Nivelamento

Seja bem-vindo ao Nivelamento!

O curso aborda introdução à cibersegurança, incluindo tipos de hackers, ethical hacking e as várias profissões no campo, além de arquitetura de computadores e a instalação de sistemas operacionais, camada de aplicação, com foco em serviços essenciais de rede e práticas de segurança, proporcionando uma base sólida para quem busca compreender os fundamentos da TI e cibersegurança.

# Introdução à cibersegurança

Neste curso, você vai conhecer qual a definição de hacker e quais os tipos e categorias mais conhecidos. Aprenderá, também, o que é ética e qual a importância desse conceito para a segurança da informação. Além disso, conhecerá o que significa os principais termos e nomenclaturas dos profissionais responsáveis pela segurança da informação de uma empresa, o que são e quais os principais tipos de vírus que causam danos a um computador e quais as boas práticas de cibersegurança que devemos adotar no dia-a-dia.

## Aula 1 - O que é Hacker e seus Tipos

Com o avanço da tecnologia e da interatividade digital, nós utilizamos cada vez mais os dispositivos eletrônicos para trabalho, para o lazer e até mesmo para compras online. Independente do dispositivo, acessar sites, lojas virtuais e redes sociais exigem a inclusão do cadastro de dados pessoais que, se forem expostos à terceiros, podem nos causar sérios prejuízos.

A segurança da informação é um campo vital na era digital, pois envolve medidas como a criptografia, autenticação multifator, firewall, entre outros, para garantir a proteção e segurança de dados sensíveis dos usuários. Porém, caso haja alguma brecha nesse sistema, pode ser uma porta aberta para o ataque de hackers.

Hackers

* Hacker é o nome dado para o indivíduo que tem grande habilidade e conhecimento em computação e tecnologia. Capazes de criar softwares e sistemas complexos, com o passar do termo, o termo hacker foi atribuído àqueles que usam suas habilidades para atividades ilegais e cometer crimes, como a invasão de sistemas e o roubo de dados e informações.

Hacking

* Hacking também pode ser definido como: o ato de comprometer dispositivos e redes digitais por meio de acesso não autorizado a uma conta ou sistema de computador.
* O termo hacking apareceu pela primeira vez na década de 1970, mas se tornou mais popular na década seguinte, com o lançamento de filmes como Tron e WarGames, que mostravam personagens invadindo sistemas de computador.
* Nessa época, também ocorreram os primeiros casos de ataques cibernéticos a grandes organizações, como o Laboratório Nacional de Los Alamos e o Sloan-Kettering Cancer Center.
* Foi então que o Congresso dos Estados Unidos aprovou as primeiras leis sobre crimes de informática e que a palavra hacker passou a ter uma conotação negativa.

Origem do termo hacker

* A palavra "hacker" surgiu nos anos 70, quando os primeiros programadores começaram a criar softwares e sistemas mais complexos.
* No entanto, com o passar do tempo, o termo acabou sendo associado a atividades ilegais e criminosas, como invasão de sistemas e roubo de informações, por exemplo. É importante ressaltar que nem todo hacker é um criminoso e que essa visão equivocada tem gerado muita confusão.

Diferença entre hacker e cracker

* A diferença entre hacker e cracker é bastante sutil, mas importante.
* Enquanto o termo hacker se refere a um indivíduo que possui grande habilidade e conhecimento em computação e tecnologia e usa essas habilidades para encontrar soluções criativas e inovadoras para problemas relacionados a essas áreas, o termo cracker é usado para se referir a um indivíduo que usa suas habilidades em computação para atividades ilegais e mal-intencionadas, como invasão de sistemas e roubo de informações.

Ética

* A ética é o ramo da filosofia que lida com questões de moralidade, ou o que é considerado comportamento certo e errado. Preocupa-se em examinar e avaliar os princípios e valores que orientam a conduta humana e a tomada de decisão.
* O comportamento ético é o comportamento consistente em princípios e valores. Envolve tomar decisões e agir de acordo com princípios morais como honestidade, integridade, justiça, respeito pelos direitos humanos e preocupação com o bem- estar dos outros.
* Em termos práticos, o comportamento ético envolve a adesão a códigos de conduta ou diretrizes éticas em várias áreas da vida, como negócios, saúde, direito e educação. Também envolve considerar o impacto potencial das ações de alguém sobre os outros e tomar decisões justas e corretas.
* Em última análise, o comportamento ético é fazer o que é certo, mesmo quando é difícil ou inconveniente. Requer o compromisso de defender os princípios e valores morais e a disposição de assumir a responsabilidade pelas próprias ações e suas consequências.

Quais são os tipos de Hackers?

Hats - chapéus

* Podemos classificar em três categorias os tipos de hackers, são eles: black hat, grey hat e white hat. Alguns hackers usam seus conhecimentos para ajudar empresas e instituições a se protegerem contra as ameaças cibernéticas, enquanto outros hackers usam seus conhecimentos para causar danos e roubar dados.

White hat hackers (hackers éticos)

* O primeiro tipo que vamos abordar é o White Hat hacker, também conhecido como hacker ético. Os hackers éticos, que são especialistas em segurança da computação que atuam fazendo testes de invasão e outras metodologias para garantir que os sistemas de informação de uma empresa sejam seguros. Eles têm autorização para acessar os sistemas e procurar por vulnerabilidades que possam ser corrigidas. Eles são os “mocinhos” da cibersegurança e são contratados por empresas e instituições para melhorar sua proteção.
* Exemplos de ataques feitos por White hat hackers (hackers éticos)
  + A descoberta do bug Heartbleed no OpenSSL em 2014, que permitiu que hackers roubassem informações sensíveis de sites que usavam o software. Os Hackers éticos descobriram a vulnerabilidade e a reportaram aos desenvolvedores para que ela pudesse ser corrigida.
  + A descoberta das vulnerabilidades Meltdown e Spectre nos processadores de computador em 2018. Os Hackers éticos descobriram as vulnerabilidades e as reportaram aos fabricantes para que elas pudessem ser corrigidas.

Black hat hackers (mal-intencionados)

* O segundo tipo é o Black Hat hacker. São os hackers criminosos, que obtêm acesso não autorizado a um sistema de computador ou rede com más intenções. Eles podem usar computadores para atacar sistemas visando lucro, diversão, motivações políticas ou como parte de uma causa social. Eles geralmente envolvem modificação ou destruição de dados, distribuição de vírus, worms e spam. Eles são os vilões da cibersegurança e estão sujeitos a punições legais.
* Exemplos de ataques feitos por Black hat hackers (mal-intencionados)
  + O ataque de ransomware WannaCry em 2017, que afetou mais de 200 mil computadores em 150 países e causou bilhões de dólares em danos.
  + A violação de dados da Equifax em 2017, que expôs as informações pessoais de mais de 147 milhões de pessoas.
  + A violação de dados da Target em 2013, que expôs as informações de cartão de crédito e débito de mais de 40 milhões de clientes.

Grey hat hackers (hackers neutros)

* Por fim, temos o Grey Hat hacker, que é uma mistura dos dois tipos anteriores. Eles às vezes agem legalmente, com boa vontade, e às vezes não. Eles não têm autorização para acessar os sistemas, mas também não têm intenções maliciosas. Eles podem invadir sistemas por curiosidade, desafio ou para alertar sobre falhas de segurança. Eles podem ocasionalmente cometer crimes durante o curso de suas explorações.
* Exemplos de ataques feitos por Grey hat hackers (hackers neutros)
  + Em 2018, um hacker neutro invadiu uma máquina de votação em uma conferência de hacking para demonstrar como era fácil fazê-lo. O hacker reportou a vulnerabilidade ao fabricante para que ela pudesse ser corrigida.

Script Kiddies ou “Iniciantes”

* Os script kiddies são hackers inexperientes que dependem de ferramentas e scripts desenvolvidos por outros para realizar seus ataques. Eles têm um conhecimento limitado e geralmente não possuem uma compreensão profunda dos sistemas que estão atacando. Eles geralmente copiam e colam códigos ou scripts que encontram na internet sem entender como eles funcionam. Os ataques realizados por script kiddies são geralmente motivados pelo desejo de se exibir, diversão e aprendizado.

Hacktivistas

* Dentro da comunidade hacker, encontramos também os "hacktivistas", cujo nome surge da junção das palavras "hacker" e "ativista". Esses hackers têm motivações políticas ou sociais e utilizam suas habilidades em ataques cibernéticos para promover causas em que acreditam. Eles podem ter diferentes visões ideológicas e podem apoiar ou se opor a governos, organizações ou movimentos sociais. Eles podem ser vistos como heróis ou vilões, dependendo do ponto de vista do público.

Conclusão

* É importante lembrar que as atividades de hackers, especialmente as dos black hats, são ilegais e devem ser evitadas. No entanto, os white hat hackers são uma exceção e podem ser usados para proteger empresas e governos de ataques cibernéticos.
* À medida que a tecnologia continua a evoluir, o papel dos hackers se tornará cada vez mais importante para garantir um ambiente digital seguro e protegido.

## Aula 2 - Conceito de Ética

Hackers éticos

Definição do conceito de Ética

* A ética pode ser definida como um código moral pelo qual uma pessoa vive, orientando seu processo de tomada de decisão e comportamento.
* No contexto da segurança da informação, a ética refere-se a um conjunto de princípios e diretrizes que os profissionais seguem ao trabalhar com dados, sistemas e tecnologias sensíveis (geralmente de terceiros).
* Isso é crucial porque os profissionais de segurança cibernética têm acesso a informações confidenciais e o poder de protegê-las ou explorá-las.

A importância da ética na segurança da Informação

* Na área da segurança da informação, a ética é fundamental para a proteção dos dados, garantindo a privacidade e a confidencialidade das informações.
* A ética na segurança da informação envolve questões como:
  + O uso ético de dados pessoais;
  + A avaliação dos reguladores em relação à proteção de dados;
  + A confiança do cliente em relação à privacidade dos dados.
* É importante que as organizações desenvolvam suas bases de dados em atenção a LGPD, prezando pela privacidade e proteção dos dados pessoais dos titulares, para resultados que não sejam uma ameaça à confiança da marca e à fidelidade do cliente.
* A ética também é fundamental na inteligência artificial e nas tecnologias de análise de dados, onde é necessário garantir que as tecnologias sejam usadas de maneira justa e igualitária, promovendo a equidade, a tomada de decisões corretas e o uso honesto dos dados.

Princípios e construção de ma cultura ética

* Um aspecto importante da ética na segurança da informação é o estabelecimento de princípios éticos comuns.
* Alguns princípios chaves são:
  + Confidencialidade
  + Integridade
  + Responsabilidade
* Confidencialidade: Profissionais de segurança lidam com informações pessoais, privadas ou proprietárias sensíveis que devem ser mantidas confidenciais. Garantir a confidencialidade é vital para manter a confiança entre organizações e clientes.
* Integridade: Profissionais de segurança devem agir com honestidade e transparência, aderindo aos mais altos padrões éticos. Isso inclui evitar conflitos de interesse, garantir relações justas e imparciais e promover uma cultura de responsabilidade.
* Responsabilidade: Os profissionais de cibersegurança têm o dever de proteger as informações e sistemas com os quais trabalham, além de relatar e abordar quaisquer vulnerabilidades ou riscos que descobrirem. Eles também devem estar preparados para enfrentar os dilemas éticos que surgem em seu ambiente de trabalho.

Para se ter sucesso na construção de uma cultura ética

* Construir uma cultura ética no campo da segurança da informação envolve incorporar esses princípios aos valores, políticas e programas de treinamento da organização e dos colaboradores.
* A tomada de decisões éticas deve ser promovida em todos os níveis da organização, desde diretoria até os colaboradores operacionais.

Benefícios da cultura ética na segurança da informação

* Promover uma cultura ética na segurança da informação tem vários benefícios como:
  + Confiança: Práticas éticas ajudam a construir confiança entre organizações e seus clientes e parceiros. Essa confiança é crucial para manter relacionamentos de longo prazo e garantir o sucesso da organização.
  + Conformidade: Adotar princípios éticos pode ajudar as organizações a cumprir requisitos legais e regulatórios, evitando penalidades e possíveis danos à reputação.

Benefícios da cultura ética

* Mitigação de riscos: A tomada de decisões e práticas éticas podem ajudar a identificar e mitigar riscos potenciais, como violações de dados ou ciberataques, protegendo a organização e seus stakeholders.
* Engajamento dos funcionários: Fomentar uma cultura ética pode aumentar o engajamento e a satisfação dos funcionários, levando a um melhor desempenho e retenção.
* Reputação: Uma organização com uma forte cultura ética é mais propensa a ser percebida positivamente por seus stakeholders, incluindo clientes, parceiros e o público em geral.

Exemplo de ética hacking

Hacking ético - estudo de caso

* Um hacker ético foi contratado por uma instituição financeira para realizar um teste de penetração em seu sistema bancário online. Nesse cenário, o hacker ético recebe permissão explícita para tentar violar os sistemas, redes ou aplicativos da organização, a fim de identificar vulnerabilidades e potenciais pontos de exploração.

Hacking ético

* Durante o teste, o hacker ético segue um estrito e rigoroso código de ética, que contempla os seguintes princípios:
  + Permissão: O hacker ético opera somente dentro dos limites definidos pela organização e com autorização adequada. Eles obtêm consentimento por escrito e definem claramente o escopo e as limitações do engajamento.
  + Confidencialidade: O hacker ético respeita a confidencialidade de qualquer informação ou dados sensíveis que possam ser encontrados durante o processo de teste. Eles não divulgam nem usam as informações para ganho pessoal ou para prejudicar a organização.
  + Integridade: O hacker ético mantém o mais alto nível de integridade durante todo o engajamento. Eles não modificam, roubam ou destroem dados ou sistemas além do necessário para demonstrar vulnerabilidades e riscos potenciais.
  + Conformidade: O hacker ético cumpre todas as leis e regulamentações aplicáveis, garantindo que suas ações não violem quaisquer limites legais ou éticos.
  + Relatório: o hacker ético fornece relatórios detalhados e precisos à organização, delineando as vulnerabilidades descobertas e recomendações para remediação. Eles comunicam suas descobertas de maneira responsável, garantindo que as informações sejam compartilhadas com segurança e somente com individuos autorizados.
* Ao aderir a esses princípios éticos, o hacker ético profissional ajuda as organizações a melhorar sua postura de segurança, identificando fraquezas antes que atores mal-intencionados possam explorá-las.
* Seu trabalho, em última análise, aprimora as defesas de cibersegurança da organização e as protege contra ameaças potenciais, garantindo a privacidade e a integridade de informações sensíveis.

Conceito de Hacking Ético

O que é hacking ético

* Hacking ético é o processo de tentativas autorizadas de obter acesso não autorizado a um sistema de computador, aplicativo ou dados.
* Hackers éticos são responsáveis por testar sistemas e identificar vulnerabilidades que poderiam ser exploradas por hackers maliciosos.
* Eles usam as mesmas ferramentas e técnicas que os hackers maliciosos, mas param antes de realmente realizar um ataque.
* Em vez disso, eles relatam quaisquer vulnerabilidades ou preocupações e buscam contramedidas para reforçar as defesas do sistema.

O que é um hacker ético

* Um profissional que domina o conhecimento técnico usado em ataques a sistemas de tecnologia da informação, mas que o utiliza para encontrar e corrigir vulnerabilidades de segurança, com o consentimento de uma empresa ou do proprietário da aplicação / dispositivo de computação.
* Hackers éticos são profissionais vitais no mundo atual, pois ajudam a desenvolver novas formas de combater as ameaças cibernéticas e são a principal linha de defesa contra spam, phishing, malware, vírus e outras ameaças à cibersegurança.

Atuação de um hacker ético

* O papel de um hacker ético é importante dentro da indústria de cibersegurança. Hackers éticos são responsáveis por proteger a infraestrutura de TI, os dispositivos de borda, as redes e os dados.
* Eles são especialistas em corrigir ameaças e as vulnerabilidades potenciais de um sistema.

