas em um único local**, evitando que, em caso de ataque, os dados fossem perdidos permanentemente. O conceito fundamental era que os pontos interligados dessa rede funcionam como células conectadas, de modo que se uma região fosse alvo de um ataque, as informações seriam preservadas na região seguinte.

Uma rede de computadores contemporânea pode ser caracterizada pela presença de **duas entidades**: uma máquina denominada **cliente** e outra chamada **servidor**, que estão interligadas por um meio de comunicação. No entanto, o campo das redes não se restringe exclusivamente aos computadores. Embora comumente **associamos redes à conectividade pela internet**, há diversas outras formas de configurações que podem ser consideradas redes de computadores. Isso inclui conexões como o emparelhamento bluetooth entre um mouse e um computador, a ligação física por cabo entre dispositivos, como um drone e um controle remoto via radiofrequência, entre outros exemplos.



Redes de computadores são **sistemas interconectados** de dispositivos de computação e comunicação que **permitem a troca de dados e informações** entre esses dispositivos. Essas redes podem ser pequenas, como uma rede doméstica que conecta vários computadores e dispositivos em uma residência, ou podem ser enormes, como a Internet, que interliga bilhões de dispositivos em todo o mundo.

Em resumo, as redes de computadores **são fundamentais** para a comunicação e a conectividade em nossa sociedade digital. Elas desempenham um papel crítico na interligação de dispositivos e na facilitação da troca de informações e serviços em **todo o mundo**.



Por que conectar o mundo?

Conectar o mundo através de redes de comunicação, como a Internet, traz vários **benefícios e impactos positivos** em várias áreas da vida humana e na sociedade como um todo. Aqui estão algumas razões pelas quais conectar o mundo é importante:

Acesso à informação

A conexão global oferece acesso a uma ampla gama de informações, educação e recursos online, promovendo a democratização do conhecimento e abrindo portas para oportunidades de aprendizado e desenvolvimento em todo o mundo.

Comunicação global

Poder se comunicar instantaneamente com pessoas em todo o planeta é crucial, seja para negócios, relações pessoais, educação, ou situações de emergência... As redes que nos ligam globalmente tornam essa comunicação muito mais ágil!

Desenvolvimento econômico

A internet aumentou as possibilidades do mundo corporativo, isso ajuda muito no desenvolvimento econômico. Assim, temos gerações de empregos e mesmo pequenas empresas conseguem vender para o mundo inteiro.

É relevante mencionar, ainda, que a conexão global traz **mobilidade e flexibilidade**, visto que ela possibilita que as pessoas trabalhem, estudem e **façam coisas de qualquer lugar do mundo**. Isso torna nosso jeito de viver mais flexível e móvel, **abrindo caminho** para novas maneiras de trabalhar e aprender.

Por outro lado, junto com os benefícios, a conexão global também traz desafios, como problemas de privacidade e segurança online, por exemplo. Por isso, na Unidade 03 vamos nos aprofundar nos conceitos de segurança online.

Internet, Ethernet e Web

Mermã, tu certamente já ouviu falar no termo **internet**, né? É um dos termos de Redes de Computadores mais utilizados no dia a dia, mas é **frequentemente confundido** com outros conceitos correlatos, tais como Ethernet e Web. Cada um desses termos representam elementos fundamentais de nossa **infraestrutura digital**, no entanto, eles abordam aspectos distintos da tecnologia de comunicação.

Internet: Sendo o alicerce da comunicação digital global, ela estabelece uma vasta teia de computadores interligados em todo o mundo. Sua principal missão é permitir a troca de informações e dados entre dispositivos situados em diferentes locais geográficos. Essa interconexão é viabilizada através de diversas tecnologias de conectividade (como Ethernet, Wi-Fi, redes móveis e outras semelhantes). A Internet atua como a base para uma ampla gama de serviços online, incluindo a Web (World Wide Web), desempenhando um papel essencial na comunicação contemporânea e na disseminação de informações.

Ethernet: Ao operar conectando dispositivos dentro de uma mesma rede local (como computadores em residências, empresas, ou instituições educacionais), essa tecnologia, que opera com conexões por cabo, estabelece um meio para a transferência de dados entre dispositivos que compartilham a mesma rede local. A Ethernet também desempenha um papel importante em infraestruturas de maior porte ao conectar várias redes e, finalmente, permitir a conexão com a Internet. Além disso, ela dispõe de um conjunto de diretrizes e protocolos que regulam a transmissão de dados, incluindo os métodos para que os dispositivos acessem a rede compartilhada e como os dados são preparados para a transmissão.

Web: A World Wide Web (Web) é um dos serviços mais famosos da Internet. Ela consiste em uma vasta coleção de páginas da web que estão todas ligadas umas às outras e cada uma delas tem seu próprio endereço, chamado URL. Para acessá-la, utiliza-se navegadores como o Google Chrome e Safari, que permitem que os usuários vejam, naveguem e interajam com coisas na internet, como os textos, fotos, vídeos e programas. Assim, a Web é uma parte da Internet cuja importância se dá na forma com que acessamos informações e serviços online.



Capítulo 2



E aí, mermã! Já se sente submersa nesse universo de Redes de Computadores? Espero que sim, pois vamos precisar desse conhecimentos para o próximo tema: **tipos de Redes**. Nesse momento da nossa jornada, vamos conhecer algumas **variações de redes** que são usadas para as conexões e comunicação, além dos **meios e dispositivos** que possibilitam isso. Vamos lá?!

LANs e WANs: o que são?

