Capa do Projeto

Título do Projeto: SmartTower – Sistema Integrado de Monitoramento Estrutural com IoT para Edificações Urbanas

Autores: Gustavo Jaccon Franquini | RA: 825150548
Matheus Diniz Vitorino Pinto | RA: 825143846
Kevin Nash Quispe Chacolla | RA: 825251331
-Rafael Tarifa da Silva | RA: 825131731
Talyson Abner Santos Julião da Paz | RA: 8251538040

Data de entrega: 26/11/2025

Descrição: Documento contendo estruturação, modelos, diagramas, tabelas e demais elementos produzidos.

SUMÁRIO

1. INTRODUÇÃO

A sociedade contemporânea depende estruturalmente da computação para realizar operações críticas em praticamente todos os setores — saúde, finanças, transporte, indústria, educação e comunicação. Com a digitalização dos processos, a tecnologia tornou-se o núcleo das atividades humanas, e o volume de dados gerado cresce de forma exponencial. Nesse cenário, torna-se fundamental compreender como os sistemas computacionais funcionam internamente e, ao mesmo tempo, como podem ser protegidos contra ameaças que evoluem continuamente.

A arquitetura computacional, área que estuda a estrutura, o funcionamento e o desempenho dos sistemas de hardware, fornece a base para o entendimento de como instruções são processadas, como dados são armazenados e como diferentes componentes interagem por meio de barramentos, memórias e processadores. Esse conhecimento é indispensável tanto para projetar equipamentos potentes quanto para otimizar softwares de alto desempenho.

Paralelamente, os princípios de segurança da informação ganham destaque devido ao aumento de ataques cibernéticos, vazamentos massivos, fraudes digitais e crimes relacionados ao uso indevido de dados. A segurança da informação busca garantir que sistemas e informações permaneçam disponíveis, íntegras e acessíveis somente a pessoas autorizadas, constituindo um pilar indispensável da tecnologia moderna.

A integração entre arquitetura computacional e segurança da informação é um elemento crítico na construção de infraestruturas confiáveis. Sistemas mal projetados ou sem proteção adequada tornam-se vulneráveis, podendo comprometer operações empresariais, privacidade individual e até a segurança nacional.

O presente trabalho oferece uma análise ampla, profunda e tecnicamente fundamentada desses dois mundos complementares, incluindo diagramas e tabelas que facilitam o entendimento de tópicos complexos como hierarquia de memória, paralelismo, criptografia e modelos de ameaça.

2. REFERENCIAL TEÓRICO

O referencial teórico reúne os fundamentos essenciais que sustentam a compreensão do tema analisado neste trabalho, abrangendo desde os princípios estruturais da arquitetura computacional até os mecanismos modernos de proteção e defesa cibernética. Essa base conceitual permite relacionar o funcionamento interno dos sistemas computacionais com os desafios contemporâneos de segurança digital.

Para isso, são apresentados três pilares principais:

- **Arquitetura Computacional**, abordando CPU, memória, barramentos, modelos arquiteturais e paralelismo;
- **Princípios de Segurança da Informação**, considerando o modelo CIA, criptografia e mecanismos de proteção;
- **Ameaças e Vulnerabilidades**, contextualizando riscos modernos e suas contramedidas.

Esses elementos teóricos fornecem o suporte necessário para as análises e discussões desenvolvidas nas seções seguintes.

3. METODOLOGIA

A elaboração deste trabalho seguiu uma abordagem **qualitativa, exploratória e descritiva**, fundamentada na análise de livros, artigos científicos, normas técnicas e publicações especializadas sobre arquitetura de sistemas computacionais e segurança da informação. A metodologia foi estruturada em três etapas principais:

1. Revisão Bibliográfica

Foram consultadas obras relevantes, como publicações do NIST, livros sobre IoT, segurança de redes, arquitetura computacional e documentos técnicos contemporâneos. Essa etapa permitiu reunir conceitos fundamentais e identificar padrões, modelos e práticas recomendadas.

2. Análise Estrutural e Comparativa

Os conceitos obtidos foram comparados, correlacionando:

- funcionamento interno de CPUs, memórias e barramentos
- princípios de segurança digital
- ameaças modernas e mecanismos de defesa
- aplicações reais em contextos como IoT, data centers e sistemas críticos

Essa análise permitiu integrar áreas tradicionalmente separadas (hardware e segurança) em uma visão sistêmica.

