SISTEMAS COMPUTACIONAIS E SEGURANÇA

IZABELA CARDOSO MOREIRA DOS SANTOS
LUIZ OTÁVIO BARTILHEIRO DE SOUSA
VICTOR GABRIEL MAQUES DIAS

MECANISMOS DE SEGURANÇA:

Betim
2025

IZABELA CARDOSO MOREIRA DOS SANTOS
LUIZ OTÁVIO BARTILHEIRO DE SOUSA
VICTOR GABRIEL MAQUES DIAS

MECANISMOS DE SEGURANÇA

Um estudo sobre como a segurança da informação protege dados, sistemas e pessoas em um mundo cada vez mais conectado.

Orientadora: Charlene Cássia de Resende

Betim
2025

SUMÁRIO

1- Introdução	**3**
2- Fundamentos da segurança – Tríade CIA	**4**
3- Criptografia e autenticação	**7**
4- Defesa em Camadas	**8**
5- Ataques DoS e DDoS	**9**
6- Mecanismos de Defesa Contra DoS e DDoS	**10**
7- Desafios Atuais e Tendências Futuras	**11**
8- Conclusão	**12**
9- Referencias	**13**

1 INTRODUÇÃO

Vivemos em uma era em que os dados são um dos recursos mais valiosos do mundo digital. A segurança da informação tornou-se um dos principais pilares da tecnologia moderna, sendo essencial para proteger pessoas, empresas e governos contra ameaças cibernéticas.

A proteção de informações sensíveis, como dados pessoais, financeiros e corporativos, é indispensável para manter a integridade e a confiabilidade das operações digitais.

O objetivo deste trabalho é apresentar e discutir os principais mecanismos de segurança da informação, explorando seus fundamentos, ferramentas e desafios atuais. Além disso, busca-se demonstrar como a segurança é um processo contínuo e coletivo, que envolve tanto tecnologia quanto conscientização humana.

2 FUNDAMENTOS DA SEGURANÇA – TRIADE CIA

A segurança da informação é sustentada por três princípios fundamentais conhecidos como a **Tríade CIA** — **Confidencialidade (Confidentiality)**, **Integridade (Integrity)** e **Disponibilidade (Availability)**. Esses pilares formam a base de toda política, estratégia e tecnologia voltada à proteção de dados e sistemas em qualquer ambiente computacional.

A compreensão e aplicação equilibrada desses três elementos garantem que as informações mantenham seu **valor, confiabilidade e utilidade**, mesmo diante de falhas, ataques ou erros humanos.

2.1. Confidencialidade

A **confidencialidade** assegura que as informações sejam acessadas apenas por pessoas, sistemas ou processos devidamente autorizados.
Seu principal objetivo é impedir o acesso, a exposição ou o roubo de dados por indivíduos não autorizados.

Para garantir a confidencialidade, são adotadas diversas medidas técnicas e administrativas, como:

- **Criptografia de dados** em trânsito e em repouso (por exemplo, HTTPS, VPNs e discos criptografados);
- **Controle de acesso** por meio de credenciais, permissões e autenticação multifator (MFA);
- **Políticas de segurança e confidencialidade**, que definem quem pode visualizar, alterar ou compartilhar determinados dados;
- **Treinamento de usuários**, reduzindo riscos de engenharia social e vazamento acidental.

2.2. Integridade

A **integridade** garante que as informações permaneçam **corretas, completas e não adulteradas** durante todo o seu ciclo de vida.
Isso significa que, uma vez criados, os dados devem permanecer inalterados, exceto por processos autorizados e documentados.
Para assegurar a integridade, são utilizados mecanismos como:

- **Assinaturas digitais** e **funções hash (MD5, SHA-256)**, que verificam se os dados foram alterados;
- **Controle de versões** em sistemas e bancos de dados, permitindo rastrear modificações;
- **Logs e auditorias**, que registram todas as operações de leitura, escrita ou exclusão realizadas em informações críticas;
- **Checksums** em transmissões de arquivos, que detectam erros de transmissão ou corrupção de dados.

2.3. Disponibilidade

A disponibilidade assegura que os dados, sistemas e serviços estejam acessíveis sempre que forem necessários.
Esse princípio é essencial para o funcionamento contínuo de empresas, governos e instituições que dependem de sistemas digitais.

Medidas para manter a disponibilidade incluem:

- **Redundância de servidores e links de internet** (para evitar pontos únicos de falha);
- **Sistemas de backup e recuperação de desastres**, que permitem restaurar dados rapidamente;
- **Balanceamento de carga**, para distribuir o tráfego e evitar sobrecarga de servidores;
- **Proteção contra-ataques DoS e DDoS**, que buscam interromper o funcionamento de sistemas;
- **Monitoramento proativo**, com alertas automáticos em caso de falhas.