Você já ouviu falar de alguma dessas siglas? Essas redes que conheceremos agora é que nos permitem fazer chamadas de vídeo com amigos do outro lado do mundo ou transmitir nossas músicas favoritas instantaneamente. Vamos então desvendar os segredos por trás dessas **redes possibilitam a conexão com o mundo exterior!**

LANs: Uma Local Area Network (rede local) é uma rede que funciona dentro de uma área restrita ou particular, como uma casa (ou condomínio), proporcionando a conexão e troca de informações entre os aparelhos daquele ambiente, seja através de fios ou pelo ar. Para facilitar seu entendimento, pense comigo essa situação: Você fez uma atividade de redação para entregar na aula do dia seguinte, sendo que ela foi digitada e deve ser avaliada de maneira física, o que você faz? Exato! Conecta seu computador a impressora da sua residência e realiza a impressão da redação. Este tipo de ação tão comum no nosso cotidiano se encaixa perfeitamente no conceito de LAN.

WANs: Uma Wide Area Network (rede de longa distância), quando vistas de uma maneira simplificada, podem ser definidas como um conjunto de LANs que se relacionam entre si, promovendo conexões entre locais distantes como cidades, estados ou até mesmo países. Dessa forma, dois mecanismos são essenciais para que esse tipo de rede funcione: as linhas de transmissão, que passam as informações entre os computadores, e os roteadores, que direcionam os dados aos locais que devem ser enviados. Com isso, trazendo exemplos da realidade, é através das WANs que conseguimos trocar mensagens nas redes sociais com alguém do outro lado do planeta, por exemplo.

Além das redes de tipo LAN e WAN, temos também uma tecnologia muito conhecida no nosso dia a dia: o Wi-Fi (Wireless Fidelity). O Wi-Fi não ganhou a fama que tem à toa: ele é que proporciona a conexão entre as LANs e a Internet, sem a necessidade de uso de fios. Essa inovação revolucionou a maneira pela qual nossa sociedade se comunica e desenvolve nas mais diversas esferas, como a educação, a saúde, o entretenimento, os esportes e múltiplas outras áreas, proporcionando novas possibilidades de criações e negócios no mundo inteiro. Assim, no contexto de redes, ele é um mecanismo praticamente indispensável para o repasse de conjuntos de informações.

Dispositivos de rede

Até aqui você já percebeu quantas variações de rede nós temos, certo? Então, para que essas redes funcionem com eficiência e rapidez, é necessário certos objetos físicos que realizem a conectividade entre elas, são os dispositivos de rede. Dê uma olhadinha aí embaixo, talvez já conheça alguns deles.

Roteadores

São dispositivos utilizados para encaminhar pacotes de dados de uma rede para outra, estando ligados a uma ou mais redes. Além disso, eles usam como direcionamento para envio dos dados os endereços IP e são um dos principais mecanismos para conexão com a Internet.



Switches

São equipamentos que contêm várias portas de conexão isoladas, o que evita colisões e encaminham pacotes de dados para o destino especificado através dos endereços MAC, tornando a conectividade veloz e eficiente. Por consequência, são muito utilizados para realizar a ligação entre LANs.



Hubs

São aparelhos com múltiplas conexões e que, ao receber um quadro de dados, repassa-os a todas as outras redes conectadas a ele, sem sequer examinar os endereços, tornando-os inúteis em sua função. No mais, na chegada de dois quadros ao mesmo tempo, acontece uma colisão.



Meios de transmissão

Os meios de transmissão são recursos, divididos em **guiados** (cabos) e **não guiados** (espaço livre), utilizados para **enviar informações** do local de origem através de sinais que são interpretados pelos dispositivos de destino por meio do processo de conversão dos dados. Vamos conhecer alguns desses meios?

- **Cabos de par trançado:** São formados por dois condutores, geralmente feitos de cobre e revestidos por plástico, tendo sua estrutura trançada como um método para impedir a interferência de sinais indesejados durante a transmissão, ou seja, o receptor não perceberá diferença na tensão elétrica, captando a informação sem alterações.



- **Cabo Coaxial:** Esse tipo de cabo consiste em um único fio condutor central revestido por um material isolante e malha metálica, sendo esta uma espécie de segundo condutor, o que proporciona uma maior qualidade na transmissão dos dados, por exemplo, nas redes de TV à cabo e de telefonia.



- **Cabos de Fibra Óptica:** Esses cabos têm uma estrutura semelhante à dos coaxiais, entretanto, tem seu revestimento interno de vidro e o externo de plástico. Por isso, promovem a transmissão da energia com o processo conhecido na Física como reflexão, que permite que a luz “corra” por um canal devido a diferença de densidade entre os materiais que compõem o condutor. Portanto, devido a sua grande velocidade no envio das informações, é o meio de transmissão mais aplicado atualmente nas redes.



- **Espaço Livre:** Para a transmissão por espaço livre, não há necessidade de elementos físicos para a condução das informações, sendo estas transportadas pelas ondas eletromagnéticas, como ondas de rádio, infravermelhas e microondas. Assim, exemplos de seu uso no dia a dia são: rádios, redes de televisão e redes via satélite.





Capítulo 3



Nesse ponto da nossa jornada, vamos para o território dos **protocolos de redes**. Prepare-se para desvendar os mistérios dos protocolos, que são como o **idioma secreto dos computadores quando eles conversam entre si**. Vamos aprender como essas **regras invisíveis permitem que você navegue** na tecnologia. Então, coloque seu chapéu de exploradora digital e embarque nesta aventura!



