

IA 012 – Segurança em Comunicação de Dados

Prof. Marco A. Amaral Henriques

Faculdade de Engenharia Elétrica e de Computação – FEEC

Vinicius D. Silveira

14/06/2025

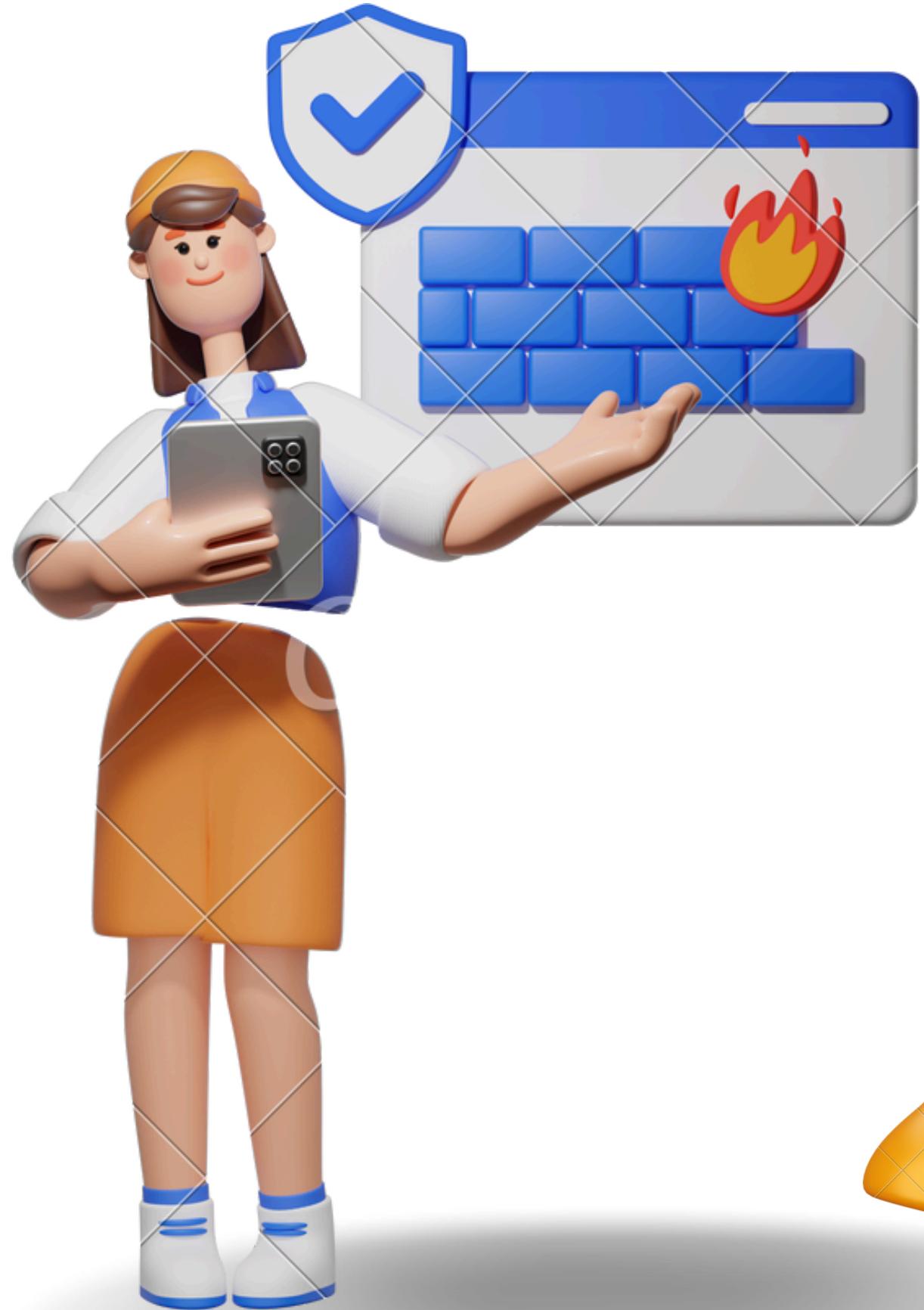
Zero Trust

Desafios de tornar técnicas de confiança zero (Zero Trust) mais amigáveis e fáceis de usar sem comprometer o alto nível de segurança esperado

