

SÃO PAULO TECH SCHOOL

SISTEMAS DE INFORMAÇÃO

Christian Silvério Miguel Bellei – RA: 03231035

Eduardo Medina Neris – RA: 03231060

Guilherme Gonçalves Silva Santos – RA: 03231037

Isabel Bermudes de Oliveira - RA: 03231028

Lívia Yasmin Ferreira de Lanes – RA: 03231003

Tiago Ferreira Navarro – RA: 03231018

**Projeto de Monitoramento de Hardware em Servidores de Dados Sensíveis em
Empresas Brasileiras**



São Paulo
2023

SÚMARIO

1. CONTEXTUALIZAÇÃO	03
---------------------------	----

2. OBJETIVOS.....	10
3. JUSTIFICATIVA	11
4. ESCOPO.....	12
4.1. RECURSOS.....	12
4.2. ENTREGÁVEIS.....	12
4.3. ROTEIRO DO PROJETO.....	13
4.4. FORA DO ESCOPO.....	13
4.5. BACKLOG DE REQUISITOS.....	14
5. PREMISSAS	16
6. RESTRIÇÕES	17
7. WEBSITE.....	18
8. MÉTRICAS (ANALYTICS).....	19
9. DIAGRAMA DE VISÃO.....	20
10. DIAGRAMA DE SOLUÇÃO.....	21
11. DIAGRAMA DE BANCO DE DADOS.....	22

1. CONTEXTO

No cenário empresarial atual, os dados são uma commodity valiosa, e a maneira como as empresas gerenciam e protegem esses dados desempenha um papel fundamental em sua capacidade de competir, inovar e, em última análise, sobreviver. Neste contexto, abordaremos a importância crucial da preservação de dados, respaldada por dados e pesquisas sólidas, destacando por que as empresas devem garantir a segurança dessas informações sensíveis.

O vazamento de dados tem sido uma das maiores causas de perdas em grandes empresas. O Brasil estando em terceiro lugar dentre os países com o maior índice de vazamento de dados é sinal suficiente para alarmar as empresas de big data.

Empresas que oferecem soluções de crédito, registro de dívidas, seguro e consulta de dados para companhias de todos os segmentos movimentam milhões de dados sensíveis todos os dias e estão sujeitas a ataques mal-intencionados a qualquer instante. As principais causas de vazamentos não são apenas ataques cibernéticos como malware, phishing, spyware, ransomware, etc mas também falhas simples de configurações de segurança que poderiam ser facilmente corrigidas por equipes especializadas.

Juntamente com a crescente importância dos dados como ativo, os riscos de vazamento de dados também aumentaram significativamente. A cada ano, vemos um número alarmante de violações de dados, algumas das quais têm consequências devastadoras. Um estudo da IBM Security revelou que o custo médio de uma violação de dados em 2020 foi de aproximadamente US\$ 3,86 milhões. Isso inclui despesas com recuperação, multas regulatórias e perda de negócios devido à perda de confiança do cliente.

Não somente isso, um caso de vazamento de dados em 2021 ocorreu com a empresa Serasa, uma empresa privada e a maior referência de análises e informações para decisões de crédito, ou seja, eles possuem um grande acúmulo de dados privados de inúmeros clientes, como CPF, Cartão de Crédito, RG e outros dados. Esse vazamento de dados por conta de uma falha de segurança interna da empresa, no qual, um ex-funcionário utilizou de um pen-drive para roubar informações privadas e sigilosas sobre milhões de pessoas e vendeu tais informações ao externo. Por conta dessa falha, o Serasa obteve um prejuízo de aproximadamente R\$200 milhões.



Em uma pesquisa, o Procon de Niterói levantou que somente em 2022 foram vazados quase 1 bilhão de dados sensíveis no Brasil.

Os vazamentos de dados podem ter impactos significativos para os envolvidos, podem levar ao roubo de identidade, fraude financeira, violações de privacidade, danos financeiros e legais, além da irreparável perda de reputação para empresas e indivíduos.