Protocolos de redes

Um protocolo de rede pode ser definido como **um conjunto de regras que controlam a comunicação dos dados entre entidades diferentes**. Portanto, ele orienta de que modo a mensagem deve ser passada, o que ela é e quando deve ser enviada. Dessa forma, sistemas com estruturas diferentes conseguem estabelecer uma relação de troca sem barreiras.

Neste capítulo, vamos aprender sobre o protocolo HTTP, o HyperText Transfer Protocol, para que **nossos estudos sobre Web possam ser estruturados da melhor forma possível**. Vamos lá?



HTTP e seus métodos

O HTTP (HyperText Transfer Protocol) é um protocolo do tipo solicitação-resposta que **organiza as mensagens que os clientes** (usuários) **podem enviar para o servidor** e as **respostas que devem receber** através dele, ou seja, ele direciona os caminhos de transmissão dos dados na comunicação via Internet.

Com base na definição de HTTP, os métodos podem ser explicados como **um recurso de solicitação ou de resposta** de uma ação pelo cliente dentro da navegação Web. Veja alguns exemplos abaixo:

GET

O método GET solicita ao servidor que leia/apresente uma página, por exemplo, ao digitar “www.google.com” e pressionar ENTER, esse método é aplicado.

POST

O método POST consiste em enviar dados do cliente para o servidor, ou seja, quando preenchemos um formulário ou compramos algum item, essas informações são repassadas como resultado.

PUT

Este método pode ser descrito como o contrário de GET pois, ao invés de demonstrar uma página, ele tem a função de escrever uma ou mais novas páginas, dessa maneira, pode armazenar um conjunto delas em um servidor.

DELETE

Como o próprio nome diz, o método DELETE tem a função de apagar/remover determinada página, ou pelos menos indica que o servidor autorizou esse tipo de ação de exclusão.

Estruturas de solicitação e de resposta

A estrutura de solicitação é composta por **quatro partes principais**:

- **Linhas de solicitação**: método, URI e versão do HTTP
- **Cabeçalhos**: configuração do documento/informações adicionais
- **Linha em branco**
- **Corpo**: contém o documento

Veja um exemplo abaixo:



```
HTTP

GET / HTTP/1.1

Host: https://mermasdigitais.vercel.app/
Accept-Language: pt-br
```

No caso da estrutura de resposta, ela é semelhante à anterior, porém com a diferença em sua primeira linha, sendo composta por:

- **Linha de status**: versão do HTTP, código e mensagem
- **Cabeçalhos**
- **Linha em branco**
- **Corpo** (em algumas situações).

Observe o exemplo:



```
HTTP

HTTP/1.1 200 OK
Date: Sat, 09 Oct 2010 14:28:02 GMT
Server: Apache
Last-Modified: Tue, 01 Dec 2009 20:18:22 GMT
ETag: "51142bc1-7449-479b075b2891b"
Accept-Ranges: bytes
Content-Length: 29769
Content-Type: text/html

<!DOCTYPE html... (here comes the 29769 bytes of the requested web page)
```

URI e URL: qual é a diferença?

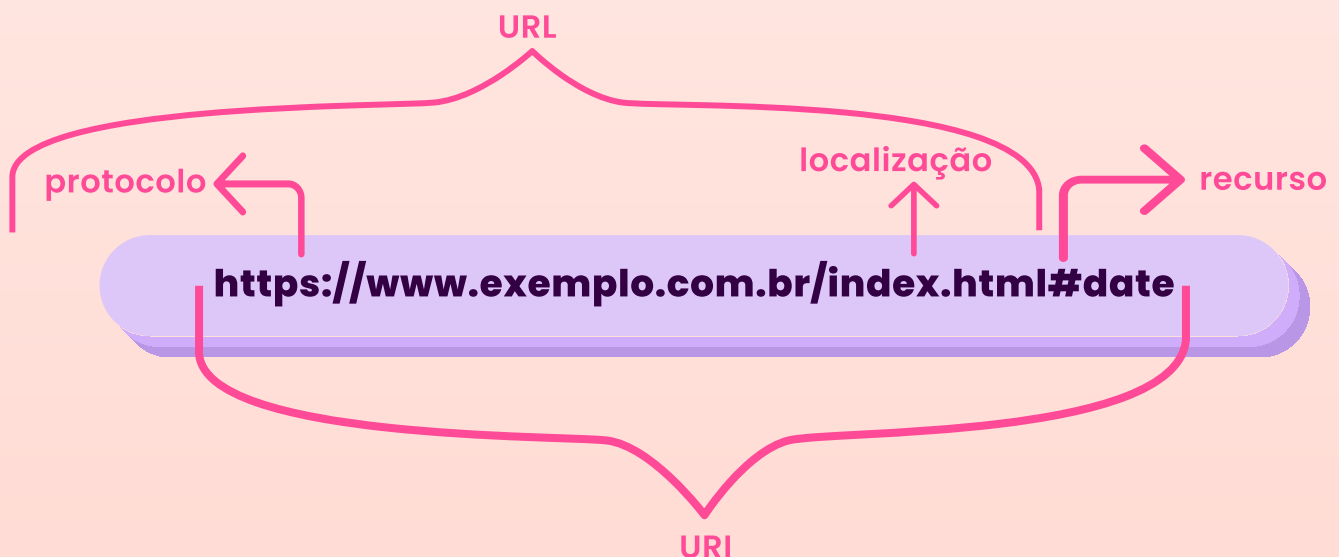
O termo URL é muito conhecido pela internet, no entanto é muito comum que se confunda ele com URI, devido à semelhança das siglas.