3. Elaboração dos Diagramas, Tabelas e Estrutura Didática

Diagramas explicativos (arquitetura Von Neumann, modelo CIA, fluxo de CPU, criptografia), bem como tabelas comparativas, foram desenvolvidos para facilitar visualmente a compreensão de conceitos complexos.

A metodologia adotada garante clareza, profundidade teórica e coerência com as práticas acadêmicas exigidas para trabalhos técnico-científicos.

4. ARQUITETURA COMPUTACIONAL

Conceito, Propósito e Importância

Arquitetura computacional é o campo que define como os componentes de um sistema computacional são organizados e como interagem para executar operações. Ela se divide em três dimensões essenciais:

1. Arquitetura de conjunto de instruções (ISA) – define instruções, modos de endereçamento, tamanho de palavras e organização lógica.
2. Arquitetura de hardware – componentes físicos: CPU, memória, barramentos, controladores, dispositivos.
3. Microarquitetura – modo como a CPU executa instruções internamente (pipelines, caches, paralelismo, predição de desvios).

Essas três dimensões determinam:

- desempenho do sistema
- escalabilidade
- compatibilidade com softwares
- capacidade de execução paralela
- nível de consumo energético
- segurança nativa da plataforma

Sistemas modernos — desde celulares até supercomputadores — dependem de arquiteturas altamente sofisticadas para lidar com tarefas intensas como computação paralela, inteligência artificial, simulações científicas e processamento de dados em larga escala.

Componentes Fundamentais da Arquitetura

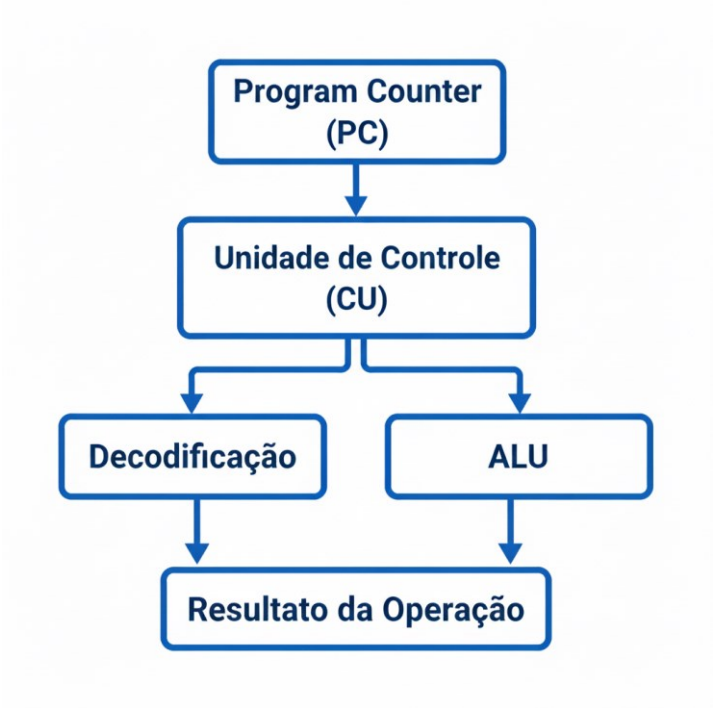
2.2.1 CPU – Unidade Central de Processamento

A CPU realiza o ciclo fundamental:

1. Busca (fetch)
2. Decodificação (decode)
3. Execução (execute)
4. Escrita de resultado (write-back)

A Figura abaixo ilustra um modelo abstrato simplificado:

Figura 4 – CPU Interna (Fluxo de Execução)



A CPU também contém:

- registradores ultrarrápidos
- pipeline para paralelismo interno
- mecanismos de previsão de desvio
- cache embutida (L1, L2 e às vezes L3)

Hierarquia de Memória

A hierarquia existe para equilibrar custo, velocidade e capacidade.