Conforme a lei, as empresas que sofrerem perda de dados por não cumprirem os requisitos podem sofrer multas de 2% do faturamento, com limite de R\$50 milhões por infração e a indenização individual para cada brasileiro afetado pode chegar a R\$ 5 mil. Fora isso, as atividades da empresa relacionadas a bancos e tratamento de dados por um período de até seis meses, causando um prejuízo ainda maior.

É necessário entender que os vazamentos de dados podem ocorrer de diversas maneiras, e os métodos usados por criminosos cibernéticos estão em constante evolução. No entanto, a maioria dos vazamentos de dados é causada por algumas das seguintes técnicas:

- **Ataques de Phishing:** Os ataques de phishing envolvem o envio de e-mails falsos que parecem ser de fontes legítimas, mas na verdade são projetados para enganar

os destinatários a revelar informações pessoais, como senhas e informações de login. Os cibercriminosos usam essas informações para acessar sistemas e redes.

Um exemplo de vazamento de dados causado por phishing foi o caso do LinkedIn, uma rede social profissional. Em 2016, um ataque de phishing permitiu que hackers acessassem dados pessoais de mais de 117 milhões de usuários do LinkedIn, incluindo nomes, endereços de e-mail, números de telefone e datas de nascimento.

Em 2020, um ataque cibernético ao Ministério da Saúde expôs dados pessoais de mais de 243 milhões de brasileiros, incluindo nomes, CPFs, datas de nascimento, endereços e telefones. O ataque cibernético foi causado por uma falha de segurança em um servidor do Ministério da Saúde. A falha foi causada por um defeito de fabricação no servidor, que permitiu que os hackers acessassem os dados sem autorização.

- **Ataques de Malware:** O malware é um software malicioso projetado para infiltrar-se em sistemas de computador e roubar dados. Isso pode incluir keyloggers que registram tudo o que você digita, ransomware que criptografa seus arquivos até que um resgate seja pago, ou trojans que abrem uma porta de entrada para criminosos.
- **Vulnerabilidades de Software:** Às vezes, as vulnerabilidades de segurança em software ou sistemas operacionais são exploradas por invasores. Isso pode incluir a exploração de falhas de segurança não corrigidas (zero-days) ou a exploração de vulnerabilidades conhecidas.
- **Vazamentos Internos:** Nem todos os vazamentos de dados são resultado de ataques externos. Funcionários descontentes ou mal-intencionados podem vaziar informações sensíveis intencionalmente ou sem querer, por exemplo, por meio de e-mails acidentalmente enviados para a lista de destinatários errados.
- **Ataques de Injeção de SQL:** Os invasores exploram vulnerabilidades em sites ou aplicativos que não tratam adequadamente os dados de entrada. Isso pode permitir que eles injetem comandos SQL maliciosos e acessem o banco de dados subjacente.

- Dispositivos USB Infetados: Os invasores podem deixar dispositivos USB, como pen drives ou discos rígidos externos, infectados com malware em locais estratégicos, como estacionamentos de empresas ou conferências. Se alguém encontrar e conectar um desses dispositivos a um computador, o malware pode ser automaticamente transferido para a máquina e, assim, permitir que os invasores acessem o sistema. Em ambientes físicos de alto risco, como data techs, um invasor pode tentar conectar um dispositivo USB diretamente a um servidor ou sistema crítico. Isso pode permitir que eles executem comandos ou acessem dados sensíveis.

Um exemplo de vazamento de dados causado por injeções de USB foi o caso do Target, uma rede de varejo dos Estados Unidos. Em 2013, um ataque de injeção de USB permitiu que hackers acessassem dados pessoais de mais de 40 milhões de clientes do Target, incluindo números de cartão de crédito, números de segurança social e datas de nascimento.

- Falhas de hardware podem ocorrer em qualquer dispositivo eletrônico, incluindo computadores, servidores, dispositivos móveis e dispositivos de armazenamento. Quando uma falha de hardware ocorre, pode levar à perda ou exposição de dados.

