UNIVERSIDADE REGIONAL DE BLUMENAU

CÂMPUS 1

CIÊNCIA DA COMPUTAÇÃO

NICOLE BRUCH E VEYDA CRISTINA BARBOSA

SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

BLUMENAU

2025

NICOLE BRUCH E VEYDA CRISTINA BARBOSA

SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Projeto de Pesquisa apresentado ao Curso de Ciência da Computação da Universidade Regional de Blumenau para aprovação na disciplina Ciência e Pesquisa.

Orientador(a): Adolfo Ramos Lamar

BLUMENAU

2025

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CIA	Confidencialidade, Integridade e Disponibilidade
VPN	Virtual Private Network
DDoS	Distributed Denial of Service

SUMÁRIO

1 INTRODUÇÃO

A segurança da informação e a cibersegurança são fundamentais na era digital. Com o aumento da dependência da tecnologia, garantir a proteção de dados e sistemas tornou-se um desafio constante. Atualmente, empresas e indivíduos armazenam grandes quantidades de informações sensíveis em ambientes digitais, tornando-os alvos de criminosos virtuais. O vazamento ou roubo de dados pode resultar em prejuízos financeiros, danos à reputação e até mesmo comprometimento da segurança nacional. Os ataques cibernéticos têm crescido exponencialmente, afetando setores públicos e privados. Por isso, este estudo tem como objetivo explorar conceitos essenciais, identificar ameaças comuns e analisar estratégias eficazes para assegurar a segurança da informação, proporcionando maior conscientização e prevenção contra ameaças digitais.

1.1 OBJETIVOS

Analisar o impacto da segurança da informação e da cibersegurança na proteção de dados e sistemas computacionais, identificando ameaças e propondo soluções eficazes para redução de riscos.

1.1.1 Objetivo geral

Analisar o impacto da segurança da informação e da cibersegurança na proteção de dados e sistemas computacionais, identificando ameaças e propondo soluções eficazes para redução de riscos.

1.1.2 Objetivos específicos

Os objetivos específicos são:

a) Identificar as principais ameaças cibernéticas e seus impactos sobre indivíduos e organizações;

b) Avaliar as estratégias de defesa e proteção mais eficazes e suas aplicações;

c) Propor recomendações para mitigar ataques cibernéticos e melhorar as práticas de segurança.

1.2 JUSTIFICATIVA

Diante do aumento dos crimes digitais e do impacto da exposição de dados, é imprescindível investir em estratégias de segurança da informação. Empresas e indivíduos devem estar preparados para enfrentar desafios e minimizar riscos. O prejuízo causado por ataques cibernéticos pode ser devastador, atingindo desde pequenas empresas até grandes corporações e governos. A implementação de medidas preventivas reduz a vulnerabilidade a ataques e protege dados sensíveis. Além disso, este estudo busca contribuir para o aprimoramento das políticas de segurança digital, promovendo boas práticas e conscientização sobre o tema.

2 REFERENCIAL TEÓRICO

A segurança da informação e a cibersegurança são áreas que evoluem constantemente devido ao avanço das tecnologias e ao surgimento de novas ameaças. Para compreender o contexto atual, é essencial explorar seus conceitos fundamentais, as ameaças existentes e as principais estratégias de defesa adotadas por organizações e indivíduos.

2.1 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

A segurança da informação busca garantir a confidencialidade, integridade e disponibilidade dos dados (ABNT, 2024). Esses três pilares são essenciais para assegurar que informações sensíveis permaneçam protegidas contra acessos não autorizados, corrupção e indisponibilidade. Já a cibersegurança está relacionada à proteção contra ataques digitais, abrangendo um conjunto de técnicas e ferramentas utilizadas para defender redes, dispositivos e sistemas de informação.

A seguir, os Pilares onde trazem Conceitos de Segurança:

Quadro 1 – Pilares de Segurança da Informação e Cibersegurança

PILAR	DESCRIÇÃO	IMPORTÂNCIA
Confiabilidade	Garante que apenas pessoas autorizadas tenham acesso às informações.	Protege dados sensíveis contra acessos indevidos.
Integridade	Assegura que os dados não sejam alterados sem autorização.	Evita corrupção e manipulação maliciosa de informações.
Disponibilidade	Garante que os dados e sistemas estejam acessíveis sempre que necessário.	Mantém a continuidade das operações e evita prejuízos.

Fonte: Stallings (2019)

2.2 PRINCIPAIS AMEAÇAS CIBERNÉTICAS

As principais ameaças incluem malware, ransomware, phishing, ataques DDoS e vulnerabilidades em software. O malware, por exemplo, é um software malicioso que pode se infiltrar em sistemas para roubar informações, danificar arquivos ou espionar atividades. O phishing é uma tática utilizada para enganar usuários e obter dados sensíveis, como senhas e informações bancárias. Essas ameaças podem causar danos significativos, comprometendo a segurança das informações e a confiabilidade de sistemas.