Como se tornar um hacker ético

Habilidades de um hacker ético

* Para se tornar um hacker ético, é preciso ter conhecimentos avançados em:
  + Sistemas de segurança de computação e internet;
  + Habilidades de alto nível de hacking;
  + Capacidade de criar relatórios claros e concisos.
* Um hacker ético profissional é capaz de identificar rapidamente as falhas de segurança e fornecer conselhos úteis sobre como melhorar o sistema.
* Hackers éticos devem ser capazes de encontrar os métodos de ataque para acessar conteúdos sensíveis de uma organização.
* Eles devem ser capazes de invadir sistemas e devem estar bem familiarizados com as ameaças e vulnerabilidades potenciais que podem ocorrer nos sistemas organizacionais.
* Eles devem estar sempre acompanhando atualizações e novidades no campo da computação e segurança.
* Como em qualquer profissão, a paixão pela tecnologia é um dos aspectos-chave do sucesso. Isso, combinado com um sólido conhecimento de redes e programação, ajudará um profissional a ter sucesso na área de cibersegurança.
* Para se tornar um hacker ético, é necessário ter uma combinação de habilidades técnicas e não técnicas (hard skills e soft skills). Algumas das habilidades técnicas são:
  + Domínio dos conceitos de informática;
  + Habilidades em programação;
  + Habilidades de banco de dados (SQL);
  + Conhecimento avançado em Linux;
  + Conceitos e técnicas de Criptografia;
  + Habilidades de engenharia social;
  + Arquitetura e funcionamento de aplicações web;
  + Habilidades de rede de computadores;
  + Proficiência em sistemas operacionais.
* As habilidades não técnicas incluem comunicação, solução de problemas, criatividade, habilidades analíticas e paixão por tecnologia.

Atividades de um hacker ético

Atividades de um hacker ético

* Os hackers éticos, também conhecidos como hackers de chapéu branco, são profissionais que usam suas habilidades e conhecimentos de hackers para identificar e solucionar vulnerabilidades em sistemas e redes de computadores.
* A seguir, alguns exemplos de atividades que estes profissionais exercem.
  + Teste de penetração
    - Hackers éticos realizam testes de penetração, que envolvem a tentativa de explorar vulnerabilidades em um sistema ou rede para identificar possíveis pontos fracos e recomendar contramedidas. Isso ajuda as organizações a identificar e lidar com vulnerabilidades antes que possam ser exploradas por agentes mal-intencionados.
  + Teste de engenharia social
    - Os hackers éticos também podem testar as defesas de uma organização contra técnicas de engenharia social, como phishing ou golpes sociais, tentando induzir os funcionários a revelar informações confidenciais. Isso ajuda as organizações a identificar pontos fracos em seus programas de treinamento de conscientização de segurança e desenvolver estratégias para mitigar os riscos de engenharia social.
  + Avaliação de vulnerabilidade
    - Hackers éticos realizam avaliações de vulnerabilidade para identificar possíveis pontos fracos nos sistemas e redes de uma organização. Isso envolve a verificação de portas abertas, o estudo das vulnerabilidades de cada porta e a recomendação de ações corretivas. O objetivo é identificar possíveis pontos fracos que possam ser explorados por agentes mal-intencionados.
  + Avaliação de risco
    - Hackers éticos realizam avaliações de risco para identificar riscos potenciais aos sistemas e redes de uma organização e recomendar contramedidas. Isso envolve a análise da probabilidade e o impacto de diferentes tipos de ameaças cibernéticas e o desenvolvimento de estratégias para mitigar esses riscos.
  + Auditoria de segurança
    - Hackers éticos realizam auditoria de segurança para avaliar a postura geral de segurança de uma organização. Isso envolve revisar as políticas e procedimentos de segurança, testar os controles de segurança e fazer recomendações para melhorias.
  + Pesquisa de segurança
    - Hackers éticos se envolvem em pesquisas de segurança para identificar novas vulnerabilidades e desenvolver novas ferramentas e técnicas para identificar e lidar com ameaças cibernéticas. Isso ajuda a manter as organizações à frente das ameaças cibernéticas emergentes.

Melhoria contínua

* O ciclo PDCA é um método para melhoria contínua de processos e produtos. Ele significa Planejar, Executar, Verificar, Agir. Em termos de cibersegurança, pode ajudar a estabelecer e manter uma segurança efetiva das informações seguindo alguns passos.
  + Planejar
    - Identificar um problema ou objetivo relacionado com a cibersegurança, como criar consciencialização entre equipe, implementar uma nova política de segurança, ou evitar o roubo de dados. Definir os recursos, ações e indicadores que tornarão o seu plano bem-sucedido.
  + Executar
    - Colocar em prática o seu plano e monitorar os indicadores. Esteja preparado para enfrentar alguns desafios ou problemas inesperados ao longo do caminho. Se possível, teste o seu plano em pequena escala antes de aplicá-lo a toda a organização.
  + Verificar
    - Avaliar os resultados e dados do seu plano. Compará-los com os resultados esperados e ver se há lacunas ou discrepâncias. Identificar as causas raiz de quaisquer problemas e aprender com os erros.
  + Agir
    - Com base na sua avaliação, decidir se precisa ajustar o plano ou implementá-lo como está. Se precisar fazer alterações, volte à fase de planejamento e repita o ciclo. Se estiver satisfeito com os seus resultados, padronize o seu plano e comunique-o aos seus stakeholders.

Conclusão

* A ética é um dos maiores requisitos para se tornar um profissional de cibersegurança, pois envolve lidar com informações sensíveis das empresas e dos usuários, bem como prevenir e combater crimes cibernéticos. Um hacker ético deve agir de forma responsável e legal, respeitando as normas e os direitos dos outros, e utilizando seus conhecimentos para proteger e melhorar a segurança cibernética.
* As principais habilidades de um hacker ético são
  + conhecimentos técnicos sobre sistemas operacionais,
  + redes,
  + protocolos,
  + aplicações,
  + vulnerabilidades e ferramentas de segurança;
  + ter capacidade de análise,
  + raciocínio lógico,
  + criatividade e persistência para encontrar e explorar falhas;
  + ter habilidades de comunicação, escrita concisa e reporte para apresentar os resultados dos testes de invasão e as recomendações de mitigação;
  + e ter atitude proativa, curiosa e colaborativa para aprender constantemente e compartilhar conhecimentos.
* A importância de se manter atualizado sobre conceitos de segurança cibernética se deve ao fato de que as ameaças e os riscos são dinâmicos e evoluem rapidamente, exigindo dos profissionais uma adaptação constante às novas tecnologias, regulamentações e cenários.
* Além disso, a cibersegurança é uma área multidisciplinar que envolve aspectos técnicos, jurídicos, sociais e éticos, que devem ser considerados na hora de criar soluções inteligentes e eficazes para ambientes cada vez mais conectados.

## Aula 3 - Profissões em cibersegurança

Red Team

Red Team (Equipe Vermelha) - O que é

* Os profissionais de Cibersegurança Red Team atuam com simulações de ataques cibernéticos contra empresas e organizações, com o objetivo de identificar e eliminar vulnerabilidades nos sistemas de defesa.
* Esse profissional precisa ter um alto conhecimento sobre as principais ameaças e técnicas de invasão existentes e atuais, e ser capaz de usar ferramentas e metodologias de hackers éticos.
* O principal objetivo de um profissional Red Team, é melhorar a segurança cibernética das empresas, demonstrando os impactos de ataques bem-sucedidos e o que funciona para os defensores (ou seja, a equipe azul – Blue Team) em um ambiente operacional.

Red Team - Atividades

* O trabalho do Red Team pode ser dividido em quatro etapas principais:
  + Planejamento,
  + Execução,
  + Análise,
  + Recomendação.
* Planejamento
  + O Red Team define o escopo, os objetivos, as regras e os limites do teste de ciberataque. Eles devem levar em conta as características da empresa, os sistemas envolvidos, os riscos associados, e as expectativas dos contratantes.
  + O planejamento também envolve a coleta de informações sobre o alvo, como endereços IP, domínios, portas abertas, serviços rodando, vulnerabilidades conhecidas, entre outros. Esses dados são usados para mapear a superfície de ataque e escolher as melhores estratégias para explorá-las.
* Execução
  + O Red Team coloca em prática as ações planejadas para tentar invadir os sistemas da empresa. Eles podem usar diferentes métodos de ataque, como phishing, brute force, SQL injection, cross-site scripting, entre outros.
  + O Red Team também pode usar técnicas de engenharia social para enganar ou persuadir os funcionários da empresa a fornecerem informações ou acessos privilegiados. Por exemplo, eles podem se passar por clientes, fornecedores ou colegas de trabalho para enviar e- mails maliciosos ou fazer ligações falsas.
  + O Red Team deve documentar todas as suas atividades durante a execução do teste, registrando as evidências das vulnerabilidades encontradas, os impactos causados e as dificuldades enfrentadas.
* Análise
  + O Red Team analisa os resultados obtidos durante a execução do teste. Eles devem verificar se conseguiram atingir os objetivos definidos no planejamento, quais foram as falhas mais críticas e frequentes nos sistemas de defesa da empresa, e quais foram as lições aprendidas com a experiência.
  + A análise também envolve a classificação das vulnerabilidades encontradas de acordo com o seu nível de gravidade, probabilidade e urgência. Assim, eles podem priorizar as correções mais importantes e efetivas.
* Recomendação
  + O Red Team elabora um relatório detalhado com as conclusões da análise. O relatório deve conter uma descrição clara e objetiva das vulnerabilidades encontradas, as evidências coletadas, os impactos gerados e as recomendações para mitigá-las.
  + O relatório deve ser apresentado aos contratantes do teste de ciberataque, que podem ser gestores ou responsáveis pela segurança da informação na empresa. O Red Team deve explicar os resultados obtidos e esclarecer as dúvidas que possam surgir.
  + O relatório também deve servir como base para a implementação das correções sugeridas pelo Red Team. Essas correções podem envolver desde a atualização de softwares e sistemas operacionais até a mudança de políticas e procedimentos internos.

Red Team - Habilidades

* Para se tornar um profissional de Cibersegurança que atua como Red Team, é preciso ter algumas habilidades e certificações específicas. Entre elas, podemos destacar:
  + Conhecimento avançado sobre redes, sistemas operacionais, protocolos, serviços e ferramentas de segurança;
  + Conhecimento sobre as principais técnicas de ataque e invasão cibernética, como exploração de vulnerabilidades, injeção de código, spoofing, sniffing, entre outras;
  + Conhecimento sobre as principais técnicas de engenharia social, como phishing, vishing, baiting, entre outras;
  + Capacidade de planejar, executar, analisar e reportar testes de ciberataque de forma eficiente e ética;
  + Capacidade de se comunicar de forma clara e objetiva com os contratantes e os demais membros da equipe;
  + Capacidade de trabalhar em equipe e colaborar com outros profissionais da área;
  + Capacidade de se atualizar constantemente sobre as novidades e ameaças do cenário cibernético.

Red Team - Desafios e benefícios

* O trabalho do Red Team é desafiador por vários motivos.
  + Primeiro, porque exige um alto nível de conhecimento técnico sobre as diversas formas de ataque cibernético existentes.
  + Segundo, porque exige uma capacidade de adaptação e criatividade para lidar com as diferentes situações que podem surgir durante o teste.
  + Terceiro, porque exige uma ética profissional e um compromisso com a confidencialidade dos dados e informações acessados.
* Por outro lado, o trabalho do Red Team também traz muitos benefícios.
  + Primeiro, porque contribui para a melhoria contínua da segurança da informação na empresa, reduzindo os riscos de ataques reais e seus prejuízos.
  + Segundo, porque proporciona um aprendizado constante sobre as novas tendências e tecnologias do mercado de cibersegurança.
  + Terceiro, porque oferece uma oportunidade de crescimento profissional e reconhecimento na área.

Blue Team

Blue Team (Equipe Azul) - O que é

* Um profissional de cibersegurança da equipe azul é um especialista em segurança responsável por defender os sistemas de informação de uma organização e garantir sua segurança contra possíveis ameaças cibernéticas.
* Eles concentram-se em manter e melhorar a postura de segurança da organização, identificando falhas de segurança, verificando a eficácia das medidas de segurança e garantindo que essas medidas permaneçam eficazes após a implementação.
* Eles usam seus conhecimentos e habilidades para fins legítimos e benéficos.
* O objetivo do Blue Team é fortalecer as barreiras e os mecanismos de proteção da empresa, e reagir rapidamente aos incidentes de segurança que possam ocorrer.
* Assim, eles ajudam a garantir a confidencialidade, a integridade e a disponibilidade das informações, e evitar os prejuízos causados por ataques cibernéticos.

Blue Team - Atividades

* Monitoramento
  + Blue Team acompanha constantemente o funcionamento dos sistemas e das redes da empresa, verificando se há algum sinal de anomalia ou intrusão.
  + Eles usam ferramentas como firewalls, antivírus, IDS (Intrusion Detection System ou Sistema de Detecção de Intrusão), IPS (Intrusion Prevention System ou Sistema de Prevenção de Intrusão), entre outras.
  + O monitoramento também envolve a coleta e a análise de dados sobre o tráfego e o comportamento dos usuários na rede, como endereços IP, portas abertas, serviços rodando, logs de acesso, entre outros.
  + Esses dados são usados para identificar padrões normais e anormais de atividade, e alertar sobre possíveis ataques.
* Detecção
  + Blue Team verifica se há alguma evidência de ataque cibernético em andamento ou concluído.
  + Eles usam técnicas como análise forense, engenharia reversa, análise de malware, entre outras.
  + O Blue Team deve validar se os alertas recebidos são verdadeiros ou falsos positivos, e classificar os ataques de acordo com o seu nível de gravidade, probabilidade e urgência.
  + Assim, eles podem priorizar as respostas mais adequadas e eficazes.
* Resposta
  + Blue Team executa as ações necessárias para conter e neutralizar os ataques cibernéticos detectados.
  + Eles usam ferramentas como isolamento de rede, bloqueio de acesso, remoção de malware, restauração de backup, entre outras.
  + O Blue Team deve documentar todas as suas atividades durante a resposta ao incidente, registrando as evidências dos ataques sofridos, os impactos causados e as soluções aplicadas.
* Mitigação
  + Blue Team analisa os resultados obtidos durante a resposta ao incidente.
  + Eles devem verificar se conseguiram eliminar ou minimizar os danos causados pelos ataques cibernéticos, quais foram as falhas mais críticas e frequentes nos sistemas de defesa da empresa, e quais foram as lições aprendidas com a experiência.
  + A mitigação também envolve a implementação das correções sugeridas pelo Blue Team. Essas correções podem envolver desde a atualização de softwares e sistemas operacionais até a mudança de políticas e procedimentos internos.

Blue Team - Habilidades

* Conhecimento avançado sobre redes, sistemas operacionais, protocolos, serviços e ferramentas de segurança.
* Conhecimento sobre as principais técnicas de defesa e prevenção cibernética, como firewall, antivírus, criptografia, backup, entre outras.
* Conhecimento sobre as principais técnicas de resposta e mitigação cibernética, como análise forense, engenharia reversa, análise de malware, entre outras.
* Capacidade de monitorar, detectar, responder e mitigar ameaças virtuais de forma eficiente e ética.
* Capacidade de se comunicar de forma clara e objetiva com os contratantes e os demais membros da equipe.
* Capacidade de trabalhar em equipe e colaborar com outros profissionais da área.
* Capacidade de se atualizar constantemente sobre as novidades e ameaças do cenário cibernético.

Blue Team - Desafios e Benefícios

* O trabalho do Blue Team é desafiador por vários motivos.
  + Primeiro, porque exige um alto nível de conhecimento técnico sobre as diversas formas de defesa e prevenção cibernética existentes.
  + Segundo, porque exige uma capacidade de reação rápida e eficiente diante dos ataques cibernéticos que possam ocorrer.
  + Terceiro, porque exige uma ética profissional e um compromisso com a confidencialidade dos dados e informações protegidos.
* Por outro lado, o trabalho do Blue Team também traz muitos benefícios.
  + Primeiro, porque contribui para a manutenção da segurança da informação na empresa, garantindo a confiança e a reputação do negócio.
  + Segundo, porque proporciona um aprendizado constante sobre as novas tendências e tecnologias do mercado de cibersegurança.
  + Terceiro, porque oferece uma oportunidade de crescimento profissional e reconhecimento na área.

Forense

Forense Cibernético - O que é

* Um profissional de cibersegurança forense, também conhecido como analista de forense digital ou analista forense de computador, é um especialista que analisa evidências digitais e investiga incidentes de segurança cibernética para extrair informações úteis em apoio à mitigação de vulnerabilidades de sistemas e redes.
* O objetivo do Forense Digital é identificar e rastrear os autores e as vítimas desses crimes ou incidentes, coletando evidências que possam ser usadas em processos judiciais ou administrativos.
* Assim, o Forense Digital contribui para a aplicação da lei e da justiça no âmbito digital.
* O Forense Digital é uma ciência que aplica métodos científicos para analisar dados e dispositivos digitais relacionados a crimes cibernéticos ou incidentes de segurança.
* Esses crimes podem envolver desde fraudes, extorsões, invasões, sabotagens, espionagens, até violações de direitos autorais, pornografia infantil, cyberbullying, entre outros.

