# CYBERSECURITY

# Contexto

Vivemos em uma era digital onde os dados são tão valiosos quanto o ouro. Ataques cibernéticos ocorrem frequentemente todos os dias, afetando desde usuários comuns até grandes corporações e governos.

Com isso, a segurança digital deixou de ser um tema técnico restrito a profissionais da área e passou a ser uma necessidade básica da vida moderna.

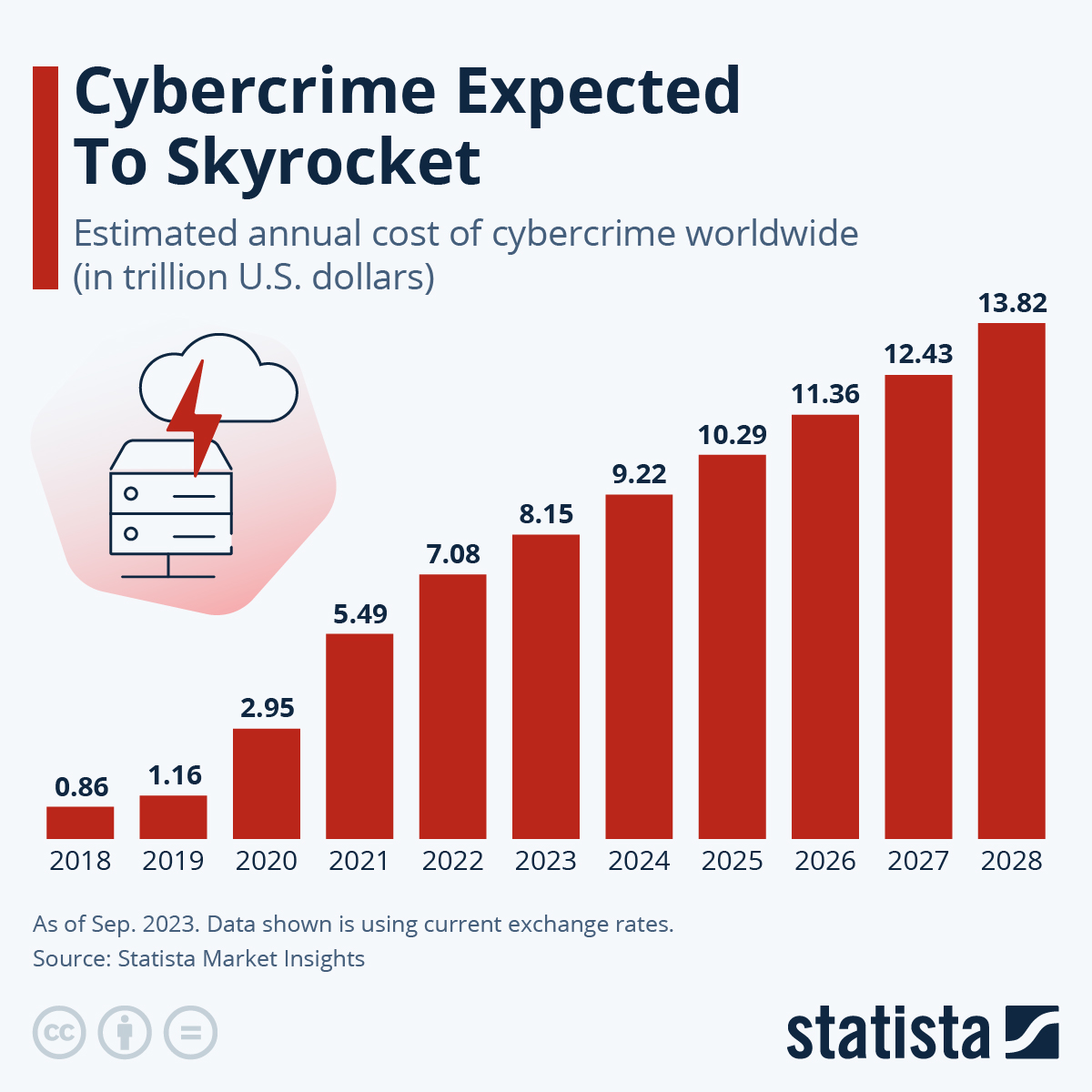
Além disso, o termo “Hacker” frequentemente é associado de forma equivocada a criminosos, quando na realidade existem diversos tipos de Hackers muitos dos quais atuam para proteger sistemas e garantir a integridade digital de empresas e pessoas.