Modelo de Segurança

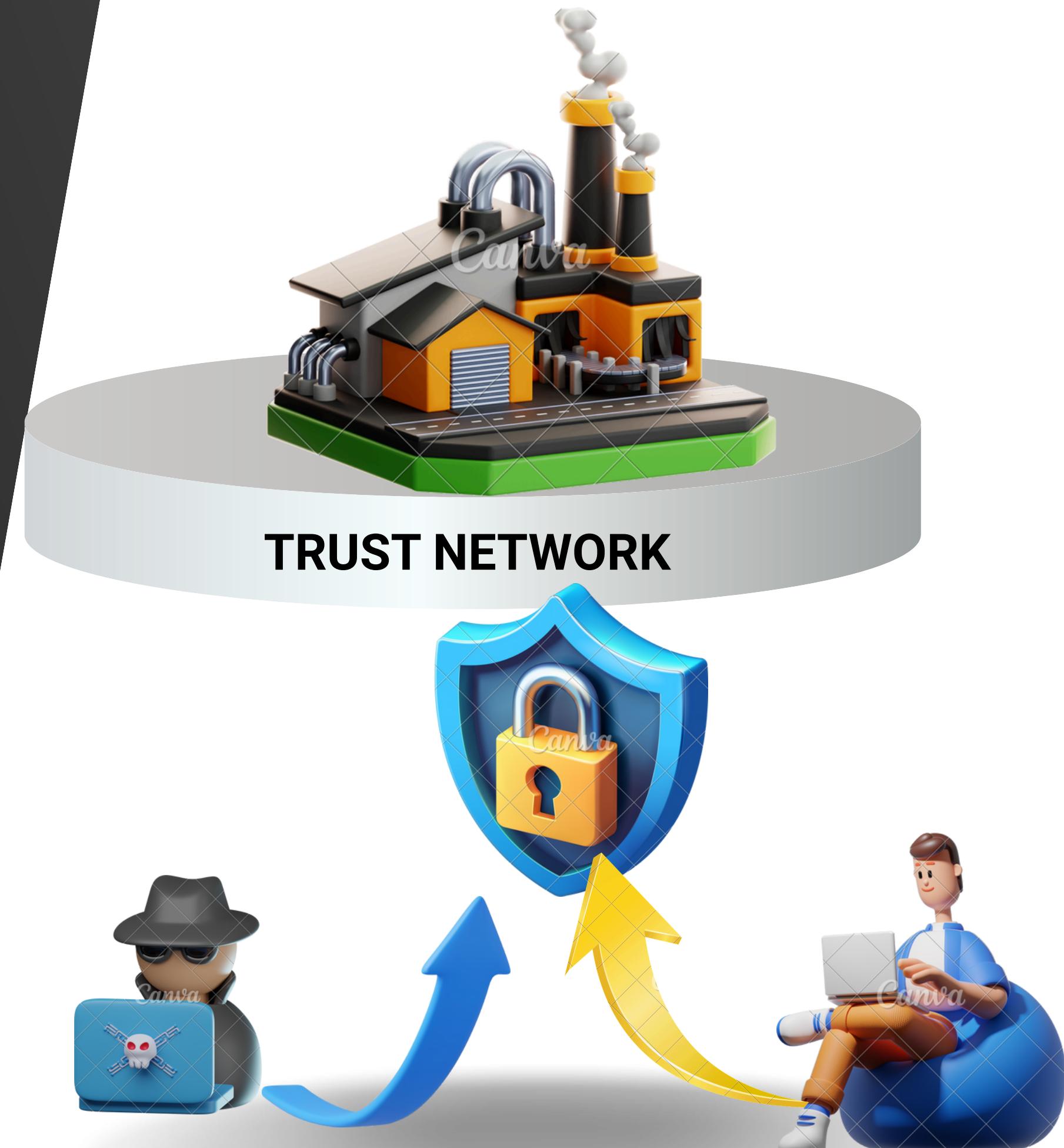
Tradicional: Baseado em perímetro

- Surgiu nos anos 1990 e início dos anos 2000.
- Motivada pelo crescimento das redes corporativas e pela necessidade de proteger o que está "dentro da empresa".
- Seguia a ideia de que a rede interna era confiável, e a ameaça estava do lado de fora.
- Usava dispositivos como:
 - Firewalls
 - IDS/IPS
 - VPNs para acesso remoto