Forense Cibernético - Atividades

* Coleta: o Forense Digital realiza a busca e a apreensão dos dados e dispositivos digitais que possam estar relacionados ao crime ou incidente investigado.
  + Esses dados e dispositivos podem estar em diferentes locais, como computadores, celulares, tablets, pendrives, cartões de memória, servidores, nuvens, redes sociais, entre outros.
  + O Forense Digital deve seguir os protocolos legais para realizar a coleta dos dados e dispositivos digitais, respeitando os direitos e as garantias dos envolvidos.
  + Além disso, o Forense Digital deve documentar todas as suas ações durante a coleta, registrando as informações sobre os locais, as datas, as horas, as pessoas, os equipamentos e os procedimentos utilizados.
* Preservação: o Forense Digital realiza a proteção dos dados e dispositivos digitais coletados contra alterações ou perdas acidentais ou intencionais.
  + Essa proteção é essencial para garantir a integridade e a autenticidade das evidências digitais.
  + O Forense Digital deve usar técnicas como selagem física (proteger fisicamente os ativos de tecnologia da informação), etiquetagem digital, criptografia, hash ou checksum para preservar os dados e dispositivos digitais coletados.
  + Além disso, o Forense Digital deve armazenar os dados e dispositivos digitais coletados em locais seguros e controlados.
* Análise: o Forense Digital realiza a extração e a interpretação dos dados e dispositivos digitais preservados.
  + Essa extração e interpretação visa encontrar as evidências que possam esclarecer o que aconteceu, quando aconteceu, como aconteceu, quem fez e quem foi afetado pelo crime ou incidente investigado.
  + O Forense Digital deve usar técnicas como duplicação de imagem forense, recuperação de dados apagados, análise de arquivos, análise de logs, análise de rede, análise de malware, entre outras.
  + Além disso, o Forense Digital deve usar ferramentas confiáveis e validadas para realizar a análise dos dados e dispositivos digitais preservados.
* Apresentação: o Forense Digital realiza a comunicação e a divulgação dos resultados da análise dos dados e dispositivos digitais preservados.
  + Essa comunicação e divulgação visa fornecer as evidências e as conclusões que possam auxiliar na tomada de decisão dos responsáveis pelo caso.
  + O Forense Digital deve elaborar um relatório técnico que contenha as informações sobre o caso, os métodos e as ferramentas utilizados, as evidências e as conclusões encontradas.
  + Além disso, o Forense Digital deve estar preparado para apresentar e defender o seu relatório perante os órgãos competentes, como juízes, promotores, advogados ou gestores.

Forense Cibernético - Habilidades

* Para se tornar um profissional de Cibersegurança que atua como Forense Digital, é preciso ter algumas habilidades e certificações específicas. Entre elas, podemos destacar:
  + Conhecimento avançado sobre sistemas operacionais, redes, protocolos, serviços e ferramentas digitais;
  + Conhecimento sobre as principais técnicas e ferramentas de análise forense digital, como duplicação de imagem forense, recuperação de dados apagados, análise de arquivos, análise de logs, análise de rede, análise de malware, entre outras;
  + Capacidade de coletar, preservar, analisar e apresentar evidências digitais de forma válida e confiável;
  + Capacidade de se comunicar de forma clara e objetiva com os contratantes e os demais envolvidos no caso;
  + Capacidade de trabalhar em equipe e colaborar com outros profissionais da área;
  + Capacidade de se atualizar constantemente sobre as novidades e ameaças do cenário digital.

Forense Cibernético - Desafios e Benefícios

* O trabalho do Forense Digital é desafiador por vários motivos.
  + Primeiro, porque exige um alto nível de conhecimento técnico sobre as diversas tecnologias e ferramentas envolvidas no cenário digital.
  + Segundo, porque exige uma capacidade de raciocínio lógico e analítico para solucionar problemas complexos e dinâmicos.
  + Terceiro, porque exige uma ética profissional e um compromisso com a verdade e a justiça.
* Por outro lado, o trabalho do Forense Digital também traz muitos benefícios.
  + Primeiro, porque contribui para a elucidação de crimes cibernéticos ou incidentes de segurança que afetam milhares de pessoas e organizações.
  + Segundo, porque proporciona um aprendizado constante sobre as novas tendências e ameaças do mundo digital.
  + Terceiro, porque oferece uma oportunidade de crescimento profissional e reconhecimento na área.

GRC - Governança, Risco e Conformidade

GRC Cibernético - O que é

* Governança, Risco e Conformidade (GRC), é um conjunto de conceitos que visa integrar e otimizar os processos de cibersegurança nas empresas.
* O objetivo é assegurar que as empresas estejam protegidas contra ataques cibernéticos, em conformidade com as normas e os regulamentos de cibersegurança, e alinhadas com as suas metas e valores.
* O papel do profissional de Cibersegurança que atua como GRC é coordenar e supervisionar esses processos, garantindo que eles sejam eficientes, eficazes e transparentes.
* Os profissionais de GRC trabalham em estreita colaboração com as equipes de TI e segurança para criar uma estratégia abrangente de cibersegurança que esteja alinhada aos objetivos de negócios, gerenciando efetivamente os riscos cibernéticos e atendendo aos requisitos regulatórios.

GRC - Atividades

* Na área de governança, o GRC é responsável por definir e implementar as políticas, os procedimentos, os papéis e as responsabilidades relacionados à cibersegurança na empresa.
* Ele também deve estabelecer e monitorar os indicadores de desempenho e qualidade da cibersegurança, bem como comunicar e reportar os resultados aos stakeholders internos e externos.
* O objetivo da governança é garantir que a cibersegurança esteja alinhada com a estratégia, a cultura e a missão da empresa, bem como com as expectativas dos clientes, dos parceiros e da sociedade.
* Na área de risco, o GRC é responsável por identificar, avaliar, tratar e monitorar os riscos relacionados à cibersegurança na empresa.
  + Ele também deve desenvolver e implementar planos de contingência e recuperação em caso de incidentes ou crises de cibersegurança.
  + O objetivo do risco é garantir que a empresa esteja preparada para enfrentar as ameaças virtuais, minimizando os impactos negativos sobre a sua reputação, a sua operação e o seu resultado.
* Na área de conformidade, o GRC é responsável por verificar e garantir que a empresa esteja em conformidade com as leis, os regulamentos, as normas e os padrões de cibersegurança aplicáveis ao seu setor ou mercado.
  + Ele também deve realizar auditorias internas e externas para avaliar a eficácia dos controles de segurança implementados na empresa.
  + O objetivo da conformidade é garantir que a empresa esteja protegida contra sanções legais ou regulatórias, bem como contra perdas financeiras ou processuais decorrentes de violações ou falhas na cibersegurança.

GRC - Habilidades

* Para se tornar um profissional de Cibersegurança que atua como GRC, é preciso ter algumas habilidades e certificações específicas.
* Entre elas, podemos destacar:
  + Conhecimento avançado sobre as leis, os regulamentos, as normas e os padrões de cibersegurança aplicáveis ao setor ou mercado da empresa;
  + Conhecimento sobre as melhores práticas e metodologias de governança, risco e conformidade em cibersegurança;
  + Capacidade de definir e implementar políticas, procedimentos, papéis e responsabilidades em cibersegurança na empresa;
  + Capacidade de identificar, avaliar, tratar e monitorar os riscos em cibersegurança na empresa;
  + Capacidade de verificar e garantir a conformidade da empresa com as leis e os regulamentos de cibersegurança;
  + Capacidade de estabelecer e monitorar os indicadores de desempenho e qualidade da cibersegurança na empresa;
  + Capacidade de comunicar e reportar os resultados da cibersegurança aos stakeholders internos e externos da empresa;
  + Capacidade de realizar auditorias internas e externas em cibersegurança na empresa;
  + Capacidade de desenvolver e implementar planos de contingência e recuperação em caso de incidentes ou crises de cibersegurança na empresa;
  + Capacidade de trabalhar em equipe e colaborar com outros profissionais da área.

GRC - Desafios e Benefícios

* O trabalho do GRC é desafiador por vários motivos.
  + Primeiro, porque exige um alto nível de conhecimento sobre as diversas leis, regulamentos, normas e padrões de cibersegurança que afetam a empresa.
  + Segundo, porque exige uma capacidade de gerenciar e coordenar múltiplos processos e projetos de cibersegurança, envolvendo diferentes áreas e pessoas da empresa.
  + Terceiro, porque exige uma habilidade de se comunicar e negociar com os diversos stakeholders internos e externos da empresa, como clientes, fornecedores, auditores, reguladores, entre outros.
* Por outro lado, o trabalho do GRC também traz muitos benefícios.
  + Primeiro, porque contribui para a proteção da empresa contra ataques cibernéticos, que podem causar danos irreparáveis à sua imagem, à sua operação e ao seu resultado.
  + Segundo, porque contribui para a conformidade da empresa com as leis e os regulamentos de cibersegurança, que podem evitar sanções legais ou regulatórias, bem como perdas financeiras ou processuais.
  + Terceiro, porque contribui para o alinhamento da cibersegurança com a estratégia e a cultura da empresa, que podem aumentar a sua competitividade e o seu valor no mercado.

DevSecOps

DevSecOps - O que é

* DevSecOps é uma abreviação de Development, Security e Operations, ou seja, Desenvolvimento, Segurança e Operações.
* Esse termo representa uma evolução do DevOps, que é uma abordagem para o desenvolvimento de software que visa integrar e agilizar os processos entre as equipes de desenvolvimento e operações.
* O DevSecOps acrescenta a segurança como um elemento essencial nessa integração e agilização, automatizando a incorporação da segurança em todas as fases do ciclo de vida de desenvolvimento de software.
* O objetivo é garantir que o software seja desenvolvido com qualidade, segurança e eficiência, reduzindo os riscos de ataques cibernéticos ou falhas na entrega.
* O papel do profissional de Cibersegurança que atua como DevSecOps é coordenar e executar as atividades de segurança em conjunto com as equipes de desenvolvimento e operações, garantindo que elas sejam realizadas de forma contínua, colaborativa e transparente.

DevSecOps - Atividades

* Na área de desenvolvimento, o DevSecOps é responsável por aplicar as práticas e os princípios de desenvolvimento ágil e contínuo, como Scrum, Kanban, Lean, entre outros.
  + Ele também deve usar as ferramentas e os frameworks adequados para cada projeto, como Java, Python, Ruby on Rails, entre outros.
  + O objetivo do desenvolvimento é criar softwares que atendam às necessidades e às expectativas dos clientes, com qualidade, funcionalidade e usabilidade.
* Na área de segurança, o DevSecOps é responsável por aplicar as práticas e os princípios de segurança por design e por padrão, como OWASP Top 10, SANS Top 25, entre outros.
  + Ele também deve usar as ferramentas e os métodos adequados para cada projeto, como análise estática ou dinâmica de código, teste de penetração ou vulnerabilidade, entre outros.
  + O objetivo da segurança é proteger os softwares contra ameaças cibernéticas ou falhas internas, com qualidade, confidencialidade e integridade.
* Na área de operações, o DevSecOps é responsável por aplicar as práticas e os princípios de operações ágeis e contínuas, como integração contínua, entrega contínua, infraestrutura como código, entre outros.
  + Ele também deve usar as ferramentas e os serviços adequados para cada projeto, como Docker, Kubernetes, AWS, Azure, entre outros.
  + O objetivo das operações é implantar e manter os softwares em ambientes de produção ou de teste, com eficiência, disponibilidade e escalabilidade.

DevSecOps - Habilidades

* Para se tornar um profissional de Cibersegurança que atua como DevSecOps, é preciso ter algumas habilidades e certificações específicas. Podemos destacar:
  + Conhecimento avançado sobre as técnicas e as ferramentas de desenvolvimento ágil e contínuo;
  + Conhecimento avançado sobre as técnicas e as ferramentas de segurança por design e por padrão;
  + Conhecimento avançado sobre as técnicas e as ferramentas de operações ágeis e contínuas;
  + Capacidade de integrar e automatizar as técnicas e as ferramentas de desenvolvimento, segurança e operações em um fluxo de trabalho contínuo e colaborativo;
  + Capacidade de se adaptar às mudanças constantes nas demandas dos clientes e nas ameaças cibernéticas;
  + Capacidade de se comunicar e trabalhar em equipe com outros profissionais da área.

DevSecOps

* O trabalho do DevSecOps é desafiador por vários motivos.
  + Primeiro, porque exige um alto nível de conhecimento sobre as diversas técnicas e ferramentas de desenvolvimento, segurança e operações.
  + Segundo, porque exige uma capacidade de integrar e automatizar essas técnicas e ferramentas em um fluxo de trabalho contínuo e colaborativo.
  + Terceiro, porque exige uma habilidade de se adaptar às mudanças constantes nas demandas dos clientes e nas ameaças cibernéticas.
* Por outro lado, o trabalho do DevSecOps também traz muitos benefícios.
  + Primeiro, porque contribui para o desenvolvimento de softwares mais seguros e mais rápidos, que podem atender às necessidades e às expectativas dos clientes com mais qualidade e eficiência.
  + Segundo, porque contribui para a redução dos riscos de ataques cibernéticos ou falhas na entrega, que podem causar danos à reputação, à operação e ao resultado da empresa.
  + Terceiro, porque contribui para o aumento da produtividade e da satisfação das equipes de desenvolvimento, segurança e operações.

Conclusão

* Red Team: são os profissionais que simulam ataques cibernéticos contra os sistemas e as redes da empresa, com o objetivo de identificar e explorar as vulnerabilidades existentes.
  + Eles usam as mesmas ferramentas e técnicas que os hackers maliciosos usariam, e reportam os resultados e as recomendações para a equipe de defesa.
  + O papel do Red Team é testar e avaliar a segurança da informação da empresa, e ajudar a prevenir ataques reais.
* Blue Team: são os profissionais que se dedicam a defender os sistemas e as redes da empresa contra os ataques cibernéticos, sejam eles simulados ou reais.
  + Eles usam ferramentas e técnicas de segurança defensiva, como firewall, antivírus, criptografia, backup, entre outras.
  + Eles monitoram, detectam, respondem e mitigam as ameaças virtuais, e fortalecem os mecanismos de proteção da empresa.
  + O papel do Blue Team é manter e melhorar a segurança da informação da empresa, e garantir a confiança e a reputação do negócio.
* DevSecOps: são os profissionais que integram as práticas de segurança da informação no processo de desenvolvimento de software.
  + Eles usam ferramentas e técnicas de automação, integração contínua, entrega contínua, monitoramento e feedback.
  + Eles colaboram com as equipes de desenvolvimento (Dev), operações (Ops) e segurança (Sec) para garantir que o software seja seguro desde o início até o fim do ciclo de vida.
  + O papel do DevSecOps é acelerar e otimizar o desenvolvimento de software seguro, e reduzir os riscos de falhas e vulnerabilidades.
* Forense Digital: são os profissionais que coletam, preservam, analisam e apresentam evidências digitais relacionadas a crimes cibernéticos ou incidentes de segurança.
  + Eles usam ferramentas e técnicas de análise forense, engenharia reversa, análise de malware, entre outras.
  + Eles podem atuar em diferentes contextos, como investigações policiais, judiciais ou corporativas.
  + O papel do Forense Digital é identificar e rastrear os autores e as vítimas dos crimes cibernéticos ou incidentes de segurança, e auxiliar na aplicação da lei e da justiça.
* GRC: são os profissionais que gerenciam os processos de governança, risco e conformidade (GRC) relacionados à cibersegurança nas empresas.
  + Eles usam ferramentas e técnicas de gestão de projetos, auditoria interna, análise de risco, controle interno, entre outras.
  + Eles alinham as estratégias de cibersegurança com os objetivos do negócio, as normas regulatórias e as boas práticas do mercado.
  + O papel do GRC digital é garantir que a empresa esteja em conformidade com as leis e os padrões de cibersegurança, e gerenciar os riscos associados à cibersegurança.

## Aula 4 - Conceitos Iniciais

Vírus

* Um vírus de computador é um software malicioso que pode ser projetado de diversas maneiras em um computador ou rede e se replica entre sistemas e arquivos, causando danos que podem afetar o funcionamento do computador ou o roubo de dados sigilosos de uma pessoa física ou empresa.
* Conceito
  + Os vírus podem se espalhar em um computador através de várias maneiras, como em anexos e e-mails falsos, downloads da internet ou em dispositivos removíveis. Existem, também, uma série de vírus que apresentam diferentes características e danos.