O URL (Uniform Resource Locator) é um **endereço** que cada página da Web possui. Ele **facilita a busca de informações** na Web e é constituído por quatro partes:

- **Protocolo:** regras para acesso
- **Host:** computador onde a informação está hospedada
- **Porta:** número
- **Path:** localização do arquivo onde a informação está armazenada

Por outro lado, o URI (Uniform Resource Identifier), é uma **generalização do URL**, como o nome de um único arquivo ao invés do endereço completo, facilitando a busca de qualquer recurso seja dentro ou fora da Web.

Segue abaixo esquema explicativo dos termos.



Assim, de modo simples, pode-se dizer que:

URL = URI - recurso

UNIDADE 03

segurança da informação





Capítulo 1



Nesta unidade, você vai adentrar o universo da Segurança da Informação. A gente sabe que, hoje em dia, **todo nosso cotidiano está interligado com informações e dados**, então é indispensável conhecer os principais termos e conceitos da área, além de aprender como se proteger nessa era digital.

Os **ataques cibernéticos** estão **cada vez mais avançados**, afetando pessoas, empresas e até países. Isso acontece por uma série de fatores que deixam o trabalho dos profissionais de segurança da informação ainda mais desafiador, mas com a mentalidade certa, a gente encara de frente essa situação!

Então, vamos tratar, neste capítulo, conceitos e ideias introdutórias a respeito da área de Segurança da Informação. O objetivo é estabelecer as bases para que, ao final desta unidade, seja possível não apenas entender a teoria do assunto em questão, mas também **lidar da maneira correta em situações de perigo nas redes**.



Introdução

Mermã, tu tá preparada pra mergulhar de cabeça em um mundo essencial para proteger nosso vasto e complexo ecossistema digital: a Segurança da Informação? Prepare-se para essa jornada que vai te levar **desde os conceitos mais elementares até as estratégias avançadas de segurança cibernética**, tudo começando aqui.

Pra começar nossa aventura, tu sabe o que significa “Segurança da Informação”? O termo “Segurança da Informação” vem ganhando maior notoriedade em decorrência dos **golpes sofridos na atual era tecnológica**. Mas precisamos entender o que ele significa.

Segurança da Informação refere-se a um **conjunto de práticas, políticas, procedimentos e tecnologias** projetadas para **proteger informações sensíveis e sistemas de informação contra ameaças, riscos e acessos não autorizados**.

A Segurança da Informação abrange **medidas que visam proteger os ativos de informação** contra ameaças que podem comprometer sua **confidencialidade, integridade e disponibilidade** (ISO/IEC, 2017). A proteção abrange tanto dados digitais quanto informações em formato físico, além dos sistemas que as manipulam, armazenam e transmitem.

Assim, podemos entender esses três pilares fundamentais da seguinte forma:

Confidencialidade

Este pilar se concentra na garantia de que as informações estejam acessíveis somente para pessoas autorizadas. Em outras palavras, as informações confidenciais não devem ser reveladas ou disponibilizadas para pessoas não autorizadas. A confidencialidade é mantida por meio de controles de acesso, criptografia e políticas de segurança.

Integridade

A integridade se refere à garantia de que as informações não sejam modificadas de forma não autorizada ou acidental. Isso significa que os dados devem permanecer precisos e confiáveis ao longo do tempo. A integridade é protegida por meio de controles de segurança que detectam e previnem alterações não autorizadas nos dados.

Disponibilidade

Este pilar diz respeito à garantia de que as informações e os sistemas estejam disponíveis e acessíveis quando necessário, sem interrupções indesejadas. Isso envolve a implementação de medidas de segurança que evitem ou minimizem interrupções, como ataques cibernéticos, falhas de hardware ou desastres naturais.

Esses três pilares são frequentemente referidos como os **Três Pilares da CIA**, do inglês, **Confidentiality, Integrity e Availability**. Além desses três pilares, outros conceitos, como **autenticidade, não repúdio e controle de acesso**, também desempenham papéis importantes na Segurança da Informação.

Importância

No dia a dia a gente usa muito a internet, né? É, de fato, muito incrível podermos dispor de tanta coisa legal: redes sociais, reuniões em casa, transações bancárias do celular... é muita coisa! Justamente por isso, **não podemos negligenciar a importância da Segurança da Informação**, já que sua ausência pode resultar em consequências adversas e, muitas vezes, irreparáveis.

Essas **consequências adversas** podem ser em várias escalas: seja individualmente, no âmbito empresarial ou mesmo governamental. Vamos entender um pouco a forma com que essas áreas são afetadas?

Privacidade Individual: É inegável o quão necessário é proteger a privacidade pessoal e evitar riscos financeiros e de identidade. Cada vez mais, nossas vidas estão entrelaçadas com a tecnologia e a internet, e, como resultado, nossas informações pessoais estão mais expostas do que nunca. Medidas como o uso de senhas fortes, a autenticação de dois fatores e a conscientização sobre phishing são essenciais para proteger nossos dados e identidade pessoal contra ameaças virtuais.

Empresas e Negócios: Independentemente do tamanho ou setor, a informação é um ativo valioso. A perda e comprometimento de dados de clientes, segredos comerciais, estratégias de mercado, etc., pode ter impactos financeiros significativos e até mesmo ameaçar a continuidade das operações. Portanto, a Segurança da Informação é essencial nesse cenário para manter a competitividade e garantir a confiança dos clientes.

Governo: Nesse cenário, a Segurança da Informação desempenha um papel vital na proteção de dados confidenciais, processos eleitorais e na manutenção da confiança pública. A integridade dos processos democráticos depende da proteção de informações relacionadas a eleições, votos e comunicações governamentais.