Fatores que evidenciaram a falência do modelo baseado em perímetro

- Stuxnet (2010) mostrou que ameaças podem estar dentro do perímetro — foi inserido via pen drive em uma rede "air-gapped" (isolada).
- BlackEnergy na Ucrânia (2015) demonstrou que infraestruturas críticas conectadas não são mais isoladas e o perímetro é facilmente burlado.
- Esses eventos marcam o ponto de inflexão para o surgimento de modelos mais robustos que buscavam responder a seguinte pergunta:



Como proteger sistemas em um cenário onde o perímetro não é confiável?

- Mobilidade, BYOD, Cloud, IoT = dispersão da superfície de ataque
- Acesso remoto e distribuído se tornou a regra
- Excesso de confiança na rede interna = brechas críticas



ZT - Zero Trust

"Nunca confie, sempre Verifique"

O Que é Zero Trust?

- Modelo de segurança proposto por John Kindervag, da Forrester Research, em 2010.
 - Toda solicitação de acesso deve ser verificada, autenticada e autorizada com base em políticas de segurança, identidade e contexto.
 - Nenhum usuário, dispositivo ou aplicação é confiável por padrão
- Baseado em:
 - Verificação contínua
 - Acesso mínimo
 - Segmentação de rede
 - Monitoramento constante



ZTA – Arquitetura Zero Trust

“A confiança em um objeto só pode ser obtida por meio da autenticação de identidade e da avaliação contínua de confiança.”

— Khan et al. (2022) [1]

Diferença entre zero trust e Arquitetura Zero Trust

NIST SP 800-207

“Zero Trust (ZT) fornece um conjunto de conceitos e ideias projetados para minimizar a incerteza na aplicação de decisões precisas de acesso por solicitação e com privilégios mínimos a sistemas e serviços de informação diante de uma rede considerada comprometida.

A Arquitetura Zero Trust (ZTA) “é um plano de segurança cibernética empresarial que utiliza conceitos de confiança zero e abrange relacionamentos de componentes, planejamento de fluxo de trabalho políticas de acesso.”

— Challener et al. (2020) [2]



7 - Princípios básicos da Confiança Zero

NIST SP 800-207



Todos os dados e serviços são considerados recursos

Não importa se estão "dentro" ou "fora" da rede. Tudo precisa de proteção.



Toda comunicação deve ser segura, independentemente da origem

Mesmo que dois sistemas estejam na mesma rede, a comunicação entre eles deve ser protegida.



Acesso aos recursos é concedido por sessão

Cada solicitação é avaliada individualmente. Não há confiança herdada de acessos anteriores.



O acesso é determinado por políticas dinâmicas baseadas em contexto

Avalia identidade, dispositivo, local, horário, comportamento e outros atributos

7 - Princípios básicos da Confiança Zero

NIST SP 800-207



Monitoramento contínuo da integridade e segurança dos ativos

Nenhum ativo é confiável por padrão. Dispositivos com vulnerabilidades podem ser isolados ou bloqueados.



**Toda autenticação e
autorização de recursos
são dinâmicas e
rigorosamente aplicadas
antes que o acesso seja
permitido.**

MFA, revalidação por política, e
detecção de anomalias em
tempo real são essenciais.



Coleta contínua de dados para reforçar a postura de segurança

Monitoramento de tráfego,
acessos e dispositivos para
ajustar políticas e responder
a ameaças rapidamente.