Tipos de Vírus

* Vírus de Arquivo
  + Anexa-se a arquivos executáveis e se espalha quando esses arquivos são executados
* Vírus de Macro
  + Explora macros em aplicativos como processadores de texto e planilhas para se espalhar.
* Vírus de Boot
  + Infecta a área de inicialização de um disco rígido, tornando-se ativo quando o computador é inicializado.
* Worms
  + Diferente de vírus, os worms não precisam se anexar a arquivos e podem se espalhar automaticamente pela rede.
* Trojans
  + Disfarçados como software legítimo, os cavalos de Troia enganam os usuários para que os executem, permitindo o acesso não autorizado ao sistema.

Termos e conceitos sobre ameaças cibernéticas

* A preocupação constante com a segurança de dados digitais é algo crucial para evitar transtornos envolvendo o ataque de hackers aos dispositivos eletrônicos.
* Devido a constante imersão online no trabalho e na vida pessoal, estamos constantemente expostos a diversas ameaças digitais, as quais evoluem na mesma velocidade que as medidas de segurança digital.
* Confira na lista abaixo algumas dessa ameaças que podem afetar a segurança e privacidade dos dados.
  + SPAM
  + Spyware
  + Worms
  + Phishing
  + Botnets
  + Ransomware

Caso um computador ou redes de computadores de uma empresa não apresente um sistema sólido de segurança, as portas ficam abertas para a entrada de vírus.

* Existem outros três tipos muito comuns que são combatidos constantemente: Botnet, Rootkit e o Cavalo de Troia.

Botnet

* É uma rede de computadores infectados por um malware que permite que um cibercriminoso controle-os remotamente.

Rootkit

* É um tipo de malware furtivo e perigoso que permite que cibercriminosos acessem o seu computador sem você saber.

Cavalo de Troia

* É um programa malicioso que se disfarça de algo legítimo ou desejável para enganar os usuários e induzi-los a instalá-lo no seu computador.

## Aula 5 - Como se proteger

Boas práticas de Cibersegurança

* Nós aprendemos até aqui que existem muitas brechas e lacunas que podem facilitar o acesso de hackers nos sistemas, através de vírus e outras técnicas de ataque. Para que essas ameaças digitais tenham pouco impacto no dia-a-dia é importante seguir algumas boas práticas que podem ser muito úteis para garantir nossa segurança digital.

Segurança

* A segurança de dados digitais abrange várias dimensões e é crucial para proteger diversos fatores, como: privacidade; integridade; disponibilidade e a reputação de nossos dados pessoais ou até mesmo os dados sensíveis de uma empresa.

Algumas estratégias de proteção de dados digitais são essenciais

* Senhas fortes
  + Usar senhas fortes e únicas. As senhas devem ser compostas por letras maiúsculas e minúsculas, números e símbolos, e ter no mínimo oito caracteres.
* Atualizações
  + Atualizar os sistemas e os aplicativos. As atualizações dos sistemas operacionais e dos aplicativos contêm correções de bugs e vulnerabilidades que podem ser exploradas por hackers.
* Antivírus
  + Instalar um antivírus. Um antivírus é um software que detecta e elimina programas maliciosos que podem infectar os dispositivos e comprometer os dados.

Como implementar?

* A etapa de implementação das boas práticas de segurança é outro ponto importante e sensível desse processo. É aqui que o usuário ou a empresa leva em conta os diversos fatores valiosos, e essas etapas precisam ser seguidas.
* Confira na lista abaixo algumas dessas etapas de implementação.
  + Avaliar o nível de exposição às ameaças digitais.
  + Escolher as medidas de proteção adequadas.
  + Implementar e monitorar as medidas de proteção escolhidas.

## Recapitulando

* Neste curso, você aprendeu o que são os hackers e quais os diferentes papeis que eles exercem, seja para realizar a proteção de dados de uma empresa, ou para fazer ataques e invasões a bancos de dados e sistemas.
* Aprendeu, também, o que significa Ética, como ela pode ser aplicada no dia-dia e o que são os hackers éticos e suas atividades em uma empresa.
* Além disso, conheceu algumas profissões relacionadas a cibersegurança, como a Red Team, a Blue Team e os analistas forenses digitais.
* Conheceu qual é o conceito de vírus e quais os principais tipos mais utilizados pelos cibercriminosos.
* Por fim, aprendeu as técnicas e boas práticas de segurança digital e como implementá-las no dia-a-dia para a proteção de dados.

# 

# Identificar Componentes de Hardware de Computador

Olá! Boas-vindas!

Você está iniciando o curso sobre Identificar Componentes de Hardware de Computadores.

Neste curso, você explorará grandezas computacionais e sistemas numéricos, compreendendo como a informação é representada e manipulada no contexto computacional.

Em seguida, mergulharemos na arquitetura de hardware, onde você entenderá como os componentes físicos de um computador trabalham em conjunto. Identificar os componentes de hardware do computador será o próximo passo, permitindo que você tome decisões informadas ao montar ou atualizar um computador.

Por fim, você aprenderá sobre a instalação de sistemas operacionais e a criação de ambientes virtuais através da virtualização.

Bons estudos!

## Aula 1 - Grandezas computacionais e sistema numéricos

O desenvolvimento da informática começa quando há a necessidade de desenvolvimento de máquinas que facilitem a resolução de cálculos complexos de forma rápida.

As grandezas computacionais são os diversos aspectos que caracterizam a capacidade e o desempenho dos sistemas de computadores. Através dessas grandezas é possível entender a eficiência e a eficácia de dispositivos, redes e algoritmos no universo da computação.

Além das grandezas de armazenamento, temos também grandezas de velocidade de transmissão principalmente usadas para definir velocidades de links de internet e cópia de arquivos.

Muito bem! Agora que você aprendeu sobre introdução às grandezas computacionais, velocidade de transmissão, bases numéricas e conversões e siga adiante para testar os seus conhecimentos.

Questionário

* Qual foi o principal motivo de criação do ENIAC?
  + Realizar Cálculos Balísticos
* Quantos bits compõem um byte em sistemas de computação?
  + 8
* Qual a principal unidade de medida para indicar a potência de uma fonte de alimentação de computador?
  + Watt

## Aula 2 - CPU, Placa-mãe, Memórias e BIOS/UEFI

Os computadores são formados por conjuntos de peças construídas e instaladas ao redor de um microprocessador. Esse componentes, que compõe o hardware, são responsáveis por diferentes funções que permitirão a execução de atividades diversas.

Rapidamente vamos conhecer os componentes de um computador:

* Processador
* Placa-Mãe
* Cooler
* Memória RAM
* HDD/SSD
* Fonte
* Placas Offboard

Placa mãe

A placa mãe é uma peça fundamental em uma máquina e é responsável por facilitar a comunicação entre os diferentes componentes de um computador. Ela é composta por diferentes partes que, em conjunto, trabalham na integração e coordenação de hardware, possibilitando o funcionamento harmonioso do sistema como um todo.

Memórias

A memória de um computador é responsável por armazenar os dados de um sistema. Além disso, ela tem papel crucial quanto a velocidade de utilização e troca de dados de um computador.

As memórias podem ser separadas em dois tipos:

Não Voláteis

* ROM (PROMs, EPROMs, EEPROMs, Memória flash)
* Armazenamento em massa (Pendrive, SSD, HD)

Voláteis

* RAM (SIMM, DIMM, SDR, DDR, DDR2, DDR3, DDR4, DDR5, etc)
* Cache (L1, L2, L3)
* Vídeo (GDDR3, GDDR4, GDDR5, GDDR6, HBM, HBM2)

Muito bem! Agora que você aprendeu os componentes do computador como CPU, memórias, placa-mae e BIOS (Basic Input Output System) e UEFI (Unified Extensible Firmware Interface), siga adiante para testar seus conhecimentos.

Questionário

* Quais são as principais arquiteturas de processador para computadores atualmente?
  + X64 (CISC) e ARM (RISC)
* Qual a função do Cooler de processador?
  + Resfriar o processador
* Quais sãos os principais tamanhos de placa-mãe?
  + ATX, mATX e ITX.

## Aula 3 - Armazenamento, Fonte, Placas Offboard e Gabinete

Para que o computador funcione precisamos de softwares como sistemas operacionais, e os dados gerados e utilizados por esses softwares são armazenados em dispositivos como:

* HDs (Hard Drives) – Discos Rígidos
* CDs / DVDs / Blu-rays – Mídias Óticas removíveis
* Pendrives / Cartões de Memória
* SSDs

Fonte

* Fonte é o componente que vai receber a energia da tomada e converter para tensão de funcionamento do computador. As fontes são projetadas para converter a energia em uma corrente contínua, responsável pelo funcionamento dos diferentes componentes de um computador.

Placas Offboard

* Atualmente muitos recursos como vídeo, som, rede com e sem fio e armazenamento estão integradas à placa-mãe e atendem grande parte dos usuários de computador, mas nem sempre o desempenho ou a capacidade desses recursos atendem determinados públicos. É ai que entram as placas offboard.

Gabinete

O gabinete, desktop ou case é o componente em hardware que protege e organiza o hardware do seu PC (Personal Computer)

Ele pode ter diversos formatos e tamanhos, mas existe uma classificação conforme tamanho da placa-mãe.

Tamanhos:

* Full Tower (placas mãe até E-ATX ou XL-ATX)
* Mid Tower (Até placas ATX)
* Mini Tower (placas até mATX ou ITX)

Muito bem! Agora que você aprendeu mais sobre Armazenamento, o que são Fontes, Placas Offboard e o Gabinete, siga adiante para testar seus conhecimentos.

Questionário

* Qual a velocidade média de um disco SATA SSD?
  + 500MB/s
* Quais são os tipos de conectores M.2?
  + M key (NVMe) e B + M Key (SATA)
* Em Fontes ATX, o cabo com pino 4+4 serve pra que?
  + Alimentação auxiliar do processador (CPU).

## Aula 4 - Instalação de SO

Após a montagem de uma máquina, o próximo passo é a instalação de um sistema operacional. Existem diversos sistemas e maneiras para realizar essa instalação, dependendo da complexidade e características dos componentes.

Questionário

* O que preciso para criar um pendrive bootável?
  + Pendrive de pelo menos 8GB, Programa (Rufus, Ventoy, etc.) e Imagem do SO desejado.
* Sobre a Particionamento do Disco no Windows, qual cuidado devo ter?
  + Verificar se o disco é o correto e se não há dados sem backup na partição.
* Na instalação do Ubuntu 23.10, o que acontece se eu escolher Experimentar Ubuntu?
  + Irá fechar a tela e deixará você utilizar o sistema pelo pendrive.

## Aula 5 - Virtualização

A virtualização é o uso de software para criar uma camada sobre o hardware que permite que os elementos do computador sejam divididos em vários computadores virtuais, chamados de VMs.

Questionário

* O que é uma máquina virtual?
  + É uma máquina gerada por software compartilhando recursos da máquina física, simulando um computador.
* Quais são as vantagens de se utilizar virtualização?
  + Menor consumo de energia, menor gasto com hardware e menos espaço em data centers
* Qual a diferença entre Virtualização Tipo 1 e Tipo 2?
  + A virtualização tipo 1 instala direto no hardware e virtualização tipo 2 instala no sistema operacional hospedeiro.

## Recapitulando

Neste curso, você aprendeu sobre os elementos de hardware e software. Você aprofundou seus conhecimentos sobre grandezas computacionais e bases numéricas, compreendeu a função e estrutura da CPU, placa-mãe, memórias e BIOS/UEFI. Ainda abordamos informações sobre armazenamento, fontes de alimentação, placas offboard e gabinetes.

Por fim, aprofundamos também nosso conhecimento sobre o processo de instalação de sistemas operacionais e a prática de virtualização. Este conhecimento será útil para entender como os programas como os programas interagem com o hardware e como otimizam o desempenho do seu computador.

# Compreender internet e camada de acesso a rede

## Aula 1 - O que é rede?

Para esse primeiro passo, entenderemos nos próximos vídeos o que é uma rede, qual a sua importância e por que ela é essencial para se tornar um hacker do bem.

Questionário

* Redes de computadores podem ser definidas como:
  + dois ou mais dispositivos interconectados, que podem trocar informações entre si.
* Assinale a alternativa que apresenta uma rede de computadores.
  + Internet.
* Para um profissional de segurança da informação, qual é a importância de compreender o funcionamento da rede de computadores?
  + Absolutamente essencial, pois o profissional de segurança da informação será responsável por manter a comunicação dessa rede segura.

## Aula 2 - História das redes

Agora que começamos a entender o que é essa rede, você deve estar curioso para entender como chegamos a ela. E é justamente a história por trás do surgimento da rede de computadores que veremos nos próximos vídeos, entendendo quais foram os motivos que levaram a sua criação e como ela foi evoluindo até hoje, com o acesso à internet.

Questionário

* Qual rede militar dos Estados Unidos foi a base tecnológica para a criação da internet como a conhecemos hoje?
  + Arpanet.
* A necessidade de criar uma rede descentralizada e que não dependesse de apenas um nó central foi motivada por qual evento geopolítico?
  + Guerra Fria
* Assinale a alternativa correta a respeito do contexto histórico das redes de computadores.
  + A internet moderna possibilitou que qualquer pessoa com um computador conectado a ela tivesse alcance global.

## Aula 3 - Tipo de redes

Depois de conhecer um pouco da história da rede de computadores desde os seus primórdios até os dias atuais, está na hora de entender o que são essas redes, seus diferentes tamanhos, tipos, objetivos etc. nos vídeos a seguir.

Questionário

* O tipo de rede que tem limitação geográfica de aproximadamente 100 metros, como uma casa ou um prédio, é conhecida como:
  + LAN - Local Área network
* Qual é a principal diferença entre redes wired e wireless?
  + Redes wired são interligadas por meio de cabeamentos enquanto redes wireless são interligadas sem a necessidade de cabos.
* Qual o nome da representação gráfica geralmente utilizada como parte da documentação de rede?
  + Topologia de rede

## Aula 4 - Padrões em comunicações de dados

Até esse ponto, já entendemos o que é uma rede, como ela surgiu e os seus principais tipos, mas agora precisamos compreender que uma rede de computadores tem como função garantir que exista uma troca de informação entre os dispositivos dessa rede, mas como essa informação é trocada e como que é possível que diferentes dispositivos, de diferentes marcar consigam “falar a mesma língua”, vamos descobrir nos vídeos a seguir.

Muito bem! Nessa aula, você aprendeu sobre os padrões em comunicações de dados. Agora, siga adiante para testar seus conhecimentos.

Questionário

* Assinale a alternativa que apresenta o objetivo de padronizações como os modelos OSI e TCP/IP dentro de redes de computadores.
  + Permitir que a comunicação dentro de uma rede de computadores possa ocorrer independentemente do fabricante dos dispositivos.
* Qual é a diferença entre os modelos OSI e TCP/IP?
  + O modelo OSI é uma estrutura conceitual de como os dispositivos de rede trocam informações enquanto o TCP/IP é também um protocolo de comunicação em uma rede.
* Por que é importante conhecer o modelo OSI mesmo que ele seja somente teórico?
  + Porque o modelo OSI pode ser utilizado como ferramenta de troubleshooting para resolver problemas que envolvam comunicação

## Aula 5 - Ativos de rede

Depois de entendermos a importância da padronização no modo que ocorre a comunicação dentro de uma rede de computadores, vamos aprender, nos próximos vídeos, quem faz parte dessa rede de computadores e como uma rede de computador é composta.

Questionário

* Qual dispositivo tem como principal função realizar o bloqueio de tráfego de rede e permitir somente os pacotes autorizados?
  + Firewall
* O roteador é um dispositivo que atua em qual camada do modelo OSI?
  + Camada 3 - Rede
* Qual dispositivo de rede deixou de ser utilizado por ser apenas um repetidor de sinais elétricos nas portas e gerar ruído desnecessário na rede?
  + Hub

## Aula 6 - Passivos de rede

Agora que sabemos mais sobre os principais dispositivos dessa rede, vamos entender por onde essa informação é propagada e descobrir as diferenças dos meios de comunicação. Esse conhecimento é essencial para um profissional de segurança da informação, pois cada meio tem suas características e vulnerabilidades.