Em resumo, a Segurança da Informação não é apenas uma opção, mas uma **necessidade inegável**: ela garante a privacidade e segurança individuais, sustenta o funcionamento de empresas e protege a integridade dos processos governamentais — a Segurança da Informação é, indiscutivelmente, uma **decisão estratégica e responsável**!



Ética X Computação

Quando falamos de Segurança da Informação precisamos falar não apenas de suas questões técnicas, mas também de **complexos dilemas éticos** que impactam diretamente nossa sociedade.

A começar, um dilema ético muito falado: a **coleta massiva de dados pessoais** por empresas de tecnologia, que levanta preocupações sobre privacidade e o uso indiscriminado desses dados para fins comerciais ou políticos, algo que **pode invadir a privacidade dos indivíduos e comprometer sua autonomia**. Como seres humanos, valorizamos nossa capacidade de tomar decisões informadas e de manter nossa vida privada intacta. Quando empresas ou governos coletam massivamente dados pessoais sem nosso consentimento, surge uma tensão ética. Devemos considerar até que ponto isso é aceitável e quais medidas éticas devem ser implementadas para proteger nossa privacidade.

É interessante pontuar, ainda, a questão de **responsabilidade ética**: sistemas mais complexos trazem à tona a discussão sobre quem é responsável por eventuais violações de dados ou ataques cibernéticos. Outra questão ética importante diz respeito à segurança cibernética: à medida que a sociedade se torna mais dependente de sistemas de informação e infraestrutura digital, a responsabilidade ética de proteger esses sistemas contra ataques cibernéticos maliciosos torna-se uma prioridade. A falta de **segurança cibernética** adequada pode resultar em sérias consequências, desde o roubo de dados pessoais até **ameaças à segurança nacional**.

O desenvolvimento de **armas cibernéticas** também levanta dilemas éticos significativos. A **capacidade de lançar ataques cibernéticos devastadores** cria um novo campo de batalha virtual, onde as normas éticas e legais estão em constante evolução. Portanto, é essencial levar em consideração a dissuasão cibernética e a busca pela estabilidade nas relações internacionais no âmbito digital.

Em resumo, as questões éticas relacionadas à computação são fundamentais para **moldar o futuro da tecnologia e da sociedade**. À medida que a tecnologia continua a avançar, é imperativo que a sociedade e os profissionais da computação se envolvam em discussões éticas robustas para **garantir que a tecnologia seja usada de maneira responsável e benéfica para todos**.



Capítulo 2



Neste capítulo, nossa jornada passará pelas **ameaças e vulnerabilidades** que podem acometer pessoas, empresas, ou mesmo países. Até o final do capítulo, vamos ter um maior entendimento sobre essas ameaças e, ainda, sobre **como se proteger e evitar danos maiores** ao navegar pela rede.

No mundo da cibersegurança, compreender as ameaças e vulnerabilidades é como **desvendar os segredos de um quebra-cabeça complexo**. Este capítulo nos conduzirá por um cenário onde navegaremos pelas brechas digitais das ameaças cibernéticas e que podem comprometer a segurança de sistemas e dados. Para proteger o que valorizamos, precisamos primeiro **compreender esses perigos e as fraquezas** que existem. Vamos embarcar nessa aventura?



Ameaças e vulnerabilidades

Uma **ameaça cibernética** representa **um risco à integridade, confidencialidade ou disponibilidade** de recursos digitais. São **eventos indesejados** que tem o potencial de **prejudicar** e comprometer a segurança dos sistemas de computador, redes, dispositivos ou dados.

O objetivo das ameaças é explorar **vulnerabilidades** em sistemas de TI para **causar danos**, roubar informações ou interromper serviços. As ameaças podem, também, envolver fatores humanos, como negligência ou má conduta de funcionários, que podem resultar em violações de segurança.

Vamos agora conhecer algumas **técnicas de ameaças** que são muito populares por afetarem muitas pessoas diariamente. Entenderemos também como são feitas, que forma elas **afetam os usuários**, além de entender como se **proteger** de cada uma delas. Bora lá?

Ataque da força bruta

Um ataque de força bruta é uma técnica usada em cibersegurança onde um invasor tenta **descobrir uma senha ou chave de criptografia** através de **tentativas repetidas e sistemáticas**. Essencialmente, o ataque de força bruta envolve o uso de um **programa de computador ou script** para gerar uma grande quantidade de combinações possíveis de senhas, números PIN ou chaves de criptografia até encontrar a correta.

Este tipo de ataque é chamado de **força bruta** porque **não há tentativa de usar técnicas sofisticadas** para adivinhar a senha; em vez disso, o atacante simplesmente testa todas as possíveis combinações até encontrar a que funciona.

Phishing

O *phishing* é uma técnica de ataque cibernético na qual os criminosos tentam **enganar** as pessoas para que revelem **informações confidenciais**, como senhas, números de cartão de crédito ou informações pessoais, geralmente se passando por uma entidade confiável. Essa técnica recebeu esse nome como uma variação da palavra em inglês *fishing*, que significa “pescaria”.



Os ataques de *phishing* geralmente ocorrem por meio de e-mails falsos, mensagens de texto, sites fraudulentos ou até mesmo ligações telefônicas. Os principais elementos do *phishing* são: **isca, engano, direcionamento para sites falsos, coleta de informações e uso malicioso**. Na primeira etapa, tem-se a criação da isca: os criminosos elaboram mensagens que aparentam ser de fontes legítimas, muitas vezes imitando empresas conhecidas, como bancos ou redes sociais. A essência do *phishing* é o elemento do engano, onde as mensagens tentam persuadir o destinatário a tomar ações urgentes, como verificar informações de conta, atualizar senhas, clicar em links maliciosos ou baixar anexos, a fim de enganar a vítima.