Um exemplo de vazamento de dados causado por falha de hardware foi o caso da Equifax, uma empresa de serviços financeiros dos Estados Unidos. Em 2017, uma falha de segurança em um servidor da Equifax permitiu que hackers acessassem dados pessoais de mais de 147 milhões de pessoas, incluindo números de cartão de crédito, números de segurança social e datas de nascimento. Os hackers exploraram vulnerabilidades e falhas de permissionamento conhecidas no sistema operacional Linux para obter acesso não autorizado aos dados. permitiu que os hackers acessassem dados que não deveriam ter acesso. Isso ocorreu porque os hackers foram capazes de obter credenciais de administrador ou de encontrar uma vulnerabilidade no sistema operacional que lhes permitisse obter acesso não autorizado.

O caso do vazamento de dados da Equifax, que foi causado por uma falha de segurança em um servidor da empresa. A falha permitiu que hackers acessassem dados pessoais de mais de 147 milhões de pessoas, incluindo números de cartão de crédito, números de segurança social e datas de nascimento.

A falha de segurança foi causada por uma sobrecarga de CPU no servidor. A sobrecarga foi causada por um ataque de DDoS, que é um tipo de ataque cibernético que inunda um servidor com tráfego de internet. A sobrecarga de CPU fez com que o servidor travasse e os hackers aproveitaram a oportunidade para acessar os dados.

Em 2022, um disco rígido de um servidor da empresa de serviços financeiros Capital One falhou e perdeu dados pessoais de mais de 100 milhões de clientes.

Em 2023, um dispositivo USB infectado com malware foi deixado em um escritório da empresa de tecnologia Hewlett-Packard, o que permitiu que hackers acessassem dados pessoais de mais de 50 milhões de funcionários

Sabendo de todas essas informações, a pergunta que fica é, como que uma empresa que lida com tantos dados privados possui uma segurança tão frágil?

Alguns dos motivos são por conta de seu alto valor dos dados governamentais. Os sistemas governamentais contêm informações valiosas, incluindo dados pessoais de cidadãos, informações de segurança nacional e dados financeiros, como já evidenciado. Isso os torna alvos atraentes para cibercriminosos e grupos de hackers.

Além disso, muitas agências governamentais têm recursos limitados para investir em segurança cibernética. Isso pode incluir orçamentos restritos, falta de pessoal especializado e infraestrutura desatualizada. Uma pesquisa realizada pelo Centro de Estudos Estratégicos e Internacionais (CSIS) constatou que a maioria dos países não está gastando o suficiente em segurança cibernética em relação ao PIB, o que deixa as agências governamentais em desvantagem.

As agências governamentais frequentemente gerenciam sistemas e redes complexas, muitas vezes resultantes de décadas de evolução tecnológica. Isso torna difícil manter a segurança, especialmente quando sistemas mais antigos não são atualizados regularmente. De acordo com uma pesquisa da SolarWinds, 85% dos líderes de TI do setor público nos EUA acreditam que suas agências estão enfrentando desafios significativos devido à complexidade da infraestrutura de TI.

A falta de conscientização em segurança cibernética entre funcionários governamentais pode ser um problema significativo. Os ataques de phishing e engenharia social muitas vezes têm sucesso devido à falta de treinamento em reconhecimento de

ameaças. Uma pesquisa da EY em 2020 mostrou que 42% das organizações governamentais listaram a falta de conscientização em segurança cibernética entre os principais desafios.

Por conseguinte, a solução do projeto em questão é capturar dados dos componentes de hardware para emitir um alerta quando a houver alguma falha ou ultrapassar de seu limite estipulado. Esse controle é essencial, pois ele permite fazer correções na máquina, consequentemente no sistema, e aos clientes, controlá-la em tempo real e mantê-la na qualidade esperada. A questão principal a ser discutida é a otimização do processo e a eficiência na antecipação de avisos diante de um possível problema. Assim, o cliente não terá um produto indesejado para seu perfil de negócio e consequente não terá perdas de dados, interrupções de serviços, entre outros prejuízos.

Com base nessa contextualização, a solução do nosso projeto se baseia na implantação de um monitoramento de hardware eficaz para prevenir a sobrecarga da CPU, o enchimento de memória e a usabilidade do disco, instabilidade de rede e detecção de USB. O ponto principal desse projeto é monitorar os hardwares para que eles trabalhem em constante harmonia e se caso isso não acontecer, alertas serão enviados para os responsáveis dessa área para que problemas maiores, custos não planejados e sobrecarga de sistemas não aconteçam.