Questionário

* Qual seria o meio mais suscetível a ruídos na comunicação, além da probabilidade maior de ter os dados interceptados, levando em consideração as características físicas do meio de comunicação?
  + Ar
* O cabo de fibra ótica transmite as informações por meio de:
  + Fótons (Luz)
* Assinale a alternativa que apresenta tecnologias de transmissão wireless.
  + Wi-fi, bluetooth e RFID.

## Recapitulando

Concluímos mais uma etapa do Hackers do Bem! Mas ainda temos um longo caminho pela frente. Este foi um módulo introdutório, no qual você aprendeu um conteúdo básico sobre redes de computadores. Nos próximos módulos, você terá um aprofundamento técnico em cada uma das camadas que compõem uma rede de computador, adquirindo um conhecimento essencial para se tornar um hacker do bem.

# Compreender acesso a rede e camada de internet (IP)

Nesta aula, você irá conhecer o que são camadas de acesso e como é o funcionamento da camada TCP/IP. Conhecerá, também, sobre o endereço MAC e tráfego de dados. Além disso, aprenderá sobre o Protocolo ARP e quais são as estruturas do IPV4.

Por fim, aprenderá as diferenças entre IP público, IP privado e NAT e o que são subredes e como configurá-las em um sistema de redes.

## Aula 1 - Camada de acesso

As camadas de acesso de dados são responsáveis por fornecer acesso simplificado aos dados armazenados em um computador. Essas camadas são projetadas para organizar e separar as responsabilidades relacionadas ao acesso aos dados, promovendo a modularidade e a flexibilidade do sistema.

Funcionamento da camada de acesso TCP/IP

Os padrões da camada de acesso são diferentes no Modelo OSI e no Modelo TCP/IP. Esses padrões são determinados por algumas entidades e organizações, que se baseiam se os modelos são físicos ou não.

Muito bem! Nessa aula, você aprendeu o que são camadas de acesso a dados e suas características nos modelos OSI e TCP/IP.

Questionário

* Quais os 5 elementos necessários para qualquer comunicação?
  + Emissor, receptor, mensagem, canal e código/protocolo.
* O IEEE dividiu a camada de enlace em duas partes. Quais são essas duas partes?
  + Controle de enlace lógico e controle de acesso ao meio
* Em qual camada do modelo OSI um switch atua em uma rede de computadores?
  + Camada de Enlace de Dados

## Aula 2 - Endereço MAC e tráfego de Dados

O endereço MAC (Media Access Control) é um identificador exclusivo associado à interface de rede de um dispositivo. Ele funciona com um número de série de 48 bits e pode identificar um dispositivo de rede Ethernet ou Wi-Fi.

Além disso, o endereço MAC é uma sequência alfanumérica que segue um determinado formato específico, geralmente representado por seis pares de caracteres hexadecimais, separados por dois-pontos.

Muito bem! Você aprendeu o que significa o MAC Address e como funciona a comunicação dos ativos nas camadas 1 e 2. Siga adiante para testar seus conhecimentos.

Questionário

* Como um switch decide para qual computador ele deve encaminhar os dados em uma rede local?
  + Com base nos endereços físicos (MAC) dos computadores.
* Em redes de computadores, o que significa "MAC"??
  + Media Access Control (Controle de Acesso ao Meio).
* Para que serve o comando "show mac address-table dynamic" em um switch de rede?
  + Para exibir a tabela de endereços MAC dinâmicos com informações sobre dispositivos conectados à rede.

## Aula 3 - Protocolo ARP

O Protocolo ARP significa "Address Resolution Protocol" e é uma parte essencial das redes de computadores, utilizado para mapear endereços IP para endereços MAC em redes locais. Este protocolo é responsável por conectar um endereço IP em constante mudança a um endereço fixo.

Muito bem! Agora que você aprendeu sobre o Protocolo ARP, siga adiante para testar seus conhecimentos.

Questionário

* Qual é o principal objetivo do Protocolo ARP?
  + Mapear um endereço IP para um endereço MAC.
* Qual é a função do ARP quando um dispositivo na rede deseja enviar dados para outro dispositivo na mesma rede local?
  + Descobrir o endereço MAC de um dispositivo na mesma rede local.
* Qual o significado da sigla ARP em redes de computadores?
  + Address Resolution Protocol

## Aula 4 - Endereço IPV4

O endereço IPv4 (Internet Protocol versão 4) é um sistema de identificação numérica atribuído a dispositivos de rede para permitir a comunicação eficaz dentro de uma rede IP. Este protocolo é escrito em um sequência de dígitos de 32 bits e composto por quatro números, entre 0 e 255, e separados por pontos.

Estrutura

* O IPV4 segue uma estrutura específica que caracteriza a sua representação. Ele possui 4 octetos separados por pontos onde cada octeto é composto por 8 bits. Além disso, cada octeto varia de 0 a 255 (decimal).

A máscara de rede é um elemento fundamental para a configuração das redes IP. Ela é utilizada para determinar como os bits em um endereço IP são divididos entre a identificação da rede e a identificação do host.

A utilização de diferentes máscaras dentro de uma rede, além de garantir a segurança dos usuários dessa rede, fazem com que cada máscara trabalhe individualmente, sem afetar a velocidades ou desempenho das demais.

Questionário

* Qual é a classe do IP 192.168.5.78?
  + Classe C
* Qual é o valor binário de 85?
  + 01010101
* Quantos hosts são possíveis em uma sub-rede com máscara /24?
  + 254

## Aula 5 - IP Público, Privado e NAT

Quando pensamos no número de IP para acesso a uma rede, devemos compreender que existem diferentes características para acessos privados e acessos públicos. Os IPs internos, ou privados, são gerados automaticamente para manter casas ou empresas conectadas. Já os IPs Públicos, ou externos, são atribuídos pelo provedor de internet contratado pelo cliente.

Questionário

* Qual dos endereços abaixo é um IP privado?
  + 192.168.0.2
* Qual é a diferença entre um endereço IP público e um endereço IP privado?
  + Um endereço IP público é fornecido pelo provedor de serviços de internet (ISP) e é único em toda a internet, enquanto um endereço IP privado é usado apenas dentro de uma rede privada.

## Aula 6 - Subrede

A subrede de IPs acontecem quando existem uma divisão de uma rede de computadores em segmentos menores. Essa prática pode melhorar o gerenciamento de endereços IP, otimizar o desempenho e a segurança, e permitir a implementação de políticas de rede.

Muito bem! Agora que você aprendeu sobre as subredes, siga adiante para testar seus conhecimentos.

Questionário

* Em uma rede 192.168.0.0 com a máscara 255.255.255.128, qual é o endereço de broadcast?
  + 192.168.0.127.
* Você precisa configurar num dispositivo a máscara de rede /22, mas o fabricante exige que seja colocado no formato de 4 octetos divididos por pontos. Escolha a máscara de rede correta:
  + 255.255.252.0.
* Você é o administrador de rede da empresa Cyber Security S.A. e está configurando um firewall para manter a segurança da rede. Para que sejam feitas as configurações corretas das regras do firewall é preciso identificar o endereço de rede do IP 192.168.0.75 255.255.255.224. Escolha a rede correta abaixo:
  + 192.168.0.64.

## Recapitulando

Neste curso, você aprendeu sobre as camadas de acesso e o significado de endereço MAC e tráfego de dados. Aprendeu, também, sobre o Protocolo ARP e as características do endereço IPV4.

Além disso, conheceu as diferenças e características de IP público, privado e NAT e aprendeu o significado de subrede e como configurar em um sistema de redes.

# 

# Compreender IPv6 e camada de transporte

Neste curso, você vai conhecer sobre o endereçamento IPv6 e suas características e diferenças quanto a versão IPv4. Conhecerá, também, os tipos de comunicação mais utilizados entre os dispositivos.

Além disso, aprenderá sobre as abreviações de IP, o significado de sub-rede IPV6, as camadas de transporte e as características de diferentes entre os protocolos TCP e UDP.

## Aula 1 - Endereçamento IPv6

Conforme o avanço da tecnologia e da internet, esses recursos estão cada vez mais presentes em nossas atividades do dia-a-dia. É cada vez mais comum encontrarmos objetos e dispositivos com acesso a internet, como eletrodomésticos, câmeras de segurança e obviamente celulares e computadores.

Nesse sentido, é fundamental para a comunicação e o roteamento de dados na internet e em redes locais um identificador numérico chamado "endereço IP". Ele permite que os dispositivos se identifiquem mutuamente e troquem informações de maneira eficiente.

Endereço IP

* Os endereços IP (Protocolo de Internet) desempenham um papel crucial no funcionamento da internet e das redes. Eles são usados para rotear dados entre dispositivos, permitindo que pacotes de informação encontrem seu caminho correto de origem para destino. Além disso, os endereços IP são usados para identificar a localização aproximada de um dispositivo na rede, embora com limitações.

Os endereços IP são elementos fundamentais para a conectividade na internet e nas redes. Quando eles surgiram, a quantidade de IPs parecia suficiente. Contudo, o avanço tecnológico exigiu das pessoas e empresas mais volume de roteamento, comunicação entre dispositivos e acesso a rede. Então a quantidade de números de IP não não suporta a demanda.

Atualmente, o IPv4 (Protocolo de Internet versão 4) é a versão mais comum de endereços de IP utilizada. Porém, uma nova versão vem sendo implementada para suprir essas necessidade, o IPv6 (Protocolo de Internet versão 6).

IPv4 (Protocolo de Internet versão 4)

* Esta é a versão de endereços de IP mais utilizada atualmente. Consiste em quatro conjuntos de números decimais separados por pontos, cada um com um valor variando de 0 a 255. No entanto, devido à crescente demanda por endereços IP, o espaço de endereçamento IPv4 está se esgotando gradualmente.

IPv6 (Protocolo de Internet versão 6)

* IPv6 é a última versão do Protocolo da Internet (IP) no qual se baseia o funcionamento da Internet. As especificações técnicas básicas do IPv6 foram desenvolvidas na década de 90 no IETF (Internet Engineering Task Force).

Mas você já parou para pensar de onde vem os endereços de IPs e como eles são criados? Eles podem apresentar características diferentes, dependendo do país e região.

O IPv6 vem sendo implantado para potencializar o processo de roteamento, apresentando um aumento muito significativo no tamanho de espaço do endereço. Se antes o IPv4 era de 32 bits, hoje o IPv6 suporta 128 bits no total. Isso traz a possibilidade de conectar múltiplos aparelhos simultaneamente.

Além disso, o IPv6 apresenta outras características, como:

* Expansão das capacidades de endereçamento.
* Autenticação e privacidade.
* Autoconfiguração.
* Simplificação do cabeçalho.

O cabeçalho IP é uma informação apresentada no início de um pacote de protocolo de internet. Essas informações são essenciais e impactam diretamente na comunicação entre os dispositivos.

Muito bem! Agora que você aprendeu como funciona o endereço IP e as principais características do IPv6, siga adiante para realizar a atividade e testar seus conhecimentos.

Questionário

* Qual é a importância de ter um endereço IP para um computador?
  + O endereço IP permite que o computador se conecte à Internet, permitindo a troca de informações com outros dispositivos na rede global.
* Como o IPv6 lida com a escassez de endereços IP em comparação com o IPv4?
  + Expande o espaço de endereçamento, permitindo um número significativamente maior de endereços IP em comparação com o IPv4, o que ajuda a enfrentar a escassez de endereços.
* Qual é o tamanho do espaço de endereçamento do IPv6 em bits?
  + 128 bits

## Aula 2 - Tipos de endereço

Para que a comunicação entre os dispositivos aconteça, elas obedecem alguns métodos diferentes, dependendo da quantidade de interfaces que recebem e trocam informações. Entre a IPv4 e IPv6 também acontecem diferentes métodos de comunicação, os quais são chamados de: unicast; anycast; broadcast e multicast.

* Unicast
  + Unicast é o tipo de comunicação feita de um para um. Ou seja, é um endereçamento para um pacote feito a um único destino.
* Anycast
  + A comunicação Anycast feita de uma interface para muitas outras, contanto que elas estejam na mesma região. Cada dispositivo anuncia o mesmo endereço de rede.
* Multicast
  + É quando um dispositivo se comunica com alguns receptores. É o método de transmissão de pacote de dados para múltiplos utilizado pelo IPv6.
* Broadcast
  + Broadcast é o método de transferência simultânea para diversos receptores. É utilizado especificamente no IPv4.

Para realizar a comunicação utilizando o IPv6 é possível encontrar quase uma infinidade de combinações diferentes quanto a sua numeração. Como já aprendemos anteriormente, esses tipos de endereço dependem de uma ou mais interfaces de comunicação.

Questionário

* No protocolo IPv6, qual opção de tipo de endereço se assemelha ao conceito de "endereço público" no IPv4?
  + Global Unicast Address
* Qual dos seguintes comandos é usado para configurar o endereço IPv6 fe80::1 de link local em um roteador da Cisco?
  + ipv6 address fe80::1 link-local
* O que é Multicast em redes de computadores?
  + É uma técnica que envia pacotes de dados de um ponto para múltiplos destinatários em um grupo específico.

## Aula 3 - Abreviações IPv6

Como você aprendeu até aqui, o protocolo IPv6 veio para substituir o modelo anterior e garantir o aumento de números de endereços de IP. Dessa forma, é possível conectar os dispositivos com umas sequência quase infinita de numerações.

E a numeração, como fica?

* Se por um lado o IPv6 resolve a situação de falta de endereços, por outro ele pode complicar o operador no momento da configuração desse número muito longo em um dispositivo. Para isso, é possível abreviar os endereços.

Questionário

* Qual é o objetivo principal das abreviações no IPv6?
  + Reduzir o tamanho dos endereços IPv6.
* Em que parte de um endereço IPv6 a abreviação "::" pode ser usada??
  + Em qualquer lugar do endereço.
* Qual é a abreviação correta para o endereço IPv6 "2001:0db8:0000:0000:0000:ff00:0042:8329"?
  + 2001:db8::ff00:42:8329

## Aula 4 - Sub-rede IPv6

Conceito

* Até aqui, você aprendeu que o IPv6 utiliza um endereço de 128 bits. Isso representa 8 grupos com 4 dígitos, o que permite mais de 340 Undecilhões de possibilidades de endereços, muito acima da quantidade do IPV4.

Você conheceu até aqui que o protocolo IPv6 pode gerar uma infinidade de possibilidades na criação de redes, pois ele fornece endereços de IP único para cada dispositivo em uma rede. Esse processo é muito importante para a comunicação dos dispositivos das mesma rede ou até mesmo de redes externas.

Contudo, é possível, também, dividir ainda mais esse protocolo em sub-redes, aumentando ainda mais as possibilidades de endereços únicos de IP.

Questionário

* Considerando a rede 2001:f032:0000:0000:0000:0000:0000:0000/32 em IPv6, qual é o próximo endereço de rede?
  + 2001:f033:0000:0000:0000:0000:0000:0000/32
* Quantos bits são utilizados para representar endereços no protocolo IPv6?
  + 128
* Quantos hexatetos é formado um endereço de IPV6?
  + 8 hexatetos

## Aula 5 - Camada transporte

Todas as configurações de rede e IP devem ser pensadas sempre privilegiando a segurança da informação. Quando falamos em acesso e armazenamento de dados em nuvem, a segurança em relação aos dados e as informações trocadas entre os dispositivos é fator crucial. Para garantir esses protocolos, as camadas de transporte são serviços provem canais de comunicação em diferentes computadores.

Para que serve?

* A camada de transporte é responsável pela transferência de dados entre duas ou mais máquinas, independente da configuração de rede utilizada. Ela transporta e regula de maneira confiável o fluxo de informações desde sua origem até o destino.

Questionário

* Qual é o número da camada que representa a Camada de Transporte no modelo OSI?
  + Camada 4
* Quais são as principais funções da Camada de Transporte no modelo OSI?
  + Segmentação dos dados, multiplexação e remonta segmentos no destino.
* Quais dos seguintes são os principais protocolos que a Camada de Transporte utiliza?
  + TCP e UDP

## Aula 6 - Protocolo TCP

Até aqui você aprendeu que a segurança dos dados e informações é o fio condutor na hora de desenvolver os protocolos de IP. Tanto para empresas que conectam múltiplos dispositivos em uma rede, quanto para ambientes doméstico que também não estão livres de ataques cibernéticos. Um dos principais protocolos para garantir a segurança na comunicação da internet é Protocolo de Controle de Transmissão (TCP).

O que é?

* O TCP e baseia em um mecanismo de confirmação e retransmissão para garantir que os dados enviados de um dispositivo para outro cheguem corretamente ao destino. Ele desempenha um papel crucial na garantia da entrega confiável e ordenada de dados em redes de computadores.