2.4. Equilíbrio entre os Pilares

Embora cada pilar tenha sua função, a verdadeira eficácia da segurança da informação depende do equilíbrio entre confidencialidade, integridade e disponibilidade**.**
Por exemplo, um sistema extremamente restritivo pode garantir confidencialidade, mas comprometer a disponibilidade; por outro lado, um sistema aberto demais pode ser funcional, mas vulnerável.
As organizações devem avaliar seu contexto, riscos e necessidades para aplicar os controles adequados a cada caso.
Esse equilíbrio é o que transforma a segurança da informação em uma prática estratégica, contínua e essencial para a sustentabilidade digital.

3. CRIPTOGRAFIA E AUTENTICAÇÃO

A criptografia é um dos mecanismos mais importantes na proteção da informação. Ela transforma dados legíveis em códigos indecifráveis para quem não possui a chave correta, garantindo confidencialidade e privacidade.
Existem dois tipos principais:

- **Criptografia simétrica:** utiliza a mesma chave para criptografar e descriptografar dados. É rápida, mas exige segurança no compartilhamento da chave.
- **Criptografia assimétrica:** usa um par de chaves — uma pública e uma privada. Muito usada em transações bancárias, comunicações seguras e assinaturas digitais.

A autenticação, por sua vez, confirma a identidade de usuários e sistemas. Pode ser feita por:

- **Senha** (algo que o usuário sabe)
- **Token ou cartão** (algo que o usuário possui)
- **Biometria** (algo que o usuário é)

Métodos modernos, como a **autenticação multifator (MFA)**, combinam duas ou mais formas, reforçando significativamente a segurança.

4. Defesa em Camadas: Firewalls, Redes Seguras e Monitoramento

A defesa em camadas (*Defense in Depth*) é uma abordagem que utiliza múltiplas barreiras de proteção para reduzir riscos e dificultar invasões. Cada camada representa um obstáculo adicional que o atacante precisa ultrapassar, aumentando o tempo e o esforço necessários para um ataque bem-sucedido.

4.1. Principais Componentes

- **Firewalls:** controlam o tráfego entre redes, bloqueando comunicações não autorizadas.
  Tipos comuns incluem:
  - *Firewall de rede:* filtra pacotes com base em portas e protocolos.
  - *Firewall de aplicação (WAF):* protege sites contra-ataques como SQL Injection e XSS.
  - *Next-Generation Firewall (NGFW):* combina inspeção profunda e detecção de intrusão.
- **VPNs (Redes Privadas Virtuais):** criam conexões criptografadas que protegem os dados mesmo em redes públicas, sendo muito utilizadas em ambientes corporativos.
- **IDS e IPS:**
  - O **IDS (Intrusion Detection System)** detecta atividades suspeitas.
  - O **IPS (Intrusion Prevention System)**, além de detectar, bloqueia automaticamente o ataque.
- **Monitoramento e SIEM:** sistemas de *Security Information and Event Management* coletam e analisam logs de servidores, firewalls e redes, permitindo identificar anomalias em tempo real.

4.2. Benefícios

A defesa em camadas traz maior **resiliência**, **reduz o impacto de falhas** e facilita o cumprimento de normas como a **LGPD** e a **ISO/IEC 27001**.
Essa estratégia é considerada uma das mais eficazes na proteção de infraestruturas críticas.

5. Ataques DoS e DDoS: Quando a Internet Vira Arma

Os **ataques de negação de serviço (DoS)** e **negação de serviço distribuído (DDoS)** têm como meta **tornar um sistema indisponível**, sobrecarregando servidores, sites ou aplicações.
Em um ataque DoS, um único computador envia um grande número de requisições falsas. Já o **DDoS** utiliza uma rede de dispositivos infectados (botnet), agindo simultaneamente e tornando o ataque mais potente e difícil de conter.

5.1. Etapas e Tipos

Infecção: o atacante cria uma botnet infectando dispositivos conectados à internet.

Comando: todos os bots são instruídos a atacar o alvo.

Ataque: o servidor é bombardeado com milhões de solicitações simultâneas.

Efeito: lentidão, falhas ou queda completa do serviço.

Principais tipos:

- **Ataques de volume:** exaurem a largura de banda (UDP Flood, ICMP Flood).
- **Ataques de protocolo:** exploram falhas em protocolos (SYN Flood, Ping of Death).
- **Ataques de camada de aplicação:** miram serviços web (HTTP Flood).

5.2. Impactos Reais

Empresas podem perder receitas, reputação e clientes.
Um exemplo marcante foi o ataque contra o **GitHub (2018)**, que atingiu **1,3 Tbps** de tráfego.
Outro caso foi o ataque à empresa **Dyn (2016)**, que derrubou sites como Twitter, Netflix e Spotify.

6. Mecanismos de Defesa Contra DoS e DDoS: Escudos Digitais em Ação

Diante da força desses ataques, surgiram ferramentas específicas para **mitigação e prevenção**, atuando desde a filtragem até a análise de comportamento.