Os benefícios trazidos para todas as empresas que englobam esse sistema são primeiramente o desempenho otimizado, ou seja, os sistemas operam em sua capacidade máxima, resultando em um fluxo mais ágil de informações e processos, além de trabalharem em sincronia, sem paralizações e atrasos, haverá um gasto de energia mais eficiente e em uma redução geral nos custos operacionais, respostas antecipadas diante da detecção precoce de possíveis desafios e um planejamento orçamentário mais preciso.

Portanto, conclui-se que há a necessidade e a importância de sempre monitorar o hardware do sistema bancário, e que a partir de certos alertas é possível evitar que o sistema não seja danificado ou perda alguma funcionalidade, garantindo a confiabilidade do cliente e do sistema. Além disso, é evidente que a utilização de um processo automatizado que permite obter uma maior eficácia e precisão no monitoramento e medição de dados do hardware, ajudando em estatísticas interessantes e importantes para o banco. Sistemas como o desenvolvido pela 6Tracker é uma resposta direta a esses desafios, visando evitar

vazamento de dados, informar possíveis invasões, perdas financeiras e prejuízos à satisfação e segurança do cliente.

2.JUSTIFICATIVA

Aumentar a previsão de dados obtidos em 95% para a antecipação de avisos diante de um possível invasão ou vazamento de dados ou nos hardwares garantindo sua saúde em Servidores de Empresas de Dados Sensíveis, além de evitar uma perda de aproximadamente R\$75 Bilhões de reais.

3.OBJETIVOS

- Desenvolver um sistema de monitoramento em tempo real para acompanhar o uso dos componentes de hardware dos servidores.
- Desenvolver uma dashboard para acompanhamento gráfico de fácil entendimento do estado da segurança e uso dos servidores.
- Detectar possíveis programas maliciosos
- Coletar e registrar dados de uso da CPU, do disco e uso da RAM.
- Notificar em forma de alerta a equipe técnica sobre quaisquer anomalias.
- Diminuir o prejuízo monetário da empresa que é causado pela degradação de componentes de hardware, através dos dados obtidos.

- Garantir que os dados de monitoramento do hardware estejam concretos e em um nível adequado.
- Ganhar confiabilidade do cliente e aumentar os lucros.
- Obter um resultado bem-sucedido e atrair mais investidores.
- Concluir o projeto até o dia 29 de novembro de 2023.
- Originar o controle eficiente dos componentes físicos.
- Atingir 80% de feedbacks positivos diante da solução apresentada.
- Aprimorar os recursos do site institucional e aumentar a nossa visibilidade.
- Estabelecer indicadores para monitoramento dos hardwares e da eficácia de seus dados.

4.ESCOPO

Nossa solução é uma aplicação client e web para o monitoramento de componentes de hardware / sistemas operacionais utilizando os conceitos do ITIL de Monitoramento de Serviços para a Gestão de Incidentes e Gestão de Problemas em Segurança de Servidores em Empresas que lidam com dados sensíveis. Permitindo que o cliente possa tomar decisões para o melhor controle de seu servidor através da análise de dados da 6Tracker.

4.1 RECURSOS

- Equipe Web – 3 pessoas responsáveis pelo site institucional – 40 horas semanais por 3 semanas;
- Equipe Técnica – 2 pessoas responsáveis pela instalação dos softwares para monitoramento dos hardwares;

- Equipe Bussiness Partner – 3 pessoas responsáveis pela parte de Recursos Humanos – 10 horas semanais por demanda;
- Hospedagem e Domínio do site;
- Banco de Dados MySQL (local) e SQL Server (nuvem);
- API's utilizadas no projeto:
 - API 1: Gravar Dados nos Banco de Dados (Node.Js);
 - API 2: Ler dados e plotar gráficos na plataforma online, Cadastro e Login, e, produzir Alertas (Chart.Js).
 - API 3: Utilizar do Loooca para capturar e auxiliar em análises de dados de máquina conectado ao banco de dados (Java, Kotlin e Python).