O protocolo TCP apresenta diversas funções para manter as informações de estado para cada conexão de rede. Além disso, pode realizar o mapeamento de diversos endereços, números de portas para identificas serviços específicos e outras características para garantir a segurança das informações dos usuários.

* Confiabilidade
  + Uma das funções mais distintivas do TCP é sua capacidade de garantir a entrega confiável dos dados. Ele faz isso por meio de um mecanismo de confirmação e retransmissão
* Ordenação de Dados
  + O TCP garante que os dados sejam entregues ao destino na mesma ordem em que foram enviados.
* Controle de Fluxo
  + O TCP monitora o fluxo de dados para garantir que o remetente não sobrecarregue o receptor com mais dados do que ele pode processar.

Questionário

* Qual é a função principal do TCP em uma comunicação de rede?
  + Garantir a entrega ordenada e confiável de dados.
* O que é o "handshake de três vias" no contexto do TCP?
  + Um processo de estabelecimento de conexão que envolve três mensagens entre o cliente e o servidor.
* Um processo de estabelecimento de conexão que envolve três mensagens entre o cliente e o servidor.
  + A capacidade do TCP de controlar o fluxo de dados entre remetente e receptor.

## Aula 7 - Protocolo UDP

Além das transmissões de dados e informações pela internet através de e-mails, redes sociais e conexões de rede, seja em uma empresa ou no ambiente doméstico, outras aplicações que costumamos realizar do dia-a-dia também se utilizam de endereços de IP e exigem todas as medidas de segurança. Por exemplo, videoconferências, jogos online e até transmissões ao vivo em plataformas de streaming. Para isso, é utilizado o protocolo UDP, que apresenta algumas características diferentes do TCP.

Como funciona?

* O protocolo UDP foi projetado para facilitar e fornecer comunicação rápida entre dispositivos em redes IP. O UDP não realiza controle de fluxo, o que significa que não tenta ajustar a taxa de transferência com base na capacidade da rede.

A camada de transporte em uma rede desempenha um papel fundamental na comunicação de dados entre dispositivos em diferentes pontos da rede. O UDP é um protocolo de transporte rápido e eficiente, adequado para aplicativos em que a velocidade e a baixa latência são mais importantes do que a garantia absoluta de entrega de dados.

Questionário

* Qual é a principal diferença entre os protocolos UDP e TCP?
  + TCP é orientado a conexão e fornece garantia de entrega confiável, enquanto UDP é não orientado a conexão e não garante entrega confiável.
* Por que o UDP é considerado não orientado a conexão?
  + Porque não há garantia de que os pacotes chegarão ao destino.
* Quais são as aplicações comuns que utilizam o Protocolo UDP?
  + Chamadas de vídeo em tempo real.

## Recapitulando

Neste curso, você aprendeu o que são endereços IP e qual a funcionalidade deles no dia-a-dia. Conheceu as características e diferenças entre o IPv4 e o IPV6 e quais são os tipos de endereços utilizados para realizar a comunicação nesse método.

Além disso, aprendeu como realizar abreviações no IPv6 para facilitar a praticidade no processo de trabalho, a sub-rede e o que são as camadas de transporte. Por fim, conheceu as características e diferenças entre o protocolo TCP e o protocolo UDP.

# 

# Compreender camada de aplicação / serviços de rede

Neste módulo, você conhecerá os serviços de rede com foco em camadas de aplicação, iniciando com e-mail, web, DNS e DHCP. Em seguida, você terá conhecimento sobre acesso remoto, transferência de arquivos e controle de usuários. Para concluir seus estudos, você também entenderá SNMP, NTP e SYSLOG.

## Aula 1 - E-mail

Origem e funcionamento do e-mail

O e-mail surgiu em 1971, porém seu uso ficou restrito às universidades e grandes empresas por conta de seu alto custo. À medida que a internet se popularizava na década de 1990, surgiram serviços de e-mail gratuitos no mercado, o que trouxe mais usuários para esse serviço.

A mensagem eletrônica realiza um percurso entre servidores para que seja transmitida do remetente ao destinatário. Para compreender essa operação, é fundamental conhecer os principais protocolos utilizados nesse processo, entre eles, o SMTP, que é o protocolo responsável pelo envio de e-mail.

Protocolos POP3 e IMAP

Nesta segunda parte da aula, você conhecerá outros protocolos utilizados pela camada de aplicação, como o POP3 e IMAP, usados para receber e-mails por meio da recuperação e transferência do servidor.

POP3

* Transfere os e-mails de um servidor para o cliente. A mensagem é excluída do servidor.

IMAP

* Faz o download dos e-mails de um servidor para o cliente. Uma cópia da mensagem permanece no servidor.

Praticando

* Qual é a função principal do protocolo POP3 (Post Office Protocol 3) em um serviço de e-mail?
  + Receber e-mails do servidor.
* Qual dos seguintes serviços de e-mail é mais adequado para acessar e-mails, em qualquer lugar, por meio de um navegador da web?
  + IMAP
* Qual é o protocolo de camada de aplicação mais utilizado para enviar e receber e-mails?
  + SMTP

## Aula 2 - Web

Estrutura da Web

* Nesta aula, você conhecerá um serviço importante da camada de aplicação: a world wide web, mais conhecida como web. Vamos lá?
* Para iniciar os estudos, você entenderá como foram os primeiros projetos que levaram ao desenvolvimento da internet.

Década de 1980

* Tim Berners-Lee é contratado pela Organização Europeia para a Pesquisa Nuclear (CERN) para desenvolver um sistema no qual uma página continha links que levavam a outras páginas, e assim sucessivamente.

Década de 1990

* Tim Berners-Lee é contratado pela Organização Europeia para a Pesquisa Nuclear (CERN) para desenvolver um sistema no qual uma página continha links que levavam a outras páginas, e assim sucessivamente.

Para sua operação, a web precisa de alguns protocolos específicos da camada de aplicação. Além disso, os servidores enviam solicitações HTTP de vários tipos, como o GET.

Métodos HTTP e o uso do protocolo HTTPS

* Na primeira parte da aula, você conheceu a solicitação GET, que é um método HTTP. Além dele, há outros dois métodos, o POST e o PUT.
* Outro aspecto importante sobre web é o uso do HTTPS para autenticação e criptografia para proteger os dados durante o trajeto entre cliente e servidor.

Praticando

* Qual protocolo de camada de aplicação é amplamente usado para acessar páginas da web?
  + HTTP
* Qual é a função principal do protocolo DNS (Domain Name System) na internet?
  + Mapear nomes de domínio para endereços IP.
* Qual é o propósito principal do protocolo HTTPS (Hypertext Transfer Protocol Secure)?
  + Criptografar a comunicação entre o navegador e o servidor web.

## Aula 3 - DNS

Como funciona um DNS

* DNS é a sigla para Domain Name System e pode ser traduzido como Sistema de Nomes de Domínio.
* O DNS surgiu na mesma época da criação da internet, visando popularizar seu uso por meio da conversão de um hostname em um endereço de IP.
* Afinal, embora um endereço de IP seja facilmente entendido por uma máquina, seria difícil que uma pessoa decorasse tais sequências de números.

hostname

* Você digita google.com.

endereço de IP

* É convertido para 192.168.0.10.

O funcionamento do DNS para o carregamento de um site consiste em quatro servidores.

Requisição DNS e cache

* Agora que você conheceu o conceito de DNS e sua função, entenderá o processo de requisição de DNS e a definição de cache.
* O cache é um componente importante do DNS e corresponde ao espaço de armazenamento utilizado com o objetivo de otimizar diversos aspectos da navegação, entre eles:
  + aumento da velocidade de processamento das páginas web;
  + melhoria de desempenho da máquina;
  + diminuição do consumo de largura de banda.

Praticando

* O que significa a sigla "DNS" no contexto da rede de computadores?
  + Domain Name System
* Qual é a função principal do DNS?
  + Traduzir nomes de domínio em endereços IP.
* Qual é o objetivo do processo de caching no DNS?
  + Acelerar as consultas DNS, armazenando em cache informações previamente obtidas.

## Aula 4 - DHCP

O que é DHCP?

* O DHCP, ou Protocolo de Configuração Dinâmica de Hosts, é um protocolo de rede amplamente utilizado para automatizar a atribuição de endereços IP e outros parâmetros de configuração a dispositivos em uma rede.
* Ele surgiu para substituir o Bootstrap Protocol (BOOTP), também usado para configurar e inicializar dispositivos em uma rede. Algumas características do DHCP são:
  + Atribuição dinâmica de endereços de IP;
  + Configuração de máscaras de sub-rede;
  + Gerenciamento da alocação de endereços IP.

Praticando

* O que significa a sigla DHCP no contexto de redes de computadores?
  + Dynamic Host Configuration Protocol
* Qual é o papel principal do DHCP em uma rede?
  + Realizar a atribuição dinâmica de endereços IP a dispositivos na rede.
* Qual é a principal vantagem da atribuição de endereços IP via DHCP em comparação com a configuração manual?
  + Simplificação da administração de rede

## Aula 5 - Acessos remotos

Como surgiu e características do acesso remoto

* O acesso remoto nas redes de computadores inovou a tecnologia e revolucionou a forma como as pessoas interagem e se comunicam a distância. Essa evolução tecnológica é gradativa e se desenvolve através dos séculos, desde o surgimento do telefone, passando pelo sistema de modems e de conexão dial-up até chegar na computação.

Os anos 1980

* Em meados dos anos 1980, o software pcAnywhere foi um dos pioneiros e mais utilizados para acesso remoto.
* A ferramenta permitia que os usuários controlassem computadores remotamente, transferissem arquivos e prestassem suporte técnico a partir de locais diferentes.

Como funciona?

* A partir da instalação de um programa de acesso remoto, é possível executar aplicações, abrir e editar arquivos e mudar configurações de dispositivos.
* Para um acesso remoto acontecer, são necessários três elementos:
  + software;
  + hardware;
  + conectividade de rede.

Existem dois tipos de acesso remoto.

* Conexão de área de trabalho remota​
  + A conexão de trabalho remota é a capacidade de trabalhar remotamente em um computador, laptop ou smartphone por meio de um dispositivo ou software que permita esse tipo de conexão.
* Conexão via Virtual Private Network (VPN​)
  + VPN significa "rede privada virtual" e é uma tecnologia que permite a criação de uma conexão segura e criptografada pela internet ou outra rede pública.

Protocolos de acesso

* Os protocolos de acesso em redes de computadores funcionam como um conjunto de regras e procedimentos para que dispositivos conectados compartilhem recursos e informações entre si.
* Existem diversas ferramentas bem conhecidas para executar acesso remoto, tais como:
  + FTP;
  + RCP;
  + Telnet;
  + Rlogin;
  + RSH;
  + SSH.

Praticando

* Qual protocolo é amplamente usado para acesso remoto a dispositivos por meio de uma linha de comando?
  + SSH
* Qual protocolo é usado principalmente para acesso remoto a desktops ou servidores Windows?
  + RDP
* Qual dos seguintes protocolos é amplamente utilizado para compartilhar arquivos e pastas em redes Windows?
  + SMB/CIFS

## Aula 6 - Transferência de arquivo

Na era digital, a transferência de arquivos é um processo essencial que permite que os usuários movam dados de um dispositivo ou local para outro de maneira rápida e eficiente.

Existem diversas maneiras e características para realizar essas transferências, seja por meio de cabo USB, via Wi-Fi ou por serviços de armazenamento em nuvem, e alguns protocolos de transferências são muito utilizados nesse processo.

SMB/CIFS

* O SMB (Server Message Block) e o CIFS (Common Internet File System) são protocolos de rede usados para facilitar o compartilhamento de arquivos e recursos entre dispositivos em redes locais.

Torrent

* Torrent é um protocolo de comunicação utilizado para compartilhar arquivos, e o termo é frequentemente associado aos arquivos compartilhados por meio desse protocolo, que são chamados de "torrents".

FTP

* O File Transfer Protocol (FTP) é um protocolo para transferência de arquivos pela internet e foi desenvolvido em meados dos anos 1970. Ele opera em um modelo cliente-servidor, no qual um cliente de FTP se comunica com um servidor de FTP para transferir arquivos.

SMB Server

* Pensando na troca e no compartilhamento de recursos e arquivos entre computadores de uma rede local, um componente fundamental para um sistema de redes é o SMB (Server Message Block). Ele opera em um modelo cliente-servidor, no qual um servidor de recursos disponibiliza outros recursos compartilhados.
* O protocolo SMB é altamente compatível com sistemas Windows e oferece uma integração perfeita com os recursos compartilhados em redes Windows. Além disso, administradores podem configurar permissões detalhadas para controlar quem pode acessar e modificar recursos compartilhados.

Torrent

* O Torrent é uma extensão de arquivo compatível apenas com o protocolo BitTorrent, que é responsável por uma grande fatia do tráfego da internet. Esse modelo de protocolo pode gerar tanto o processo de compartilhamento quanto de downloads de arquivos diversos.

Praticando

* Qual dos seguintes protocolos é amplamente utilizado para compartilhar arquivos e pastas em redes Windows?
  + SMB/CIFS
* O que significa a sigla SMB no contexto de compartilhamento de arquivos em rede?
  + Server Message Block
* Qual protocolo é comumente associado ao compartilhamento de arquivos ponto a ponto e à transferência de grandes arquivos pela internet?
  + Torrent

## Aula 7 - Controle de usuário

Outro fator indispensável e que desempenha um papel crucial quando falamos sobre a segurança e o gerenciamento eficiente de recursos de rede é o serviço de controle de usuários de rede. Esse elemento garante que apenas usuários autorizados tenham acesso aos recursos e às informações da rede.

Ao longo do tempo, com a evolução tecnológica e o crescimento massivo de redes, os modelos de baixo custo foram substituídos por protocolos mais avançados, garantindo, assim, o controle do grande número de usuários.

Camada de aplicação

* As camadas de aplicação desempenham um papel fundamental na comunicação de rede, sendo responsáveis por permitir a interação entre aplicativos e serviços em dispositivos de rede diferentes.

Praticando

* Qual é a principal função do LDAP (Lightweight Directory Access Protocol) em sistemas de controle de usuários?
  + Autenticação e autorização
* O que o Active Directory é usado principalmente para em ambientes Windows?
  + Controle de usuários e recursos de rede
* O que significa RADIUS (Remote Authentication Dial-In User Service) no contexto de controle de acesso?
  + Um método de autenticação remota

## Aula 8 - SNMP, NTP e SYSLOG

Como você aprendeu nos módulos anteriores, os protocolos de gerenciamento e monitoramento têm um papel muito importante no mundo da tecnologia da informação. Com o avanço tecnológico e o aumento do uso de computadores e dispositivos em rede, os protocolos servem para, além de garantir a segurança dos usuários, melhorar o desempenho da infraestrutura de rede em geral.

O que é SNMP?

* O SNMP (Simple Network Management Protocol) é um protocolo do conjunto TCP/IP que permite monitorar e controlar os dispositivos da rede. Dessa forma, ele auxilia na identificação de possíveis falhas dentro dos equipamentos da rede.
* Esse protocolo pode ser usado em:
  + servidores;
  + storages;
  + roteadores;
  + switches.

Protocolo NTP

* O Network Time Protocol, ou NTP, permite a sincronização dos relógios dos dispositivos de uma rede e define uma série de algoritmos utilizados para consultar os servidores, calcular a diferença de tempo e encontrar algum erro nesse processo.

Syslog

* O System Logging Protocol é um sistema que registra eventos em log, armazenando mensagens de eventos dentro de uma rede. Dessa forma, é possível que o administrador da rede identifique as possíveis falhas do sistema ou até mesmo tentativas de invasão, garantindo, assim, a segurança da rede.

Praticando

* Qual é o objetivo principal do protocolo SNMP (Simple Network Management Protocol) em uma rede de computadores?
  + Coletar e gerenciar informações sobre dispositivos de rede.
* O que significa a sigla NTP no contexto de redes de computadores?
  + Network Time Protocol
* Qual é a principal função do protocolo Syslog?
  + Coletar informações de gerenciamento de rede.

## Recapitulando

Neste curso, você aprendeu a origem e o funcionamentos do e-mail e como foi a evolução da web com o passar do tempo até chegar aos métodos e protocolos HTTPS. Você entendeu também como funciona o DNS em um endereço de IP, bem como o conceito e as atribuições do DHCP.

Além disso, estudou o surgimento e as características do acesso remoto e aprendeu as transferências de arquivos e os principais protocolos utilizados. Por fim, conheceu o conceito de controle de usuários de rede e os principais protocolos utilizados para garantir a segurança e o desempenho de um sistema de rede.