Negligência em medidas de proteção contra ameaças online, como ataques cibernéticos, roubos de dados e fraudes pode ter consequências graves, incluindo perdas financeiras, danos à reputação e até mesmo perigo para a segurança pessoal.



Este projeto surge como uma forma de educar, informar e engajar, apresentando conceitos técnicos com uma linguagem acessível e conteúdos visuais envolventes.

Segundo um relatório da **Cybersecurity Ventures**, os danos financeiros causados pelo cibercrime podem atingir US$ 10,5 trilhões por ano em 2025, superando até mesmo o tráfico de drogas como uma das atividades ilícitas mais lucrativas.



# Objetivo

Objetivo Geral:

Promover a conscientização sobre segurança digital, desmistificar o Hacking e apresentar medidas práticas de proteção no ambiente online, com dicas e roteiros de ensinos básicos ao usuário.

Objetivos Específicos:

* + Explicar o que é Hacking e seus diferentes tipos (White Hat, Black Hat, etc.).
  + Ensinar boas práticas de segurança digital (uso de senhas fortes, autenticação em dois fatores, backups, etc.).
  + Conscientizar sobre ameaças cibernéticas reais.
  + Estimular o interesse no Hacking ético como carreira e desmitificar a área.
  + Oferecer uma experiência interativa por meio de quizzes, vídeos e seções didáticas.



# Justificativa

A ideia do projeto parte de uma motivação pessoal e de uma realidade crítica: muitas pessoas estão vulneráveis por desconhecimento.

Dado este fato a segurança digital ainda é vista de forma limitada, e é necessário mostrar que ela vai além do uso de antivírus, e não passar seus dados a terceiros. Ponto este que é de extremamente necessário atenção, pois ações maliciosas estão constantemente sendo atualizadas e gerando novos riscos.

Além disto, devemos saber como as pessoas mal intencionadas agem para que possamos prever ações de segurança, assunto este que deveria ser muito mais apresentado ao publico, para que haja mais ciência e conhecimento sobre este perigo e para que possamos melhorar cada vez mais nossa segurança digital e minimizar os ataques cibernéticos.

# ONU e ODS

A ONU, ou Organização das Nações Unidas, é uma organização internacional fundada em 1945 para promover a paz e a segurança internacionais, a cooperação econômica, social, cultural e humanitária, e o respeito pelos direitos humanos.

Papéis e Missões da ONU:

● Plataforma para diálogo, negociação e cooperação internacionais, permitindo que os países trabalhem juntos para enfrentar desafios globais.

● Promoção do desenvolvimento sustentável, dos direitos humanos e da justiça social em todo o mundo.

● Paz e segurança, desenvolvimento, direitos humanos, cooperação económica e social, meio ambiente, saúde, e emergências humanitárias.

Juntamente aos papeis e missões a ONU propôs a ODS (Objetivos de Desenvolvimento Sustentável) , também conhecidos como Objetivos Globais, são 17 objetivos globais estabelecidos pela Organização das Nações Unidas (ONU) para serem alcançados até 2030.



Conforme os objetivos citados acima, este projeto inclui-se em um tópico sendo ele o numero 4° (Educação de Qualidade). Pois a educação é fundamental ao desenvolvimento da sociedade, além disto ela é de extrema importância para o progresso econômico, cultural, político e social.

A educação, capacita os indivíduos a exercer sua cidadania, a buscar novas oportunidades e a contribuir para um futuro mais justo e igualitário. Concomitantemente a falta de conhecimento e discernimento da **educação digital** faz com que varias pessoas corram riscos digitais, sendo alguns deles: Roubo de identidade, Roubo de documentos pessoais, Roubo de recurso monetário, obstrução de dados, Ameaças, entre muitos outros.