Um truque comum no *phishing* envolve o **redirecionamento para sites falsos**: quando as vítimas seguem as instruções enganosas, são levadas a páginas da web falsificadas que imitam perfeitamente sites legítimos, que são habilmente projetadas para coletar informações sensíveis quando inseridas pela

vítima e, como resultado, os criminosos coletam informações pessoais, como **senhas, números de cartão de crédito e detalhes bancários**. Com acesso a esses dados confidenciais, os criminosos podem realizar **atividades maliciosas**, como roubo de dinheiro, compras não autorizadas e crimes de identidade.

Pharming

O *pharming* é uma técnica que **se assemelha ao phishing** em alguns aspectos, mas tem uma abordagem diferente: enquanto o phishing visa enganar os usuários para que revelem informações confidenciais por meio de mensagens, o *pharming* envolve a **manipulação dos sistemas de resolução de nomes de domínio** (DNS, do inglês *Domain Name System*) **para redirecionar o tráfego da web de forma fraudulenta**.



O *pharming* é composto de vários elementos. Começa com a **manipulação** do DNS, explorando vulnerabilidades nos servidores DNS ou infectando os computadores das vítimas com software maliciosos (os famosos malwares) para redirecionar o tráfego da web para sites falsos, **mesmo quando os usuários inserem os endereços corretos**. A segunda fase envolve o redirecionamento para esses sites falsos para que, com a **coleta de informações confidenciais**, como senhas e números de cartão de crédito fornecidas pelas vítimas, os criminosos possam **realizar atividades fraudulentas**.

Baiting

O *baiting* é um termo que se originou da palavra em inglês *bait*, que significa "iscar". Em termos de segurança da informação, o *baiting* é uma tática de ataque na qual os criminosos **oferecem algo atraente**, como um arquivo ou link, para enganar as vítimas e induzi-las a realizar **ações prejudiciais**, como clicar em um link malicioso ou baixar um arquivo infectado.



Tudo começa com a criação de uma isca atraente pelos criminosos. Eles elaboram **arquivos com nomes sugestivos**, como "Relatório de Bônus 2023" ou oferecem links tentadores, **prometendo conteúdo interessante**, como downloads

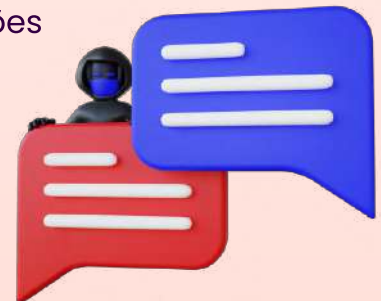
gratuitos de músicas, filmes ou software. O elemento crítico do *baiting* é a propagação de um malware: quando a vítima clica no link ou baixa o arquivo, o malware é **silenciosamente instalado em seu sistema**.

Uma vez que o malware se infiltra no sistema da vítima, ele pode ser utilizado para várias **atividades maliciosas**, como roubo de informações, controle remoto do sistema ou criptografia de arquivos para extorsão de resgate. Assim, o *baiting* consegue cumprir seu propósito de explorar a falsa promessa de obter algo valioso e gratuito, levando as vítimas a caírem na armadilha, levando a danos significativos em vez do benefício prometido.

Pretexting

O *pretexting* é uma técnica em que um atacante **cria um pretexto para obter informações** pessoais ou confidenciais de uma pessoa, o que envolve a manipulação psicológica da vítima, fazendo-a **acreditar** que está fornecendo informações a alguém **legítimo** ou em uma situação legítima.

A primeira etapa do *pretexting* é a criação de um pretexto pelo atacante, que **inventa uma história plausível** para obter informações desejadas, frequentemente se passando por uma **figura confiável** — o objetivo é ganhar a confiança da vítima, usando informações que parecem genuínas. Com a confiança estabelecida, o atacante avança para a fase de solicitação de informações confidenciais, onde busca dados altamente sigilosos e, para **aumentar** suas **chances de sucesso**, podem usar **táticas de manipulação** psicológica, como pressão ou urgência, para persuadir a vítima a divulgar as informações solicitadas. Por fim, munidos das informações desejadas, o atacante utiliza-as para diversos **fins maliciosos**.



Mermã, sabia disso?



Essas técnicas, todas envolvendo manipulação psicológica, fazem parte da **engenharia social**. Nesse campo, cibercriminosos exploram a natureza humana, enganando e persuadindo pessoas a divulgar informações sensíveis ou realizar ações em benefício dos atacantes.



Malwares

Agora, nossa jornada nos levará ao intrigante e muitas vezes sombrio **mundo dos malwares**, ou softwares maliciosos. Prepare-se para mergulhar fundo nesse universo, onde encontraremos vírus, worms, trojans, ransomware e muitos outros tipos de inimigos cibernéticos. Pegue sua mochila tecnológica e vamos entender e implementar estratégias eficazes de proteção contra malwares e **defender a trindade da integridade, confidencialidade e disponibilidade** das informações vitais em computadores e redes!

Vírus: É um tipo de programa, geralmente prejudicial, que se espalha ao se infiltrar em outros programas ou arquivos em um sistema. Essa infiltração permite que o vírus se torne parte desses programas e arquivos, aguardando a execução do programa hospedeiro para se tornar ativo e iniciar o processo de infecção. Uma característica dos vírus é sua capacidade de criar cópias de si mesmos, o que lhes permite se multiplicar dentro do computador, tornando-se uma ameaça persistente e desafiadora para a segurança. Os efeitos dos vírus podem variar desde simples travamentos e desaceleração do sistema até a perda de dados significativa e danos a programas e arquivos importantes.