Caso de uso escolhido

Estratégia de Segurança Zero Trust para Sistemas de Colaboração

— Bouazizi et al. (2023) [3]

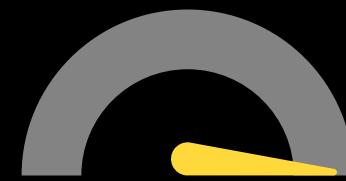
- **Objetivo:**
 - Implementar uma arquitetura de segurança baseada no modelo Zero Trust em um ambiente de nuvem comunitária, com o objetivo de viabilizar a colaboração segura entre organizações autônomas que compartilham recursos (como dados, máquinas virtuais, softwares, etc.), eliminando qualquer tipo de confiança implícita e garantindo controle, autenticidade e rastreabilidade nas interações.

Componentes da Arquitetura



Identidades e Credenciais via Blockchain

- Cada organização possui Identificadores Descentralizados (DIDs) e emite Credenciais Verificáveis (VCs) para seus usuários.
- Informações de identidade e recursos são registradas em blockchain.
- A autenticação é realizada por meio de contratos inteligentes que validam as VCs com chaves públicas.
- Permite controle total da identidade, com revogação e validade temporal.



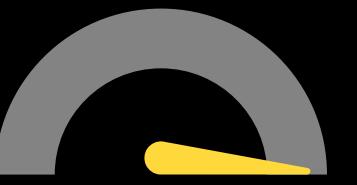
Mecanismo de Confiança e Monitoramento

- Avalia a confiança entre organizações com base em interações anteriores e reputação comunitária.
- O valor de confiança determina a autorização para colaboração.
- Realiza monitoramento contínuo de níveis de confiança, contratos, identidades, atores e recursos em tempo real.

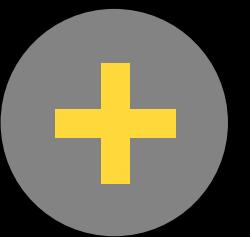
Quais foram os resultados produzidos?



Identificação e autenticação robusta de usuários e organizações via DIDs e VCs, com autenticação via smart contract.



Avaliação dinâmica de confiança (Trust Inference) para decidir se uma organização pode ou não participar de uma colaboração com base na qualidade dos recursos já fornecidos.



Contratos inteligentes de colaboração e regras de acesso claras e adaptáveis.

Quais ainda não foram alcançados?



Avaliação de Desempenho

Medidas de desempenho, como tempo de autenticação, tempo de inferência de confiança ou sobrecarga da blockchain.

Questões de Usabilidade e Adoção

A pesquisa não aborda os desafios organizacionais e culturais que poderiam dificultar a adoção do Zero Trust

Modelo de Confiança Simples

O modelo de inferência de confiança proposto é básico e não inclui questões mais complexas

Privacidade de dados sensíveis

Não se discute como garantir a privacidade dos dados transacionados ou dos próprios contratos de colaboração

**Desafios de tornar técnicas de confiança zero
(Zero Trust) mais amigáveis e fáceis de usar sem
comprometer o alto nível de segurança esperado**

Desafios na Adoção do Zero Trust na Prática

- Técnicas de segurança muitas vezes:
 - Exigem múltiplos fatores de autenticação.
 - Impõem fricção ao usuário.
 - Criam barreiras para produtividade.
- Dilema: Segurança vs Experiência do Usuário
- Exemplos Práticos de Dificuldade
 - Funcionários que precisam autenticar a cada acesso.
 - Apps que não integram bem com soluções Zero Trust.
 - Falta de visibilidade e controle para usuários comuns.



Caminhos para Tornar Zero Trust Mais Amigável

- **Autenticação Adaptativa (Baseada em Risco/Contexto)**
 - Ajusta o nível de autenticação conforme o comportamento do usuário e condições do acesso (localização, horário, dispositivo, etc.).
 - Exemplo: se o acesso é feito do mesmo dispositivo e local de sempre, o sistema pode exigir menos validações.
 - Reduz atrito sem comprometer a segurança.



Caminhos para Tornar Zero Trust Mais Amigável

- **SSO + MFA Leve**
 - SSO (Single Sign-On): permite que o usuário acesse vários sistemas com um único login.
 - MFA (Autenticação Multifator): ainda é necessário, mas pode ser integrado de forma rápida e fluida (ex: reconhecimento facial, token via app).
- - Combinados, mantêm a segurança e melhoram a experiência do usuário.