Sabendo desta importância e dos riscos da falta de educação e o aumento da presença da tecnologia em nossas vidas, este projeto visa levar o máximo de conhecimento sobre segurança digital, para que todos usuários possam se prevenir e entender como funciona os ataques, para que consigam se proteger, como se proteger, quando e onde.

# Valores e Motivação Pessoal

Este projeto reflete minha paixão pessoal pela área da tecnologia, segurança da informação e Hacking. Desde cedo, sempre fui curioso sobre como os sistemas funcionavam, como era as estruturas digitais.

Juntamente quando pequeno via muitos filmes de ação sempre envolvia um pouco Hacking, ação onde haviam um nerd especialista em tecnologia que invadia câmeras, satélites, computadores, fazia rastreio de dispositivos e sempre chamando muito minha atenção, trazendo este interesse e essa curiosidade, por isto iniciei minha jornada na tecnologia, porém inicialmente em hardware.

Meu Objetivo desde pequeno era ter uma assistência técnica de computadores, voltado mais para manutenção avançada de placas eletrônicas. Nunca tive coragem de seguir área de programação, pois já achava muita dor de cabeça trabalhar com hardware, eu já imaginava que programação seria pior, no entanto por mais que eu tivesse vontade, por receios não progredi no assunto.

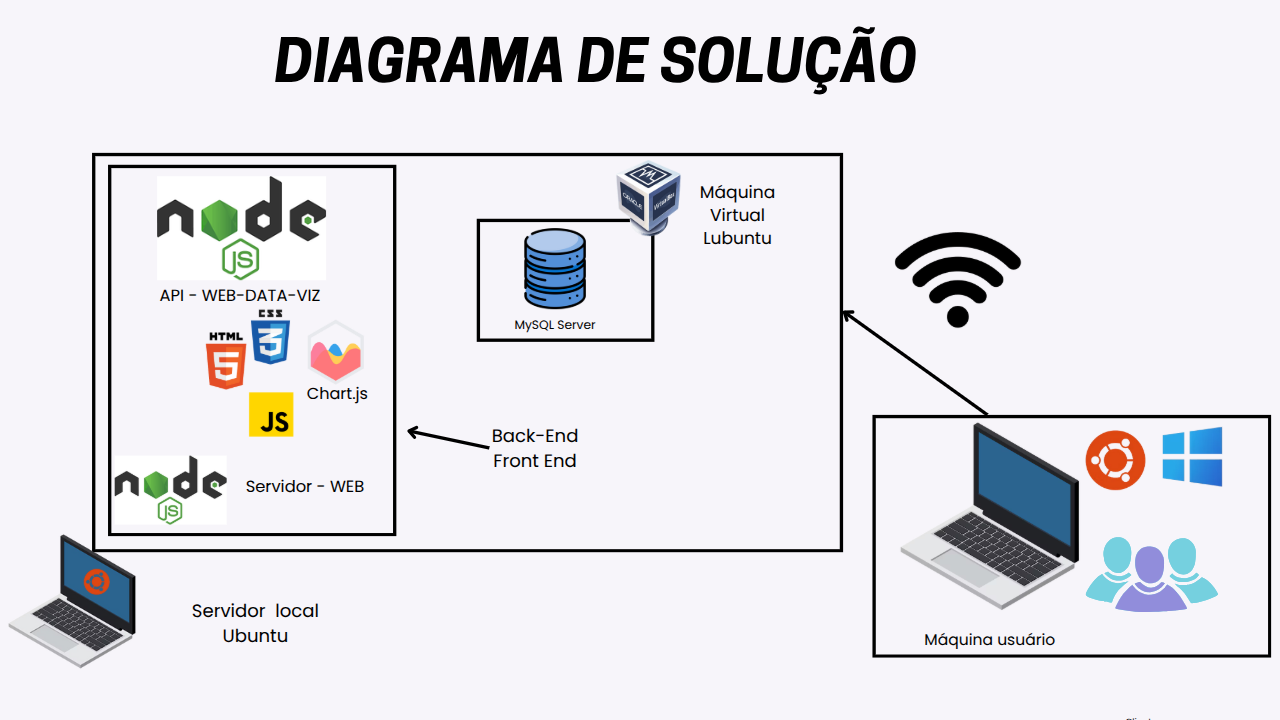
Como dito sempre fui apaixonado por filmes de ação, bem como os principais filmes e series contendo atiradores de elite, fiz curso técnico para seguir a área, e também mantive estudos na tecnologia por Hobbie, no entanto no meio desta formação desisti de seguir carreira militar por motivos pessoais.