Trojan: Também conhecido como cavalo de Troia, é um programa que se disfarça como algo inofensivo para enganar o usuário (conforme a lenda grega). No entanto, além de suas funções aparentes, um *trojan* executa operações ocultas e frequentemente maliciosas, como abrir portas de acesso não autorizadas, desativar ferramentas de segurança e enviar informações sobre o sistema do usuário, que podem ser exploradas por invasores para planejar ataques. Assim, escondendo suas verdadeiras intenções, representam uma ameaça à segurança do computador e à privacidade do usuário.

Spyware: Como o próprio nome sugere, esse malware é como um espião. São softwares que monitoram e rastreiam as atividades de um sistema, enviando as informações coletadas para terceiros. Embora possam ser usados legitimamente, esses programas são frequentemente implantados de maneira dissimulada e maliciosa. Sua presença representa uma ameaça à privacidade e segurança, tornando a detecção e remoção cruciais para proteger o sistema e a privacidade do usuário.

Worms: Já esse tipo de software malicioso, tem a capacidade de se espalhar automaticamente através de redes, explorando vulnerabilidades em programas, sistemas ou configurações de software. Eles possuem alto potencial de disseminação e, ao contrário dos vírus, não se incorporam a outros programas ou arquivos e não precisam da execução do usuário para se propagar. Eles podem abrir portas de acesso para permitir a entrada de novos *worms*, o que os torna uma ameaça de propagação rápida. Podem ter objetivos variados, desde causar danos a sistemas e arquivos até interromper serviços de rede ou permitir a entrada de outros malwares nos sistemas afetados.

Botnets: Também chamados de redes de bots na internet, são grupos de computadores comprometidos por malware e controlados por cibercriminosos. Esses *bots* são máquinas infectadas que realizam tarefas automatizadas sob o comando do invasor e, além disso, se espalham explorando vulnerabilidades em sistemas e software desatualizado. Uma vez implantados, conectam-se a um servidor de comando e controle (C&C) controlado pelo criminoso e permitindo que os invasores conduzam várias atividades maliciosas.

Ransomware: É uma ameaça cibernética grave que funciona como um sequestro digital. Os criminosos infectam o sistema da vítima e criptografam seus dados, tornando-os inacessíveis. Em troca, exigem um resgate em criptomoedas para fornecer a chave de descriptografia. Geralmente, a infecção começa com o usuário abrindo um arquivo malicioso de e-mail ou site comprometido. Empresas são alvos frequentes, causando interrupções graves e perda de dados. A prevenção é crucial, envolvendo a conscientização dos funcionários, uso de software de segurança atualizado e backups regulares de dados como medidas de segurança.

Agora que exploramos vírus, worms, trojans, spyware, e até mesmo botnets e ransomware, é hora de **fortalecer nossas defesas** e **encarar o futuro digital** com confiança. Lembre-se, essa jornada de aprendizado nunca termina, pois o cenário cibernético está em constante evolução — mas, com o conhecimento e a vigilância que adquirimos até aqui, estamos mais preparados do que nunca para navegar por essa paisagem digital desafiadora. Vamos continuar nossa exploração, pois estamos quase no fim dessa emocionante jornada pela cibersegurança!



Capítulo 3



Com grandes conexões vêm grandes responsabilidades, por isso, vamos dar continuidade na nossa aventura neste capítulo capítulo do livro. É hora de explorar os segredinhos para ser o mestre da segurança online e aprender a **navegar pelo ciberespaço como um expert**. Afinal, viver nesse mundo ultraconectado à internet é tudo, e nós vamos te mostrar como é fácil ficar por dentro desse assunto! Você vai ficar por dentro das melhores formas de **como se proteger online**. Vamos dominar esse conteúdo e mostrar pro mundo todo **a força que nosso conhecimento adquirido tem!**

Backup

Prevenir a perda de dados é essencial e isso pode acontecer devido a diversas razões, como falhas no hardware, ataques de malware, erros humanos ou até mesmo desastres naturais. O backup evita a perda desses arquivos importantes e é por isso que é uma ferramenta tão essencial para sua segurança cibernética.

E como fazer backups eficazes?

1. Escolha uma solução de backup: Existem várias opções disponíveis, como unidades externas, serviços de armazenamento em nuvem e software de backup. Escolha a que melhor atenda às suas necessidades.
2. Faça backups regulares: Estabeleça um cronograma para fazer backups, seja diária, semanal ou mensalmente, dependendo da quantidade de novos dados que você cria.
3. Armazene seus backups em locais seguros: Se você está usando dispositivos de armazenamento físico, mantenha-os em locais seguros. Para backups em nuvem, escolha provedores confiáveis.
4. Teste seus backups: Periodicamente, verifique se você pode restaurar dados dos seus backups. Isso garante que seus backups sejam funcionais quando você mais precisar deles.

Senhas

Senhas fortes são cruciais porque dificultam que invasores adivinhem ou quebrem a senha e acessem suas contas, que frequentemente contêm informações pessoais sensíveis. Além disso, usar senhas diferentes para cada conta impede que um único vazamento de senha comprometa todas as suas contas.

Então, como criar senhas fortes e seguras?