4.2 ENTREGÁVEIS

- Utilização Python para realizar as capturas de dados dos componentes físicos das máquinas;
- Utilização do Kotlin para backend do sistema;
- Utilização CSS, HTML e JS para o desenvolvimento do site institucional, o qual terá as seções de home, menu, nossos serviços, sobre a equipe, fale conosco, rodapé, login e cadastro de empresas e usuários e área de dashboard onde os dados do monitoramento serão apresentados aos clientes;
- Sistema de alertas e notificações para o cliente;
- Construção do Banco de Dados MySQL (armazenamento local) e SQL Server (armazenamento na nuvem), permitindo o histórico de eventos para futura análise pela plataforma;
- Criação do website contendo as seguintes seções:
 - Pagina Home: Apresentação inicial da empresa e dos produtos;
 - Pagina Sobre nós: Apresentação aprofundada da empresa e seus princípios;
 - Pagina Nossos Serviços: Explica como funcionamos e com o que atuamos nesse ramo de hardwares e softwares;
 - Página Fale Conosco: Exibição dos meios de contato pelos quais o usuário poderá se comunicar/ esclarecer dúvidas sobre o projeto;

- Pagina Faça seu orçamento: Nossa calculadora financeira que pede algumas informações dos servidores e indica os valores estimados que podem ser ganhos com a instalação do nosso método.
- Página Login: Formulário para permitir e verificar o acesso à área restrita da plataforma;
- o Página Cadastro: Formulário de inscrição para acesso à área restrita da plataforma;
- Cadastrar Funcionário - Tela onde um usuário Admin pode cadastrar seus funcionários. Podendo assim escolher se quer dar permissão Admin ou não.
- Área de Gerenciamento: Área privada da plataforma na qual serão exibidos os dados coletados pelos componentes de hardware, permitindo a análise através de gráficos, métricas, estatísticas e com o auxílio de alertas;
- Menu: Grupo de Links na parte superior que permitirá a navegação pelo site;
- Rodapé: Bloco de informações sobre a empresa localizado na parte inferior do site.

4.3. ROTEIRO DO PROJETO

- Reunião com o cliente para definição da regra de negócio e levantamento de requisitos;
- Pesquisa de Campo para entender as reais e maiores necessidades dos clientes e áreas de maior atenção;
- Simulação e definição das áreas monitoradas;
- Construção da área de gerenciamento dentro da aplicação web;
- Tratamento e visão analítica de dados coletados;
- Reuniões com o cliente para revisões do projeto;
- Entrega do projeto completo;

4.4. FORA DO ESCOPO

- Implementação do nosso sistema de monitoramento de hardware em todas as máquinas das empresas;

- Acompanhar dados de outros componentes que não sejam CPU, Memória, Disco, Rede, Bateria e Tempo a Máquina está ligada;

4.5. BACKLOG DE REQUISITOS

Requisitos do site 6TRACKER							
Requisitos	Descrição	Funcionalidade	Classificação	Tamanho	Tam (#)	Prioridade	SPRINT
Tela Inicial - home	Página de apresentação da empresa e do projeto.	Funcional	Essencial	Médio	5	A	S1
Sobre nós	Página que irá contar sobre a empresa, seus serviços e seus fundadores.	Funcional	Desejável	Pequeno	5	C	S1
Fale Conosco	Página onde o cliente poderá nos contatar e ter suporte.	Funcional	Importante	Pequeno	5	B	S1
Sistema de Suporte	Configurar programa de suporte para o site.	Funcional	Importante	Pequeno	5	B	S1
Login	Página onde o cliente poderá acessar sua conta.	Funcional	Essencial	Médio	8	A	S1
Cadastro do profissional responsável e unidade	Página onde o cliente poderá cadastrar a unidade em que gerencia e se cadastrar.	Funcional	Essencial	Médio	8	A	S1
Cadastro de Funcionário	Página onde o profissional responsável consegue cadastrar seus funcionários.	Funcional	Essencial	Médio	8	A	S1
Dashboard	Página onde o cliente terá acesso aos dados de segurança e de processos da empresa.	Funcional	Importante	Grande	13	B	S2
Sistema de login e cadastro	Utilizar API para fazer um sistema de login funcional.	Funcional	Essencial	Grande	13	A	S2
Banco de dados	Criar banco de dados do projeto.	Funcional	Essencial	Pequeno	5	B	S1
Estratégias fixas	Menu de navegação superior, Rolagem vertical, Log-off de usuário.	Funcional	Desejável	Médio	8	B	S1
Segurança	O sistema deve ser altamente seguro, garantindo que os dados coletados sejam	Não funcional	Importante	Médio	8	C	S2