Figura 3 – Hierarquia de Memória (Diagramada)

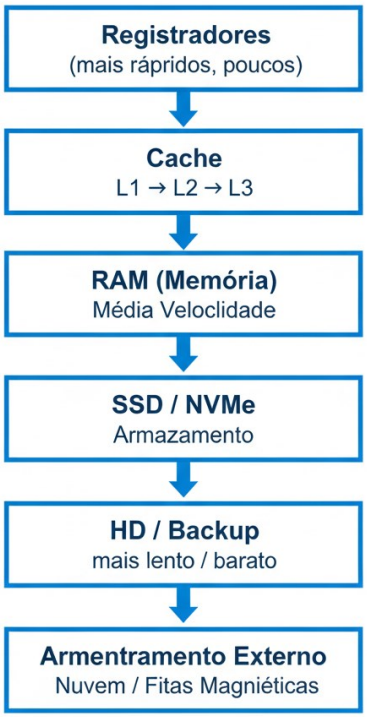


Tabela 1 – Características das Memórias

Nível	Velocidade	Custo	Capacidade	Exemplo
Registradores	Altíssima	Altíssimo	Baixa	PC, SP, R1
Cache L1	Muito alta	Alta	Pequena	Instruções/dados
Cache L2/L3	Alta	Média	Média	Processadores modernos
RAM	Média	Médio	Alta	DDR4, DDR5
SSD/NVMe	Baixa	Baixo	Muito alta	PCIe 4.0/5.0
HD	Muito baixa	Muito baixo	Extremamente alta	Armazenamento

Barramentos

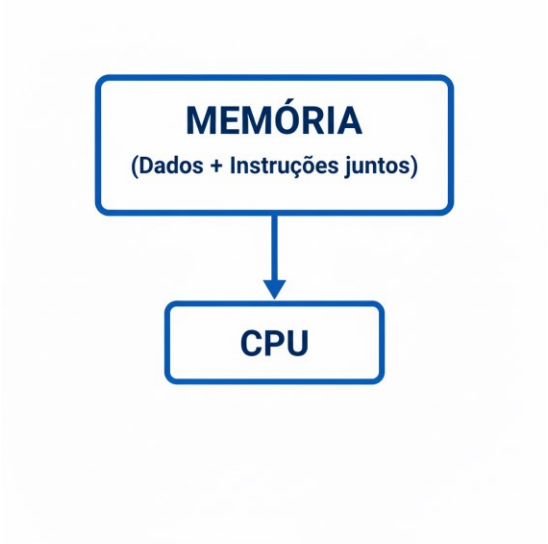
Os barramentos transportam sinais elétricos ou ópticos entre os componentes do computador.
Três tipos principais:

- Barramento de Dados – transporta informações
- Barramento de Endereços – indica localização da operação
- Barramento de Controle – sincroniza operações

O desempenho de um computador depende diretamente da largura dos barramentos e de sua frequência.
Exemplos modernos:

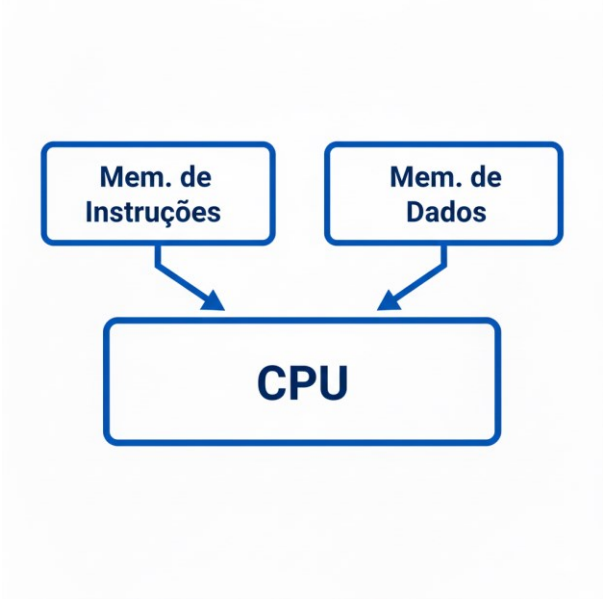
- PCI Express
- USB 4.0
- NVLink (NVIDIA)

Arquiteturas de Processamento
Modelo de Von Neumann
Figura 1 – Arquitetura de Von Neumann



Limitação: gargalo de Von Neumann, onde tudo passa pela mesma via.

Arquitetura
Figura 2 – Arquitetura



Permite paralelismo natural.

CISC vs RISC
Tabela 2 – Comparação CISC x RISC

Característica	CISC	RISC
Nº de instruções	Alto	Baixo
Complexidade	Alta	Baixa
Exemplo	Intel/AMD	ARM

Paralelismo, Multicore e GPUs

A evolução dos processadores ocorreu mais horizontalmente (mais núcleos), pois limites físicos impedem aumento infinito do clock.