Mesmo tendo essa paixão por tecnologia e muitos a minha volta me aconselhando seguir esta área, não me sentia seguro, não tinha visão dessa oportunidade. Porém, assim que tive a oportunidade de fazer parte do projeto da **SPTECH**, percebi que este sonho de criança deixou de ser sonho para ser uma meta de vida, sendo ela me formar em segurança digital.

Escolhi esse tema por que acredito que o conhecimento é a melhor defesa. Vivemos conectados, mas muitas vezes vulneráveis por desconhecimento. Mostrar que segurança digital vai muito além de antivírus é uma missão que carrego comigo e pretendo expandir por meio deste projeto.

Além disso, este trabalho representa minha identidade: curiosidade, ética, responsabilidade digital e paixão por aprender.

# DIAGRAMA DE SOLUÇÃO



# Escopo

Conteúdo do Site:

* + Home:
    - Frase de impacto.
    - Introdução ao conceito de Hacking e cibersegurança.
    - Texto chamando atenção do leitor.
    - Imagens chamativas com o tema “matrix”.
  + Como se Proteger?
    - Explicações sobre boas práticas de segurança digital.
    - Exemplo de boas práticas e prevenção.
    - O que é ?.
    - Perigos desta pratica ao usuário comum.
  + Hacking:
    - Tipos de Hackers.
    - Suas motivações e possíveis objetivos.
    - Tipos de perfis (Black Hat, White Hat, etc.).
    - Conteúdo sobre dispositivos de Hacking e ferramentas físicas
      * Como funcionam?.
      * Qual finalidade?
      * Por que?
      * Especificações dos dispositivos.
  + Quiz Segurança:
    - Três Questionários interativos sobre Hacking e segurança para testar conhecimentos do usuário.
    - Captura de pontuação do usuário para acompanhar performance na DashBoard.
  + Login:
    - Área de autenticação
  + Cadastro:
    - Área de registro do usuário.
  + DashBoard:
    - Incluso gráfico linha sobre quantidade de acertos do usuário.
    - Incluso gráfico pizza sobre quantidade de perfis de usuários já cadastrados.
    - KPI mostrando área de maior conhecimento do usuario.

Design e Experiência do Usuário:

* + Vídeo de fundo com estética cyberpunk/matrix.
  + Navegação fluida com menu fixo.
  + Ícones temáticos em cada seção.
  + Tipografia e cores que remetem ao universo hacker (verde, preto, branco).

Tecnologias Utilizadas:

* + HTML e CSS para estrutura e estilo.
  + JavaScript fazendo parte do back-end
  + Node.js no back-end portando e dando funcionalidade ao servidor-web para o site.
  + Node.js no back-end portando e dando funcionalidade para API, fazendo a manipulação dos dados..
  + MYSQL sobre banco de dados hospedando todos dados do site e usuários.
  + VirtualBox portando um SO (Sistema Operacional) Lubuntu base linux, hospedando o banco de dados.
  + VSCODE Interface para desenvolvimento de todos códigos.

# Metodologia utilizada:

SCRUM: Metodologia de desenvolvimento ela se baseia em princípios como transparência, inspeção e adaptação, com foco na entrega de valor ao cliente de forma rápida e eficiente.

Além disto ela define papéis específicos como Product Owner, Scrum Master e Equipe de Desenvolvimento, e utiliza reuniões regulares (Daily Scrum, Sprint Planning, Review e Retrospective) para garantir alinhamento e progresso.