	protegidos contra acesso não autorizado.						
--	--	--	--	--	--	--	--

5. PREMISSAS

- O sistema opera em um ambiente controlado, onde a infraestrutura de rede e energia elétrica é confiável.
- O gerente administrador deverá fornecer informações confiáveis e verídicas sobre os funcionários cadastrados.
- Cada usuário terá uma única senha que não deve ser compartilhada
- Cliente irá dispor funcionários especializados para realizar o monitoramento de alertas para possível tomada de decisão.
- O cliente fornecerá todas as informações dos servidores a serem monitorados em relação ao hardware.
- O hardware monitorado é de responsabilidade do cliente.

- Qualquer dano físico ou de funcionamento do hardware é de responsabilidade do cliente.
- O contratado não terá acesso a nenhum dado dos investidores da plataforma monitorada para manter a privacidade dos mesmos.
- A monitoração não exclui a necessidade de verificações periódicas do servidor e manutenções preventivas do hardware.
- O cliente deve ter no mínimo 1 servidor a ser monitorado;
- O cliente deve possuir um funcionário técnico capaz de compreender o manual de instalação e uso;
- O cliente possui acesso à internet para utilização da plataforma;
- O cliente concorda em disponibilizar todos os materiais necessários para o desenvolvimento da aplicação;

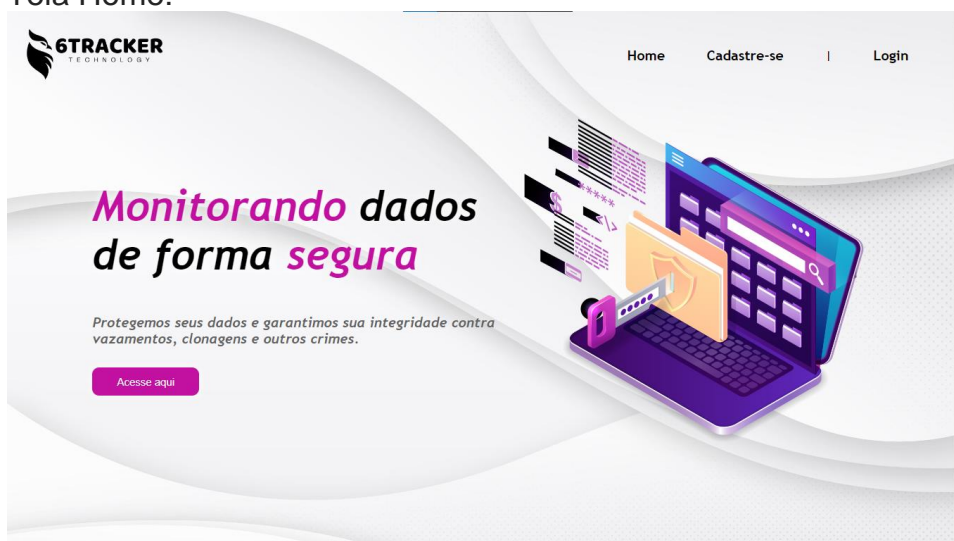
6.RESTRIÇÕES

- O programa não deve ser alterado por quaisquer usuários.
- O sistema de monitoramento não deve comprometer a privacidade dos clientes, coletando apenas dados relevantes para o desempenho do hardware.
- O sistema não será responsável pela comunicação entre os funcionários.
- A plataforma irá somente notificar não reagindo e parando qualquer processo.
- Será monitorado somente dos componentes de hardware.
- Não deverão ser utilizados recursos ou softwares que estejam fora do escopo;
- O projeto deve ser aplicado apenas em Empresas que lidam com dados sensíveis;
- Os componentes monitorados são CPU, Rede, Disco, Armazenamento e USB.
- O sistema de monitoramento precisa de energia constante.