# Utilizar sistemas operacionais - Windows

Neste curso, você vai aprender as principais funcionalidades do Windows, conhecendo sua história de criação e as versões até os dias de hoje. Aprenderá, também, como funciona o sistema e as estruturas dos diretórios e alguns atalhos do Windows para facilitar o processo de trabalho.

Aprenderá, também, como criar usuários e permissões, pensando na seguranças do usuários, como fazer o backup de arquivos e a instalação de programas e drivers.

## Aula 1 - Versões

Windows

* Windows é um dos sistemas operacionais de multitarefas mais utilizados nos computadores de dispositivos móveis ao redor do mundo. Desenvolvido ainda em meados da década de 1980, é bem provável que você utilize esse sistema em algum dispositivo em casa ou, especialmente, no ambiente de trabalho.
* Ao longo da história, o Windows é apenas um dos produtos desenvolvidos pela Microsoft, empresa fundada por Bill Gates e Paul Allen em 1975. Para conhecer um pouco mais esse caminho, vamos analisar a linha do tempo a seguir.

1970-1980 - O início

* A Microsoft foi fundada por Bill Gates e Paul Allen em 1975. Inicialmente, a empresa focou seus esforços no desenvolvimento de uma linguagem de programação chamada BASIC para o Altair 8800, um dos primeiros computadores pessoais.

1981 - MS-DOS

* Em 1981, a Microsoft comprou os direitos do sistema operacional QDOS (Quick and Dirty Operating System) de uma pequena empresa chamada Seattle Computer Products. Eles o renomearam para MS-DOS (Microsoft Disk Operating System) e o licenciaram para a IBM, que o usou no IBM PC.

1985 - Windows 1.0

* A primeira versão do Windows foi lançada em 1985. No entanto, o Windows 1.0 era mais uma interface gráfica para o MS-DOS do que um sistema operacional completo. Ele introduziu recursos como janelas sobrepostas e ícones, mas não foi amplamente adotado.

1990 - Windows 3.0

* O Windows 3.0, lançado em 1990 e trouxe melhorias significativas na interface do usuário e na capacidade de multitarefa.

1995 - Windows 95

* O Windows 95 foi um lançamento crucial para a Microsoft. Ele introduziu a barra de tarefas, o botão "Iniciar" e o suporte a dispositivos Plug and Play. Esse sistema operacional teve um enorme impacto no mercado e definiu a experiência de computação para muitos usuários durante anos.

2001 - Windows XP

* O Windows XP foi um dos sistemas operacionais mais populares da história da Microsoft. Sua estabilidade e interface aprimorada o tornaram uma escolha dominante para empresas e usuários domésticos.

2015 - Windows Vista, 7, 8 e 10

* O Windows 10, lançado em 2015 unificou muitos recursos do Windows 7 e do Windows 8 e introduzindo atualizações regulares do sistema operacional.

2021 - Windows 11

* O Windows 11 foi anunciado em 2021, trazendo uma nova interface e recursos aprimorados para melhorar a produtividade e a experiência do usuário.

Licenciamento

* A licença de softwares tem um papel fundamental no mundo da tecnologia e na relação entre desenvolvedores e usuários.
* São regras que definem o que o usuário pode ou não fazer com aquele programa.
* Isso porque, na compra de um softwares, o usuário adquire os direitos de uso do programa, e não o software em si.
* Existem outros pontos cruciais sobre a importância de utilizar um softwares licenciado.
  + Legalidade e Cumprimento das Leis
    - A licença de software estabelece os termos e condições sob os quais o software pode ser usado. Isso ajuda a garantir que os usuários estejam em conformidade com as leis de direitos autorais e propriedade intelectual.
  + Garantia e Qualidade do Suporte
    - Muitas licenças de software comercial incluem garantias e suporte técnico. Isso é importante para os usuários, pois eles podem confiar na qualidade do software e obter ajuda quando enfrentam problemas.
  + Segurança e Atualizações
    - Através da licença de software, os desenvolvedores podem definir como as atualizações e correções de segurança são distribuídas aos usuários.

Praticando

* Quem foram os criadores da Microsoft?
  + Bill Gates e Paul Allen
* Qual versão do Windows foi muito criticada por suas falhas de estabilidade e segurança?
  + Windows ME
* Qual sistema operacional Windows trouxe a assistente virtual Cortana?
  + Windows 10

## Aula 2 - Entendendo o file system

Sistema de Arquivos

* O sistema de arquivos, ou File System em inglês, é uma parte fundamental de qualquer sistema operacional de computador.
* Ele desempenha um papel essencial na organização, armazenamento e recuperação de dados em um dispositivo de armazenamento, como discos rígidos, SSDs, pendrives e outros dispositivos de armazenamento digital.

Um sistema de arquivos é uma estrutura de organizações de dados que permite que os arquivos sejam armazenados, localizados e acessados em um conjunto de regras, estruturas de dados e métodos que definem como os arquivos são nomeados, organizados e manipulados

Existem vários sistemas de arquivos em uso hoje, cada um com suas próprias características e finalidades. Com o passar do tempo, e os avanços tecnológicos, os tipos de sistemas de arquivo evoluíram conforme as demandas de trabalho.

Confira na lista abaixo alguns tipo de sistemas de arquivos do Windows.

* FAT16 – File Allocation Table 16 Bit
* FAT32 – File Allocation Table 32 Bit
* exFAT – extensible File Allocation Table
* NTFS – New Technology File System
* ReFS – Resilient File System

Praticando

* O que é um Sistema de Arquivos (File System)?
  + Uma forma de organizar e gerenciar dados em um dispositivo de armazenamento, como discos rígidos ou pen drives.
* Qual sistema de arquivos é amplamente utilizado no Windows e oferece suporte a arquivos grandes e partições de grande capacidade?
  + NTFS
* O que significa "cluster" no contexto de sistemas de arquivos?
  + Um bloco de alocação mínima em um sistema de arquivos, usados para armazenar dados.

## Aula 3 - Estrutura dos diretórios

Organização

* Em uma sociedade cada vez mais exigente quanto a produtividade, seja no mercado de trabalho, ou nas tarefas pessoais, a organização é fundamental para garantir a eficácia e otimizar as tarefas.
* Quando pensamos em nossos dispositivos e computadores, não manter a organização de nossos arquivos pode se tornar uma dor de cabeça no futuro. É para isso que existem os diretórios e pastas do Windows. Vamos entender melhor para que elas servem?

O que são diretórios do Windows?

* Diretórios, ou pastas, são containers virtuais que ajudam a organizar e agrupar arquivos relacionados em um sistema operacional Windows.
* Eles são usados para criar uma estrutura hierárquica que facilita a organização e a navegação nos dados armazenados em um disco rígido, SSD ou outro dispositivo de armazenamento.

Além da organização de pastas e arquivos, os diretórios podem ser muito úteis para outras tarefas, pensando na organização pessoal e de trabalho. Confira na lista abaixo algumas dessas funcionalidades.

* Organização pessoal
  + Você pode criar diretórios para organizar seus documentos, imagens, músicas e outros tipos de arquivos de acordo com suas preferências.
* Instalação de programas
  + Muitos programas são instalados em diretórios específicos, geralmente em "Arquivos de Programas" ou "Program Files," para manter uma estrutura organizada e facilitar a desinstalação posterior.
* Compartilhamento de arquivos
  + Você pode criar diretórios compartilhados em redes para permitir o acesso a arquivos e recursos em computadores conectados.
* Backup e recuperação
  + Diretórios são usados em operações de backup para selecionar quais arquivos e pastas devem ser copiados ou restaurados.

Navegação

* No momento de criar um sistema operacional, os desenvolvedores pensam em diversos fatores para facilitar o acesso e a navegação do usuário. Tem um sistema simples e intuitivo é peça chave para garantir o sucesso do programa.

Praticando

* Qual é a função da pasta "Desktop" (área de trabalho) no perfil de usuário?
  + Conter atalhos para programas e arquivos frequentemente usados.
* Qual pasta geralmente contém arquivos de sistema e configurações do Windows?
  + C:\Windows
* O que são atalhos no contexto do sistema operacional Windows?
  + Atalhos são ícones que apontam para arquivos, pastas ou programas em locais diferentes.

## Aula 4 - Criar, remover, apagar

Manipulação de arquivos

* Outro ponto essencial e que facilita muito o dia-a-dia de trabalho no Windows é a criação e edição de pastas.
* É possível criar pastas vazias completamente editáveis para que seja possível inserir outros documentos, vídeos e arquivos.
* Para criar e renomear as pastas no Windows, podemos seguir maneiras diferentes para o mesmo objetivo.

Comandos em modo texto

* Para facilitar o fluxo de trabalho no windows, é possível realizar a busca pelas pastas e dispositivos diretamente no prompt de comando.
* Para isso são utilizados alguns código e abreviações na língua inglesa ao realizar a busca por esses arquivos.

Confira na lista abaixo alguns comandos comuns utilizados no modo texto do Windows

* cd ou chdir – Change Directory – Mudar de Diretório (pasta);
* dir – lista os arquivos do diretório;
* cls – Clear Screen – limpar a tela;
* md ou mkdir – make directory – criar diretório;
* ren ou rename – renomear arquivo ou diretório;
* rmdir – remove directory – apaga diretório;
* Del – delete ou erase – apagar arquivo;
* copy - copiar arquivo.

Atalhos do Windows

* As teclas de atalho são combinações feitas no teclado do computador com o intuito de executar alguma ação no programa com mais rapidez e facilidade.
* Esta é outra forma utilizada para otimizar o processo de trabalho no Windows e para deixar o fluxo de trabalho mais intuitivo.

Praticando

* Qual é a maneira correta de criar uma nova pasta dentro do disco local D: no sistema operacional Windows?"
  + Abrir o Explorador de Arquivos, navegar até o disco D:, clicar com o botão direito e escolher "Novo" e depois "Pasta"
* Qual comando é usado para listar o conteúdo de um diretório no prompt de comando do Windows?
  + dir
* Qual é a combinação de teclas utilizada para abrir o Gerenciador de Tarefas no Microsoft Windows?
  + Ctrl + Shift + Esc

## Aula 5 - Criação de usuários e permissões

É muito comum no ambiente de trabalho ou no doméstico que o mesmo dispositivo seja compartilhado com duas ou mais pessoas os mesmo tempo. Se por um lado esse compartilhamento possa gerar uma economia financeira, por outro, esse procedimento pode deixar brechas na segurança dos indivíduos e no sistema operacional de uma empresa. Nesse sentido, o Windows apresenta a possibilidade da criação de usuários diferentes dentro do sistema. Vamos entender como isso funciona?

Usuários

* A criação de usuários no Windows é um aspecto fundamental para a segurança, organização e personalização de um sistema operacional. Essa prática desempenha um papel crucial em ambientes pessoais, corporativos e educacionais, oferecendo uma série de benefícios importantes.

Segurança

* A criação de usuários individuais permite que cada pessoa que utilize o computador tenha sua própria conta. Isso é essencial para manter a privacidade e a segurança dos dados.

Controle de Acesso

* Através da criação de usuários, é possível controlar quem tem acesso ao computador e aos recursos compartilhados.

Personalização

* Cada usuário pode personalizar sua própria área de trabalho, configurações de sistema e preferências.

Gerenciamento de grupos e permissões

* Para continuar com a configuração da criação de usuários do Windows, outro passo importante é a criação das permissões do sistema operacional Windows. Esta etapa é muito importante para o gerenciamento de segurança e acesso a recursos, como arquivos, pastas, impressoras e compartilhamentos de rede.
* Confira na lista abaixo alguns pontos essenciais sobre as permissões do Windows.
  + Camadas de Proteção
    - O sistema de permissões do Windows opera em várias camadas, oferecendo um nível de granularidade impressionante.
  + Grupos de Usuários
    - Para simplificar a atribuição de permissões, o Windows permite que os usuários sejam agrupados em conjuntos chamados "grupos".
  + Backup e Recuperação
    - Permissões bem gerenciadas ajudam a proteger dados importantes de exclusões acidentais ou maliciosas.

Compartilhamento em Rede

* Uma ferramenta do Windows muito vantajosa para as empresas é o compartilhamento de rede. Essa funcionalidade permite a troca de informações e recursos entre computadores em uma rede local, melhorando a colaboração, a acessibilidade e a eficiência de diversas maneiras.
* O compartilhamento de rede também pode trazer outros benefícios aos usuários, como o acesso remoto aos arquivos, a centralização de recursos e armazenamento de dados em um só ambiente e a segurança no controle de acesso dos usuários.

Praticando

* Como criar uma conta de usuário local no Windows usando o Gerenciador de Computador?
  + Gerenciador de Computador > Usuários e Grupos Locais > Botão direito do mouse em "Usuários" > Novo Usuário Local
* Qual é a diferença principal entre um usuário limitado e um administrador no Windows?
  + Um usuário limitado tem permissões restritas e acesso limitado a configurações e funções do sistema, enquanto um administrador tem controle completo sobre o sistema e pode realizar tarefas críticas de gerenciamento.
* Qual é o procedimento correto para compartilhar uma pasta em uma rede no Windows?
  + Clicar com o botão direito na pasta, selecionar "Propriedades", ir para a guia "Compartilhamento" e configurar as permissões de compartilhamento para usuários da rede.

## Aula 6 - Backup pontos e restauração registro

O que é Backup?

* Com o acúmulo de tarefas diárias no trabalho, e o grande número de pastas, arquivos e planilhas digitais que devemos controlar e gerenciar, é muito comum que esses materiais se percam em meio a tantos e-mails e repositórios.
* Para evitar dor de cabeça ao perder algum arquivo importante, é muito importante criar cópias de segurança desses documentos. Esse processo é chamado de backup.

Backup

* O Backup de arquivos no sistema operacional Windows é o processo de criar cópias de segurança de seus dados, como documentos, fotos, vídeos e outros arquivos importantes, e armazena-los em um local separado do seu computador. Ele garante a recuperação de informações valiosas em caso de falha de hardware, ataques cibernéticos ou erros humanos, proporcionando tranquilidade e segurança tanto para uso pessoal quanto empresarial.

Pontos de restauração e registros

* O sistema operacional Windows, assim como qualquer outro, em algum momento pode apresentar algum conflito. Isso pode acontecer por diversos fatores, como o mal funcionamento de algum software ou até mesmo a instalação de programas ou arquivos maliciosos.
* Pensando na segurança dos usuários é possível criar pontos de restauração no Windows, que ajudam os usurários recuperar seus sistemas para um estado anterior em caso de problemas ou mudanças indesejadas.

Pontos importantes sobre a criação de pontos de restauração do Windows

* Recuperação de Problemas
  + Os pontos de restauração fornecem uma maneira rápida e eficaz de resolver problemas e erros do sistema sem a necessidade de reinstalar o sistema operacional do zero.
* Segurança das Configurações
  + Eles permitem que você experimente configurações e instalações de software sem medo, sabendo que pode sempre voltar a um estado anterior do sistema, se necessário.
* Proteção contra Atualizações Problemáticas
  + Se uma atualização do sistema ou um novo driver causar problemas no funcionamento do computador, um ponto de restauração anterior pode ser a solução para o problema.

Praticando

* Qual é a finalidade principal de fazer um backup no Microsoft Windows?
  + Proteger seus dados contra perda.
* Qual é o procedimento correto para criar um ponto de restauração no sistema operacional Windows?
  + Acessar as "Propriedades do Sistema" e criar um ponto de restauração através das configurações de proteção do sistema.
* Qual é o procedimento correto para habilitar a exibição dos segundos no relógio do Windows usando o Editor de Registro (regedit)?
  + Navegue para "HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" no regedit e crie um novo valor DWORD chamado "ShowSecondsInSystemClock" com o valor 1.

## Aula 7 - Instalações de programas pacotes drivers

Como instalar programas no Windows?

* Um procedimento que aparentemente é bem simples no Windows é a instalação de programas. Contudo, é muito importante seguir algumas medidas de segurança para evitar justamente a instalação de programas maliciosos que possam afetar a funcionalidade do próprio Windows, além da exposição de arquivos e pastas com informações sensíveis do usuários.

]

Pacote de drivers

* Os drivers no sistema operacional Windows são componentes fundamentais que permitem a comunicação eficaz entre o hardware do computador e o software do sistema operacional. Eles atuam como intermediários, traduzindo solicitações do sistema operacional em comandos compreensíveis pelo hardware específico.

O que são Drivers do Windows?