Caminhos para Tornar Zero Trust Mais Amigável

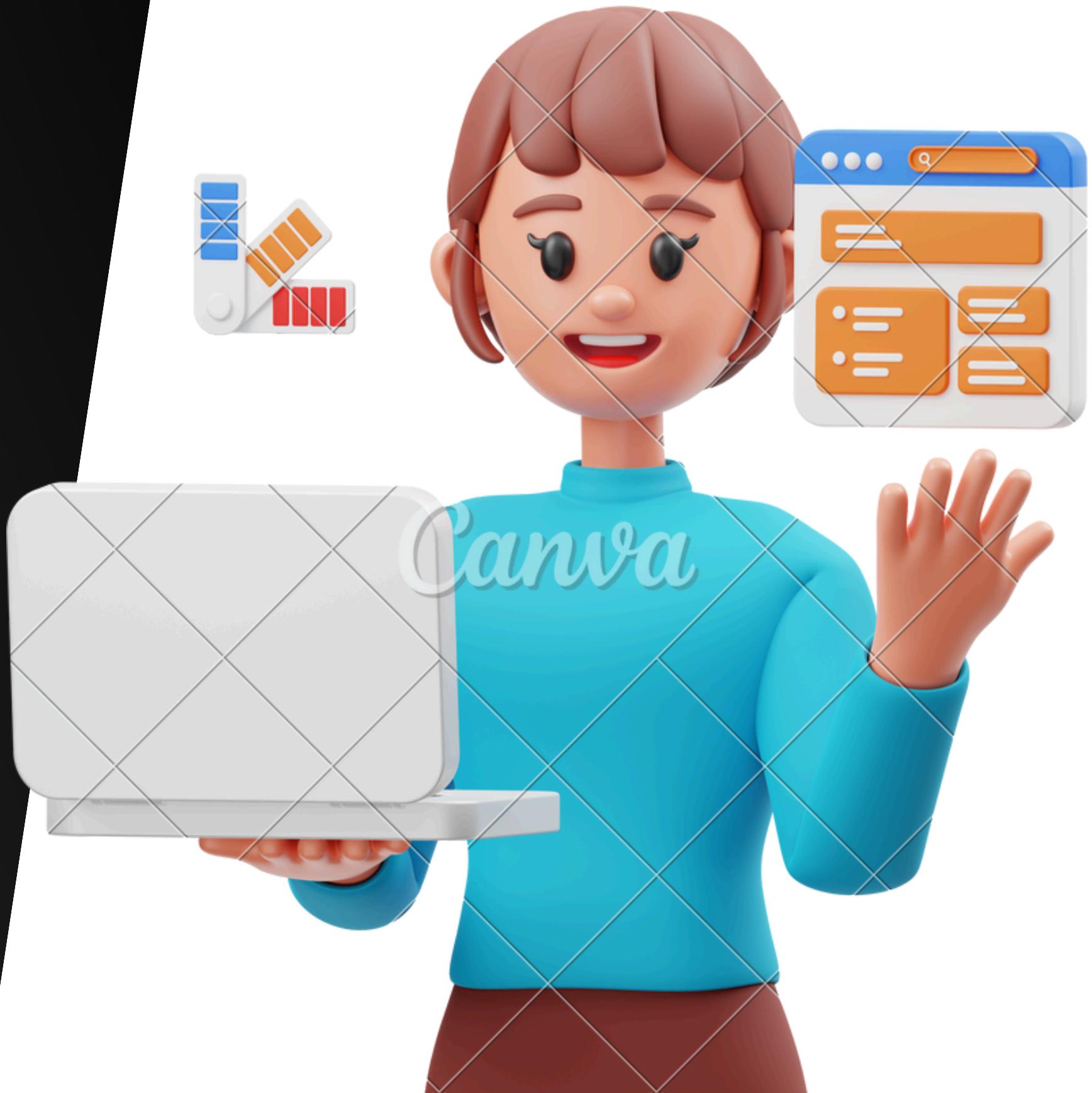
- **Segurança Invisível ao Usuário**

- Implementação de segurança sem interferência direta ou interrupções frequentes.
- Exemplo: monitoramento de sessão, análise comportamental em segundo plano.
- O sistema atua silenciosamente, mas alerta ou bloqueia se algo parecer suspeito.
- Usuário sente fluidez, mas continua protegido.