1. Complexidade: use uma combinação de letras maiúsculas, minúsculas, números e caracteres especiais como !, @, #, \$.
2. Tamanho: quanto mais longa a senha, melhor, então tente criar senhas com pelo menos 12 caracteres.
3. Evite informações fáceis de adivinhar: nomes de familiares ou datas de nascimento são sempre muito óbvios.
4. Senhas exclusivas para cada conta: gerenciar várias senhas pode ser desafiador, mas você pode contar com um gerenciador de senhas confiável para mantê-las seguras.
5. Autenticação de dois fatores.
6. Atenção a e-mails suspeitos: nunca compartilhe senhas por meio de links suspeitos.

Criptografia

A criptografia é uma técnica que embaralha seus dados, tornando-os ilegíveis para qualquer pessoa que não tenha a chave de descryptografia correta. É usada para proteger informações confidenciais durante a transmissão, armazenamento e até mesmo enquanto estão em uso.

A criptografia é usada em várias áreas da cibersegurança, incluindo comunicações seguras pela Internet (como HTTPS), armazenamento de dados sensíveis, proteção de senhas, autenticação de usuários e na segurança de transações financeiras online.

Autenticação de dois fatores

A autenticação em dois fatores é um método que requer não apenas uma senha, mas também algo que apenas você possui, como um código gerado por um aplicativo ou um dispositivo físico.

Mesmo que alguém obtenha sua senha, não poderá acessar sua conta sem o segundo fator de autenticação. O 2FA torna mais difícil para os atacantes enganá-lo, mesmo que saibam sua senha.

Para implementar com sucesso a **criptografia** e a **autenticação de dois fatores** (2FA), é essencial seguir algumas etapas cruciais. Primeiramente, certifique-se de que todas as suas contas estejam protegidas com **senhas robustas** e exclusivas. Em seguida, acesse as configurações de segurança das suas contas online e **ative a autenticação em dois fatores** sempre que essa opção estiver disponível. Para facilitar o gerenciamento de senhas, considere o uso de um **gerenciador de senhas confiável**, que pode ajudar na geração e armazenamento de senhas seguras.

Além disso, é fundamental manter seus **dispositivos e aplicativos** regularmente **atualizados** para garantir que você esteja aproveitando as últimas medidas de segurança, incluindo a criptografia. As atualizações de software são vitais para proteger nossos dispositivos contra ameaças online: elas corrigem vulnerabilidades, adicionam segurança e melhoram o desempenho. Gerenciar atualizações adequadamente envolve configurar atualizações automáticas, verificar regularmente se há atualizações, priorizar as de segurança e fazer backups antes das atualizações importantes. Seguindo essas diretrizes, você estará **fortalecendo significativamente** a segurança das suas contas e informações pessoais online.



Proteção nas redes sociais

O **uso responsável das redes sociais** é outro ponto fundamental de se discutir quanto à **presença online**. É importante lembrar que as redes sociais podem afetar nossa autoestima, por isso evite a constante comparação com os outros, proteja sua privacidade ajustando as configurações de privacidade e denuncie casos de cyberbullying. Evite, também, postagens impulsivas, pois elas podem ter consequências duradouras. Além disso, esteja ciente de notícias falsas e desinformação e promova a positividade online.

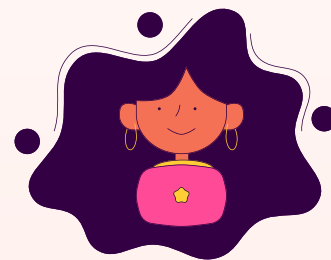
Gerenciar seu tempo nas redes sociais também é muito importante, pois elas podem se tornar uma distração significativa. Estabeleça limites de tempo e evite usá-las durante a noite para preservar a qualidade do sono. Lembre-se de reservar tempo para atividades offline, como exercícios e interações pessoais.

O **compartilhamento de informações** é uma parte fundamental da vida online, mas deve ser feito com responsabilidade. Proteja sua privacidade pensando cuidadosamente sobre quais informações compartilha e com quem. Evite contribuir para a disseminação de notícias falsas e verifique a precisão das informações antes de compartilhá-las. Lembre-se de que suas palavras e ações online têm um impacto real, então seja responsável pelo que compartilha e respeite a privacidade dos outros.

O compartilhamento de informações na era digital é uma ferramenta poderosa para a conexão e a aprendizagem, mas também pode ter consequências negativas se não for feito com responsabilidade. Portanto, lembre-se sempre de pensar no impacto de suas ações online e de **agir com responsabilidade para manter um ambiente online seguro e construtivo**.



Referências



ALVES, Igor. **Informática Básica. Sistemas Operacionais**. Disponível em: <https://docentes.ifrn.edu.br/igorlves/informatica-basica/sistemas-operacionais-1/view>

ALVES, Igor. **Informática Básica. Sistemas Operacionais**. Disponível em: <https://docentes.ifrn.edu.br/igorlves/informatica-basica/sistemas-operacionais-2/view>

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 4. ed. McGraw-Hill, 2008.

KUROSE, J.F. **Redes de Computadores e a Internet: uma abordagem top-down**. 6. ed. São Paulo: Pearson, 2014

MACHADO, F. N. R. **Segurança da Informação: Princípios e Controle de Ameaças**. 1 ed. São Paulo: Érica, 2014.

MANZANO, J. A. OLIVEIRA, J. F. **Algoritmos: lógica para desenvolvimento de programação de computadores**. 29 ed. São Paulo: Érica, 2019

MONTEIRO, M. A. **Introdução à Organização de Computadores**. 5 ed. Rio de Janeiro: LTC, 2007.

SOUSA, L. B. **Rede de Computadores: Guia Total**. 2 ed. São Paulo: Érica, 2009.
TANENBAUM, A. S. **Redes de Computadores**. 5ª Ed. Pearson, 2011.