* Os drivers são programas de software que funcionam como uma "ponte" entre o sistema operacional Windows e os dispositivos de hardware do computador. Cada componente de hardware, como placa gráfica, placa de som, impressora, mouse, teclado e outros, requer um driver específico para funcionar corretamente com o sistema operacional.

Praticando

* Quais são os cuidados importantes a serem observados ao instalar um software em um computador?
  + Ler os requisitos do sistema e garantir que o computador atenda a eles.
* Qual é o principal propósito do utilitário "winget" no Windows?
  + Facilitar o gerenciamento de instalação e desinstalação de aplicativos
* Qual é o procedimento correto para identificar se um driver está instalado em um sistema operacional Windows?
  + Acessar o Gerenciador de Dispositivos e procurar pelo dispositivo correspondente na lista.

## Recapitulando

* Neste curso, você conheceu a história de criação do Windows, os caminhos e mudanças até os dias atuais e a importância de utilizar softwares devidamente licenciados. Conheceu, também, o significado de sistema de arquivos e sobre a organização de arquivos em diretórios.
* Além disso, aprendeu sobre a manipulação de arquivos e alguns comandos do Windows, a criação de usuários no sistema, a importância do backup para a segurança dos dispositivos e como instalar programas e seus drivers com segurança.

# Utilizar Sistemas Operacionais - Linux

## Aula 1 - Versões

O Linux é um dos sistemas operacionais de código aberto, ou seja, seu código-fonte está disponível para qualquer pessoa modificar, melhorar e distribuir de acordo com os termos das licenças de software livre.

Desenvolvido pelo engenheiro de software finlandês Linus Torvalds, no início do anos 1990, os Linux cresceu rapidamente em popularidade devido a facilidade no processo de colaboração no desenvolvimento do sistema operacional.

Interfaces

* Uma interface gráfica do usuário é conhecida pela sigla "GUI", que vem do termo em inglês graphical user interface. Este é um meio de interação entre um usuário e um sistema operacional que utiliza elementos visuais, como ícones, botões, janelas e menus, para facilitar a comunicação e a execução de tarefas.
* A interface gráfica do usuário pode ser dividida por elementos visuais (ícones, botões e painéis); dispositivos de entrada (mouse, teclado, telas); menus e barras de ferramentas; entre outros elementos.

Praticando

* Quem é o criador do sistema operacional Linux?
  + Linus Torvalds
* Quais opções abaixo são distribuições Linux?
  + Debian, Fedora, Arch Linux
* Quais são os “ambientes desktops” mais populares no Linux?
  + GNOME e KDE

## Aula 2 - Estrutura de diretórios

Para facilitar a navegação, armazenamento e organização de pastas e arquivos, a estrutura de diretórios é processo essencial em um sistema operacional. No contexto do Linux, a estrutura de diretórios segue um padrão específico, que é projetado para fornecer consistência e ordem. Confira na lista a seguir alguns exemplos dessa estrutura para Linux.

* raiz (/)
  + Diretório primário no sistema de arquivos do Linux
* /boot (inicialização)
  + Armazena os arquivos necessários para a inicialização do sistema
* /home (pasta do usuário)
  + Diretório pessoal para cada usuário armazenar seus próprios arquivos e configurações.
* /root (usuário root)
  + Pasta pessoal do usuário root, o superusuário com privilégios administrativos.

Praticando

* Qual é o diretório raiz no sistema de arquivos do Linux?
  + /
* Qual é o caminho completo para o diretório pessoal do usuário "kaique" no Linux?
  + /home/kaique
* Qual é o diretório onde os arquivos de configuração do sistema são armazenados no Linux?
  + /etc

## Aula 3 - Entendendo o file system

Sistema de arquivos

* O sistema de arquivos é outro elemento fundamental quando pensamos na organização e armazenamento eficiente de arquivos dentro do sistema operacional Linux. Além disso, é peça chave para a recuperação de dados, para a estabilidade, segurança e eficácia do sistema operacional.

Organização e segurança

* O Linux segue uma hierarquia de diretórios padronizada que oferece consistência e previsibilidade. Além disso, os diretórios seguem uma estrutura separada e bem específica.
* O Linux também implementa um sistema robusto de permissões de arquivos. Cada arquivo e diretório possui atributos de permissão que regulam quem pode visualizar, modificar ou executar determinado conteúdo.

Particionamento

* Processo de dividir um disco rígido ou outro dispositivo de armazenamento em seções separadas é chamado de particionamento.
* O particionamento permite a criação de unidades lógicas em um disco físico.
* É possível, também, criar limites físicos e lógicos entre diferentes conjuntos de dados, ajudando a isolar sistemas operacionais, dados do usuário e arquivos de sistema, proporcionando maior segurança e estabilidade.

Praticando

* No contexto dos sistemas de arquivos Linux, qual sistema de arquivos é utilizado devido à sua confiabilidade, integridade e suporte a journaling?
  + Ext4
* Quais são os três aspectos essenciais que devem ser considerados ao realizar a formatação de um disco em um sistema Linux, de acordo com as melhores práticas recomendadas?
  + Faça backup dos dados importantes, escolha do sistema de arquivos e tamanho das partições.
* Qual é o principal objetivo do sistema de arquivos swap em um sistema Linux?
  + Servir como uma área de memória virtual quando a RAM física está cheia.

## Aula 4 - Comandos básicos

Ubuntu

* O Ubuntu é um dos sistemas operacionais mais utilizados pelos usuários Linux. Lançado em outubro de 2004, trata-se de um sistema operacional em código aberto projetado para ser amigável e acessível, tanto para usuários iniciantes quanto para avançados.
* Outro ponto essencial é que o Ubuntu simplifica a instalação, remoção e atualização de aplicativos.
* Este sistema é conhecido por sua robusta segurança, pois inclui recursos como que impõe políticas de segurança para os aplicativos e que facilita a configuração de regras de firewall.

Comandos

* A manipulação de arquivos e pastas no sistema operacional Linux é realizada principalmente por meio da linha de comando, oferecendo aos usuários um conjunto de comandos para gerenciar e interagir com o sistema de arquivos.

Praticando

* Qual o comando utilizando para criar um diretório (pasta) “meus\_dados” no terminal Linux?
  + mkdir meus\_dados
* Qual comando é usado para listar os arquivos e diretórios no diretório atual no Linux?
  + ls
* Qual é o comando utilizado elevar privilégios de root (administrador) no Linux?
  + sudo

## Aula 5 - Tipos de usuários

A criação de usuários no sistema operacional Linux é uma tarefa essencial para gerenciar a segurança e os acessos ao sistema. Este processo é geralmente realizado usando comandos de linha de comando, mesmo com a utilização do sistema Ubuntu.

Permissões

* Permissões são um conjunto de regras que regulam o acesso a arquivos e diretórios e determinam quem pode ler, gravar ou executar um determinado arquivo ou pasta.
* Nesse sentido, as permissões ajudam na segurança dos dispositivos, garantindo que apenas usuários autorizados tenham acesso aos recursos do sistema.

Praticando

* Qual é o tipo de usuário no Linux que possui permissões administrativas completas e pode realizar qualquer ação no sistema?
  + Usuário root
* Qual é o comando no Linux usado para criar um novo grupo de usuários chamado "contabilidade"?
  + addgroup contabilidade
* No contexto do sistema de arquivos Linux, qual das seguintes afirmações sobre permissões de usuários está correta?
  + As permissões de usuário determinam quem pode acessar um arquivo ou diretório, e quais ações (leitura, escrita ou execução) eles podem realizar.

## Aula 6 - Instalação de programas e pacotes

Softwares

* A instalação de softwares no sistema operacional Linux pode ser realizada de diversas maneiras.
* A forma mais comum se dá através do código fonte.
* Contudo, as distribuições mais populares, como Ubuntu, Debian, Fedora e CentOS, possuem sistemas de gerenciamento de pacotes que simplificam o processo de instalação e atualização de software.

Praticando

* Qual é a função do comando apt no Linux?
  + Instalar novos pacotes no sistema e atualizar ou remover pacotes existentes.
* O que é flatpak?
  + Uma tecnologia de empacotamento de software para Linux.
* No contexto do gerenciamento de pacotes em sistemas Linux, o que são "dependências"?
  + São pacotes que precisam ser instalados separadamente para que um determinado software funcione corretamente.

Recapitulando

Neste curso, você conheceu a história de criação do Linux, os caminhos e mudanças até os dias atuais e o que são as interfaces gráficas deste sistema operacional. Conheceu, também, o que são estruturas de diretórios e a importância do sistema de arquivo e do particionamento nas unidades lógicas em um disco físico

Além disso, conheceu os sistema Ubuntu, um dos mais utilizados em Linux, e os comandos para criar, remover e apagar arquivos. Por fim, aprendeu sobre os tipos de usuários, como criar permissões no sistema operacional e como realizar a instalação e remoção de programas e pacotes no Linux.

# Lógica de Programação

Neste curso, você estudará sobre a entrada e saída de dados, analisando as diferenças entre softwares e hardwares e como os programas são criados. Além disso, aprenderá sobre as variáveis e os comandos utilizados para entrada, saída e processamento de dados.

Por fim, aprenderá sobre os conceitos de estruturas, operadores e as características e diferenças entre os comandos while e for.

## Aula 1 - Entrada, Saída e Processamento

Quando pensamos sobre a lógica de programação, nos referimos a um dos conceitos fundamentais para o desenvolvimento de softwares independentemente da plataforma. Este conceito ajudar a criar estruturas lógicas e regras para desenvolver soluções de problemas computacionais.

O que é?

* A lógica de programação é a capacidade de organizar e estruturar instruções de maneira lógica e coerente, de modo que um computador possa executá-las corretamente. Ela fornece a estrutura necessária para que os programadores resolvam problemas de maneira eficaz

Os comandos de entrada, saída e processamento de dados em um computador possibilitam a interação efetiva entre o usuário e o sistema, bem como a execução de operações complexas. Os comandos de entrada permitem que um programa receba informações do usuário ou de outras fontes de dados. Já os de saída, são responsáveis por exibir informações ao usuário ou armazená-las em um local específico.

Python

* Uma das mais conhecidas linguagens de programação, o Python foi desenvolvido no início dos anos 1990 e rapidamente se tornou uma das linguagens mais populares e amplamente utilizadas no mundo do desenvolvimento de software. Ele é muito utilizado para desenvolvimento web, automação de tarefas, ciência de dados, inteligência artificial, aprendizado de máquina e desenvolvimento de jogos.

Os comandos de processamento no Python podem executar muitas tarefas diferentes no sistema, como realizar cálculos, manipular dados ou outras funções mais complexas envolvendo a tecnologia de inteligência artificial.

Praticando

* O que é uma linguagem de programação?
  + Um conjunto de comandos para realizar tarefas específicas em um dispositivo.
* Qual é o comando em Python que usamos para exibir uma mensagem como saída de um programa?
  + print("texto qualquer aqui")
* Qual das seguintes afirmações é verdadeira em relação a uma linguagem de programação?
  + Possui tanto símbolos reservados como comandos/palavras reservadas.

## Aula 2 - Variável

As variáveis funcionam como rótulos ou referências para localizar e manipular informações para armazenar valores na memória de um computador. Elas armazenam temporariamente valores que podem ser manipulados e utilizados em diferentes partes do código e são essenciais para operações matemáticas e controle de fluxos, por exemplo.

Em Python, existem diversos tipos de variáveis que podem armazenar diferentes tipos de dados. Os tipos mais comuns são:

* Inteiro (int)
  + Variáveis desse tipo armazenam números inteiros, sem parte decimal.
* Ponto Flutuante (float)
  + Variáveis desse tipo armazenam números com parte decimal.
* String (str)
  + Variáveis desse tipo armazenam sequências de caracteres, como texto.
* Lista (list)
  + Variáveis desse tipo armazenam uma coleção ordenada de itens.

Variáveis matemáticas

* A principais operações matemáticas, adição, subtração, multiplicação e divisão também podem ser desenvolvidas em Python através das variáveis.
* Ao desenvolver a linguagem de programação adequada, podemos chegar a cálculos do dia a dia de forma mais prática, como encontra o número do IMC (Índice de Massas Corporal) de uma pessoa.

Praticando

* Qual é a finalidade de usar variáveis em programação?
  + Armazenar informações temporárias para processamento
* Qual tipo de variável em Python é utilizado para armazenar sequências de caracteres, como texto?
  + String

## Aula 3 - Estrutura Condicional

Dentro da linguagem de programação, a estrutura condicional é um conceito fundamental e que permite que um programa tome decisões com base em condições específicas. E com essa capacidade que se torna possível a criação de algoritmos dinâmicos e adaptáveis, respondendo a diferentes cenários durante a execução do código.

Operadores Relacionais

* Os operadores relacionais na programação permitem a comparação de valores e a avaliação de expressões lógicas.
* Essas operações são essenciais para construir estruturas condicionais e tomar decisões com base em condições específicas durante a execução de um programa.

Operadores Lógicos

* As operações lógicas são muito usadas em conjunto com estruturas condicionais para controlar o fluxo de execução com base em múltiplas condições.

Praticando

* O que é um algoritmo?
  + Uma sequência finita de passos que levam a um resultado ou solução.
* Qual é a saída do operador "and" em uma comparação lógica?
  + Qual é a saída do operador "and" em uma comparação lógica?
* Considere um programa de computador que realiza a soma de dois números. Com base nas etapas de processamento descritas, qual das seguintes sequências de instruções representa corretamente o funcionamento desse programa?
  + Receber o primeiro número do usuário (num\_1).
  + Receber o segundo número do usuário (num\_2).
  + Somar num1 e num2.
  + Exibir o resultado da soma na tela do computador.

## Aula 4 - Estrutura de Repetição

Para que um conjunto de determinadas instruções seja executado repetidamente em Python, são empregadas as estruturas de repetição. Também conhecidas como loops, são componentes essenciais em programação quando uma tarefa precisa ser executada repetidas vezes.

Comando While

* While é um loop em Python que realiza o controle de fluxo que permite a execução repetida de um bloco de código enquanto uma condição específica permanece verdadeira.

Comando For

* O comando For é uma estrutura de controle de fluxo que facilita a iteração sobre uma sequência de elementos e é utilizado quando o número de iterações é conhecido antecipadamente.

Praticando

* O que define a lógica de programação?
  + A forma estruturada de raciocinar e criar algoritmos, utilizando sequências lógicas.
* Qual é a finalidade do comando "for" em programação?
  + Iterar sobre uma sequência de valores, como uma lista.
* Qual é a principal função do comando "while" em programação?
  + Repetir um conjunto de instruções enquanto uma condição for verdadeira.

## Recapitulando

Neste curso, você aprendeu o que significa linguagem de programação, conheceu um pouco da história da criação do sistema Python e os comandos de entrada, saída e processamento. Conheceu o que são variáveis matemáticas e como utilizá-las em Python.

Além disso, aprendeu sobre os tipos de Estrutura Condicional e os diversos exemplos práticos operadores. Por fim, aprendeu o conceito de estrutura de repetição e as diferenças de comandos na linguagem de programação.

# Desenvolvimento de Scripts

Neste curso, você irá conhecer sobre os scripts de Windows e sua importância para a linguagem de programação. Conhecerá sobre as técnicas avançadas de desenvolvimento de scripts em Windows e as características e diferenças entre os sistemas Batch e PowerShell.

Além disso, aprenderá sobre os scripts do sistema Linux, as características de ambiente de desenvolvimento e como realizar a manipulação de arquivos mantendo a segurança no desenvolvimento de scripts.

## Aula 1 - Scripts Windows

Um script é um conjunto de instruções escritas em uma linguagem de programação projetada para realizar uma tarefa específica. Ele funciona como um arquivo de texto com comandos executáveis, visando a agilidade e assertividade no processo de programação.

Os scripts podem ser usados em uma variedade de contextos, desde simples automações em sistemas operacionais até tarefas mais avançadas, como processamento de dados, manipulação de arquivos, ou mesmo controle de servidores e redes.

Técnicas avançadas

* O uso de técnicas avançadas de scripts são ferramentas versáteis e ágeis na automação de tarefas, além de apresentar um linguagem mais prática e sofisticada. Além disso, com o uso dessas técnicas, os scripts se tornam mais flexíveis, mais organizados e interativos com outros cenários.

Batch

* Este algoritmo Batch é essencial para sistemas operacionais e processamento de dados em larga escala, garantindo a conclusão de tarefas em lotes. Este sistema opera com base na execução de trabalhos em lote, onde um conjunto de tarefas é agrupado e processado sequencialmente sem a intervenção direta do usuário.