O processo é guiado pelo Product Backlog e Sprint Backlog, priorizando colaboração, transparência e adaptação contínua.

Entre seus principais benefícios estão a entrega rápida, flexibilidade diante de mudanças, melhoria contínua, comunicação eficiente e aumento da motivação da equipe.

# Premissas

* + Educação como foco principal: site com propósito educativo, visando conscientizar, informar e capacitar usuários sobre segurança digital, não para práticas ilícitas.
  + Abordagem ética do Hacking: todo o conteúdo relacionado ao Hacking terá caráter instrutivo e ético, destacando o papel de hackers White Hat e desmistificando a figura do hacker criminoso.
  + Responsabilidade digital como valor central: todo o projeto será pautado em princípios de ética, respeito à privacidade, combate a fraudes e uso responsável da tecnologia.
  + O usuário terá acesso à internet e um navegador atualizado. Para que o sistema funcione corretamente, parte-se do princípio de que os usuários acessarão o site por meio de navegadores modernos, como Chrome, Firefox ou Edge.
  + O banco de dados MySQL estará acessível via rede local ou configurado na máquina virtual. Assume-se que o VirtualBox estará com o Lubuntu operacional e com o MySQL disponível para armazenamento de dados dos usuários, respostas aos quizzes e geração de métricas para o dashboard.
  + Usuários realizarão login/cadastro para acesso completo. Pressupõe-se que apenas usuários autenticados terão acesso ao dashboard com estatísticas personalizadas, protegendo suas informações.
  + O site será executado localmente ou hospedado em ambiente seguro. A funcionalidade pressupõe que o site poderá rodar localmente para testes ou ser publicado em um ambiente seguro, com controle de acesso e HTTPS, se possível.
  + A dashboard exibirá dados em tempo real com base nas interações do usuário. Considera-se que o sistema conseguirá consultar o banco de dados e renderizar gráficos e KPIs atualizados dinamicamente.

# Restrições

* + Sem incentivo ou instrução a práticas ilícitas: nenhum conteúdo poderá ensinar técnicas de invasão real ou disseminação de malwares, nem promover qualquer prática ilegal.
  + Privacidade dos usuários: O site, deverá seguir boas práticas de proteção de dados, com política de privacidade clara.

# BackLog

* + Documentação detalhada do projeto.
  + Planejamento e organização pela plataforma trello.
  + Modelagem logica do banco de dados (DER).
  + Desenvolvimento em HTML, javascript e CSS.
  + DashBoard com atualização em tempo real.
  + Na DashBoard deve incluir uma KPI e dois Gráficos.
  + Virtual machine hospedando somente o banco de dados.
  + Site contendo uma home-page apresentando projeto.
  + Quizz para teste de conhecimento do usuário.
  + Página sobre segurança digital, (Conceitos, estrategias, por que e como são originadas).
  + Página sobre Hacking (Conceitos, estrategias, por que e como originadas).

Bibliografia.

* + Instituto Nacional de Cibersegurança da Espanha (INCIBE) https://www.incibe.es
    - Informações práticas e educativas sobre segurança digital para usuários e empresas.
  + Centro Nacional de Cibersegurança do Reino Unido (NCSC)🔗 https://www.ncsc.gov.uk
    - Guia de boas práticas, ameaças e defesa contra ataques cibernéticos.
  + CyberHoot https://cyberhoot.com
    - Explicações simples sobre termos, ataques comuns e medidas de proteção.
  + Stay Safe Online (NCA / CISA)🔗 https://www.staysafeonline.org
    - Iniciativa educacional da CISA (EUA) sobre segurança e privacidade online.
  + IBM – Cibersegurança🔗 https://www.ibm.com/think/topics/cybersecurity
    - Artigos técnicos e visões corporativas sobre segurança da informação.
  + Amazon AWS – Cybersecurity 🔗 https://aws.amazon.com/pt/what-is/cybersecurity
    - Explicação clara sobre o que é cibersegurança e como proteger sistemas na nuvem.