Tipos de paralelismo:

- ILP – paralelismo de instruções
- TLP – paralelismo de threads
- DLP – paralelismo de dados (GPUs)

GPUs possuem milhares de núcleos pequenos especializados em operações simultâneas.

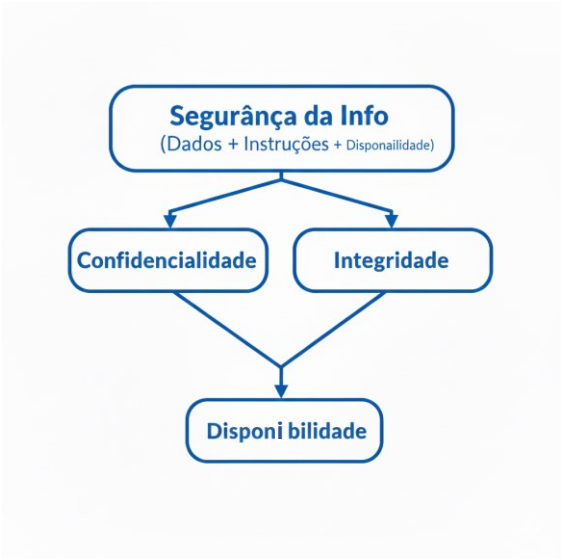
Usos:

- IA
- criptografia
- modelagem climática
- big data

5. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Os sistemas modernos precisam ser resilientes. A segurança da informação se apoia no modelo CIA:

Figura 5 – Modelo CIA



Confidencialidade

Evita acesso não autorizado.

Mecanismos:

- criptografia

- controle de acesso
- autenticação forte
- segregação de funções

Integridade
Garante que dados não sejam alterados de maneira indevida.
Ferramentas:
- hash (SHA-256)
- assinaturas digitais
- blockchain
- auditoria de logs

Disponibilidade
Mantém sistemas operacionais mesmo sob ataque.
Soluções:
- redundância
- balanceamento de carga
- backups
- mitigação de DDoS

6. MECANISMOS E AMEAÇAS

Autenticação e Autorização
Métodos:
- senhas
- biometria
- tokens
- autenticação multifator
- RBAC e ABAC

Criptografia
Figura 6 – Criptografia Assimétrica (RSA)

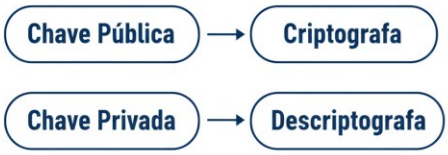


Tabela 3 – Comparação de Criptografia

Tipo	Chaves	Velocidade
Simétrica	1	Rápida
Assimétrica	2	Lenta
Hash	0	Muito rápida

Ameaças Modernas

Tabela 4 – Ameaças e Contramedidas

Ataque	Descrição	Defesa
Phishing	Engenharia social	Educação
Ransomware	Sequestro	Backup
SQL Injection	Falha em query	Prepared statements
MITM	Interceptação	TLS/SSL

7. APLICAÇÕES PRÁTICAS

Integração entre arquitetura e segurança é essencial em:

- datacenters
- sistemas embarcados
- IoT
- nuvem
- redes corporativas
- defesa cibernética
- sistemas críticos (hospitais, energia, transporte)

8. CONCLUSÃO

A arquitetura computacional e a segurança da informação, quando estudadas de forma integrada, proporcionam uma visão holística dos sistemas digitais. Profissionais capazes de compreender hardware e segurança conjuntamente possuem vantagem significativa na construção de sistemas modernos, eficientes e resilientes. Em um mundo hiperconectado, com dispositivos inteligentes e ataques cibernéticos cada vez mais sofisticados, esse conhecimento é fundamental para garantir inovação sem comprometer a confiabilidade.

9. REFERÊNCIAS

AMARAL, F. *Internet das Coisas: conceitos e aplicações.* São Paulo: Novatec, 2020.
ZHANG, X. et al. *Structural Health Monitoring: A Review.* Journal of Civil Engineering, 2021.
RAO, S. et al. *Low-cost sensor networks for urban monitoring.* Sensors, 2022.
NIST. *IoT Reference Architecture.* SP 500-325.
BRASIL. Lei nº 13.709/2018 (LGPD).