- Prazo para a conclusão do projeto é até novembro de dois mil e vinte e três (novembro de 2023).
- A plataforma atenderá a língua Português – Brasil.

7. WEBSITE

Tela Home:



Tela o que fazemos:




Tela sobre nós:

Tela nossa equipe:



Footer (rodapé):

Tela cadastre-se do cliente:



Home Cadastre-se | Login

Bem-vindo!

NOME DA EMPRESA

CNPJ

CEP

ESTADO

RUA

NÚMERO

BAIRRO

CIDADE

Cadastrar

Tela cadastre-se do administrador:

Bem-vindo!

NOME DA EMPRESA

CNPJ

CEP

ESTADO

RUA

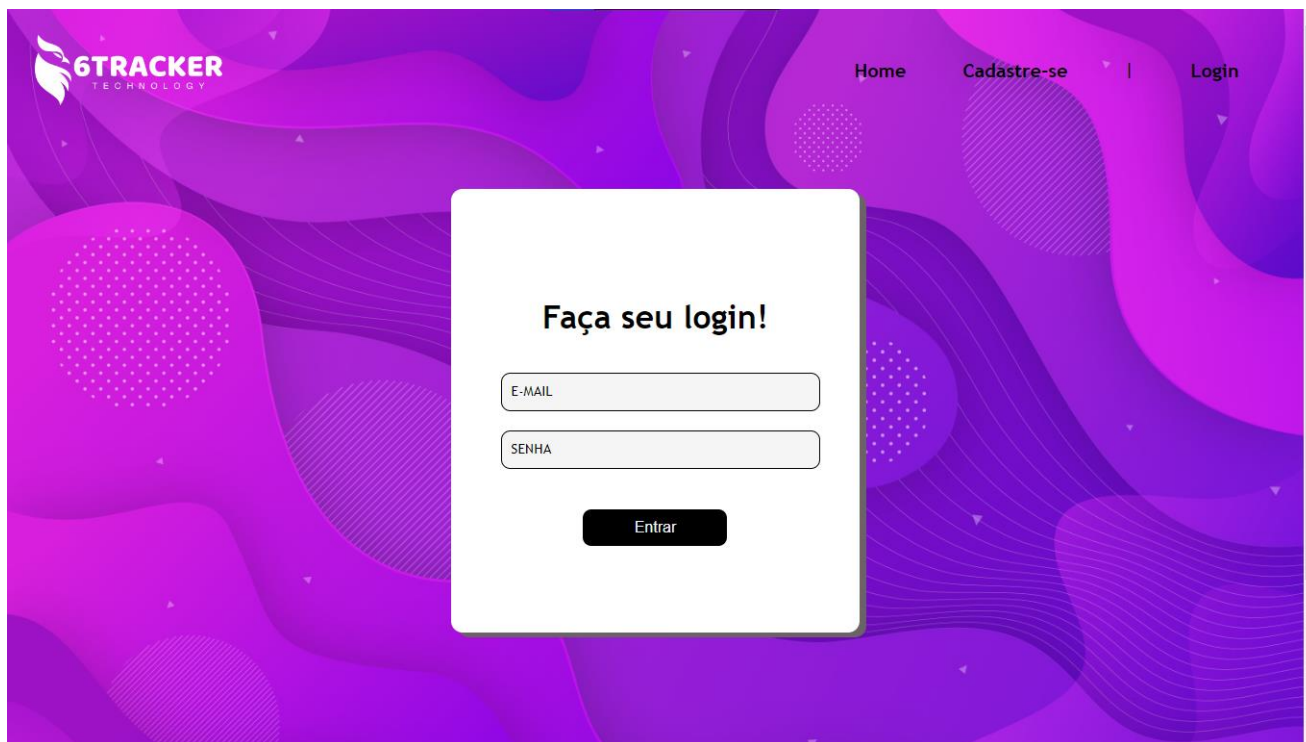
NÚMERO

BAIRRO

CIDADE

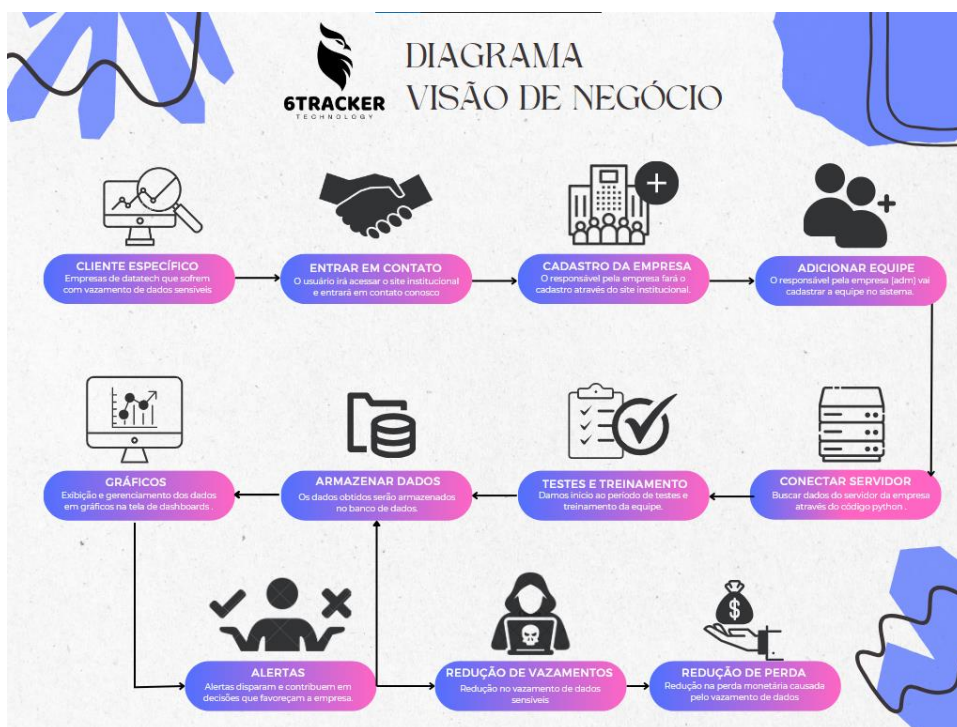
Cadastrar

Tela login:

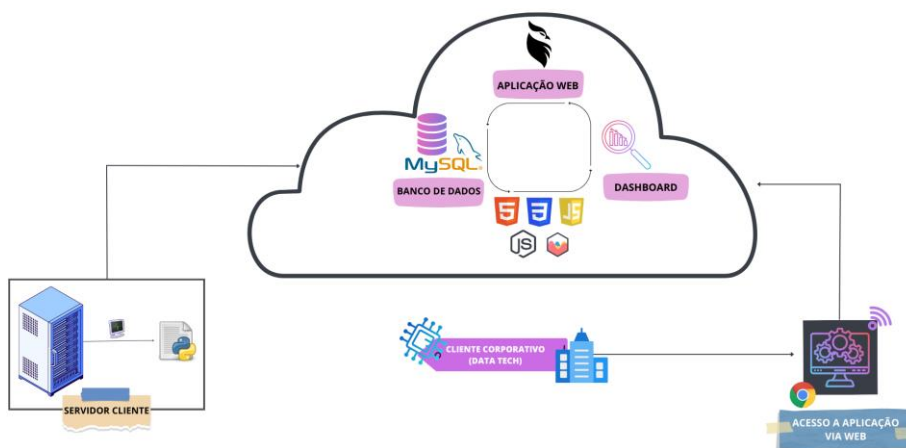


8. MÉTRICAS (ANALYTICS)

9. DIAGRAMA DE VISÃO



10. DIAGRAMA DE SOLUÇÃO



11. DIAGRAMA DE BANCO DE DADOS.