6.1. Principais Técnicas

- **Balanceamento de carga:** divide o tráfego entre múltiplos servidores, evitando sobrecarga.
- **Filtragem e listas negras:** bloqueia IPs suspeitos antes que cheguem ao servidor.
- **CDN (Content Delivery Network):** distribui o conteúdo em servidores globais, absorvendo picos de tráfego.
- **Rate Limiting:** limita o número de requisições por IP em um intervalo de tempo.
- **Soluções anti-DDoS em nuvem:** como Cloudflare, AWS Shield e Akamai, utilizam IA e aprendizado de máquina para detectar anomalias.
- **Redundância e failover:** garantem que o serviço continue ativo mesmo que um servidor falhe.

6.2. Boas Práticas

- Planejar **planos de contingência e resposta a incidentes**.
- Realizar **testes de estresse e simulações** periódicas.
- Manter **monitoramento contínuo e atualização de sistemas**.
- Promover **treinamentos de conscientização** entre colaboradores.

A combinação dessas estratégias forma uma defesa robusta e adaptável, essencial para enfrentar as ameaças atuais.

7. Desafios Atuais e Tendências Futuras

O avanço tecnológico traz novas oportunidades, mas também **novos vetores de ataque**.
A segurança da informação precisa acompanhar a evolução de áreas como **computação em nuvem**, **IoT (Internet das Coisas)** e **inteligência artificial**.

Tendências:

- Segurança em nuvem: provedores estão investindo em criptografia avançada, auditorias e políticas de conformidade.
- Uso de IA na cibersegurança: sistemas inteligentes detectam padrões suspeitos e respondem automaticamente a incidentes.
- Zero Trust Security: modelo que parte do princípio de que nenhum acesso é confiável por padrão, exigindo verificação constante.
- Proteção de dados pessoais: impulsionada por leis como a LGPD, exige políticas rigorosas de privacidade e consentimento.

Essas tendências indicam um futuro em que a segurança será mais automatizada, proativa e descentralizada.

8. Conclusão

A segurança da informação é um pilar indispensável da sociedade digital moderna, sustentando desde transações financeiras até a comunicação entre pessoas, empresas e governos.
Ao longo deste estudo, foi possível compreender que proteger informações não significa apenas instalar softwares ou configurar firewalls, mas sim adotar uma estratégia contínua, integrada e consciente, baseada em princípios sólidos, tecnologias eficazes e cultura organizacional.

A Tríade CIA — Confidencialidade, Integridade e Disponibilidade — forma a base conceitual dessa proteção, orientando o desenvolvimento de políticas, processos e mecanismos que asseguram o valor e a confiabilidade dos dados.
Ferramentas como criptografia, autenticação multifator, firewalls, VPNs, IDS/IPS e sistemas de monitoramento (SIEM) demonstram como a aplicação prática desses conceitos se traduz em camadas reais de defesa.
Ao mesmo tempo, o estudo dos ataques DoS e DDoS e de suas contramedidas revela a constante necessidade de atualização tecnológica e preparação para incidentes de alta complexidade.

Vivemos em um cenário onde a quantidade de dados cresce exponencialmente, e com ela, aumentam também as ameaças digitais.
A adoção de modelos como o Zero Trust, o uso de inteligência artificial na detecção de anomalias e a segurança voltada à nuvem e à IoT representam o futuro da área — um futuro em que a automação e a análise inteligente serão essenciais para garantir respostas rápidas e eficazes.

Por fim, é fundamental reconhecer que a segurança da informação vai além da tecnologia.
Ela depende, sobretudo, de pessoas conscientes, políticas bem estruturadas e comprometimento ético com o uso e a proteção de dados.
A segurança é, portanto, um processo contínuo e coletivo, que deve ser incorporado à cultura organizacional e pessoal como um valor permanente.
Somente assim será possível construir um ambiente digital confiável, resiliente e sustentável, capaz de acompanhar a velocidade das inovações sem abrir brechas para as ameaças do mundo cibernético.

9.REFERÊNCIAS

ANDERSON, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems.* 3. ed. Hoboken: Wiley, 2020.

CERT.br. *Guia de Segurança para Internet.* Disponível em: https://www.cert.br. Acesso em: 03 nov. 2025
.
DIGENALDO, D. *Detecção de ataques DDoS na camada de aplicação: um esquema com aprendizado de máquina.* Instituto Federal da Paraíba, 2023. Disponível em: https://repositorio.ifpb.edu.br. Acesso em: 03 nov. 2025.

ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements.* International Organization for Standardization, 2013.

JOÃO PAULO, C. *Segurança Cibernética: Uma abordagem conceitual com elementos de política nacional.* Escola Superior de Guerra, 2024. Disponível em: https://repositorio.esg.br. Acesso em: 03 nov. 2025.

STALLINGS, William. *Cryptography and Network Security: Principles and Practice.* 7. ed. Boston: Pearson, 2017.