Caminhos para Tornar Zero Trust Mais Amigável

- **Design Centrado no Usuário nas Ferramentas de Segurança**
 - Interfaces de segurança precisam ser intuitivas, claras e acessíveis.
 - Reduz erros de configuração e resistência dos usuários.
 - Ajuda na adoção mais rápida das políticas de segurança.
 - Exemplo: dashboards simples para gestores controlarem acessos com poucos cliques.



Oportunidades de pesquisa em Confiança Zero



Estabelecimento da Confiança Inicial

Como confiar em partes sem informações prévias?



Gestão da Confiança Dinâmica

Avaliar continuamente a confiabilidade com base no contexto e histórico.

Ameaças Internas

Privilegiados maliciosos ou descuidados representam riscos críticos.

Alta Entropia de Dados

Grandes volumes de dados heterogêneos e ruidosos.

Ambientes de Nuvem Complexos

Latência, autenticação frequente e gerenciamento massivo de identidades

Dispositivos IoT Limitados

Recursos computacionais limitados dificultam autenticação contínua.

Privacidade e Eficiência em Tempo Real

Proteção de dados sensíveis e resposta em tempo real são essenciais.



Demonstração de Zero Trust para acesso a nuvem

Implementação de uma aplicação de acesso à nuvem baseada no modelo Zero Trust, com uso de contratos inteligentes e credenciais verificáveis (VCs) para garantir segurança, controle de acesso e auditabilidade das interações.

Demonstração de Zero Trust para acesso a nuvem

V 2025 06 21 18 13:35

ZeroTrust Cloud

Sistema de acesso Zero Trust para provedores de nuvem

Rede: Ethereum Sepolia Owner: 0xDb93...Abba

⚠ Diagnóstico de Acesso

Owner do Contrato: 0xDb938156988933FF867f1BE01048245e9d1eAbba

Endereço Contrato: 0xDb938156988933FF867f1BE01048245e9d1eAbba

💡 Você é o owner! Pode acessar todas as áreas.

⚙️ Gerenciamento de Credenciais

Área exclusiva para o owner do contrato gerenciar credenciais

Owner Autenticado

Watch on YouTube

Emitir Nova Credencial



The screenshot shows a web-based ZeroTrust Cloud interface. At the top, there's a navigation bar with tabs for MetaMask, ZeroTrust Cloud Access, and Remix - Ethereum IDE. The main content area has a light blue header with the ZeroTrust Cloud logo and a subtitle in Portuguese. Below this, it displays network information (Ethereum Sepolia) and ownership details (Owner: 0xDb93...Abba). A large yellow box on the left contains sections for 'Diagnóstico de Acesso' (with a note about being the owner) and 'Gerenciamento de Credenciais' (with a note about authenticating the owner). To the right of these boxes is a large, semi-transparent overlay featuring a 3D fox head logo. At the bottom of the page, there are links to watch a YouTube video and to issue new credentials.

Referencias

- 1- KHAN, Muhammad Kashif et al. A Survey on Zero Trust Architecture: Challenges and Future Trends. Wiley, 2022. Disponível em:
<https://onlinelibrary.wiley.com/doi/full/10.1155/2022/>. Acesso em: 21 jun. 2025.
- 2- CHALLENGER, John et al. Zero Trust Architecture. NIST Special Publication 800-207, 2020. Disponível em:
<https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf>. Acesso em: 21 jun. 2025.

Referencias

- 3– BOUAZIZI, Mohamed Salah et al. Security Strategy for Collaboration Systems. IEEE ISNCC 2023. DOI: <https://doi.org/10.1109/ISNCC58260.2023.10323911>.

- 4– SILVEIRA, Vinicius D. ZeroTrust_VCs. GitHub, 2025. Disponível em: https://github.com/vdsilveira/ZeroTrust_VCs. Acesso em: 21 jun. 2025.

Obrigado pela atenção!

Fico à disposição para perguntas e comentários.