A seguir, o exemplo de Ameaças Cibernéticas:

Quadro 2 – Tipos de Ameaças Cibernéticas

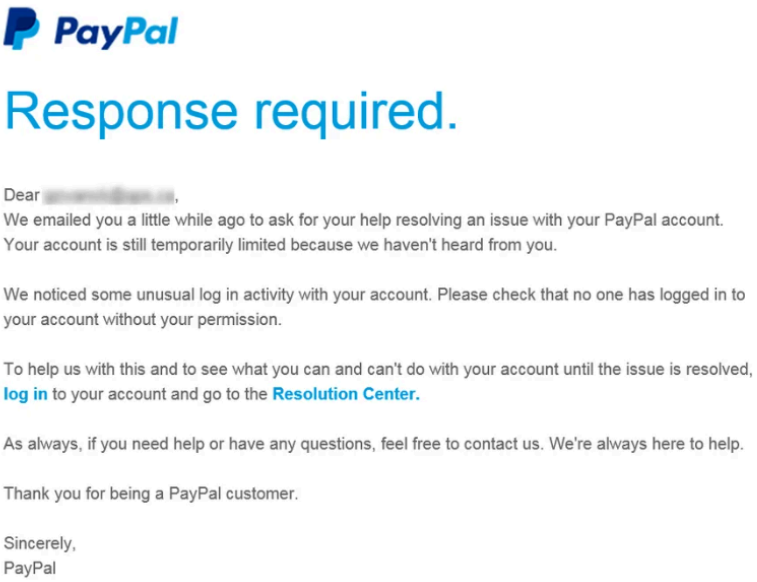
TIPO DE AMEAÇA	DESCRIÇÃO	OBJETIVO	EXEMPLO
Malware	Software malicioso que se infiltra em sistemas.	Roubar/danificar dados.	Trojan.
Phishing	Engana usuários para obter informações sensíveis.	Roubo de credenciais.	Falsos e-mails de bancos.
DDoS	Sobrecarga de servidores com múltiplos acessos.	Derrubar serviços.	Ataque massivo e site de e-commerce.
Ransomware	Software que criptografa dados e exige resgate.	Extorquir dinheiro da vítima.	WannaCry, Cryptolocker

Fonte: Bravo Tecnologia (2024)

Figura 1 – Malware Trojan

Fonte: Kelvin Zimmer (2023)

Figura 2 - Phishing Scam



PayPal

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

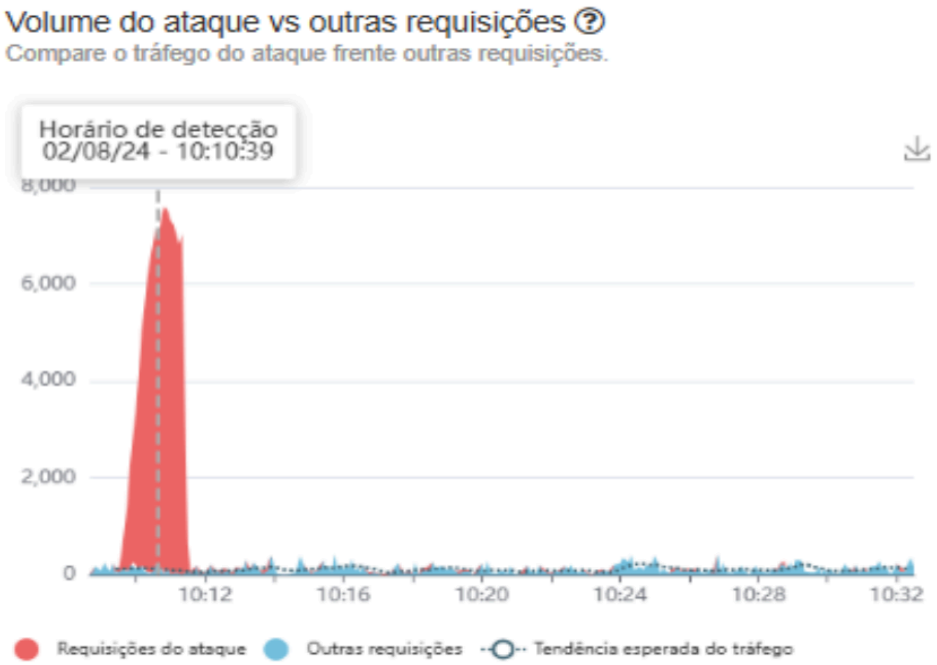
As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

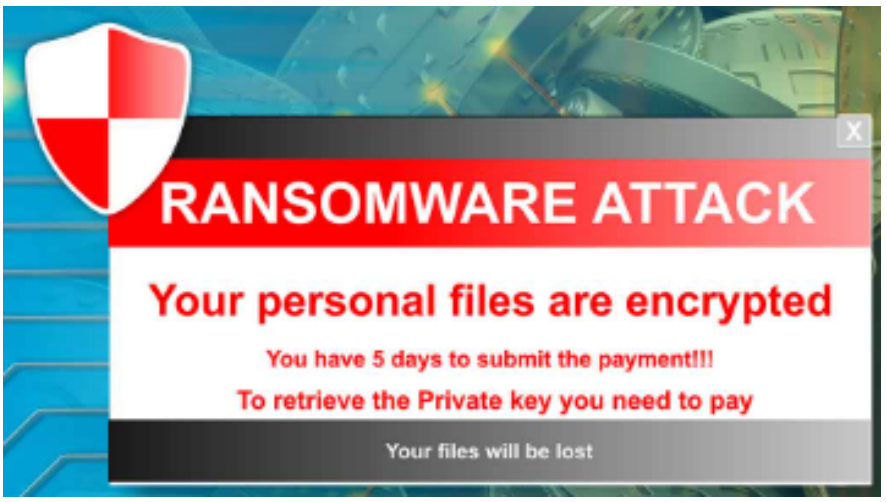
Fonte: Community Bank & Trust (2025)

Figura 3 - Ataque DDoS Visualizado



Fonte: Sectigo Store (2025)

Figura 4 – Ransomware



Fonte: Infosec (2021)

2.3 ESTRATÉGIAS DE PROTEÇÃO

O uso de firewalls, criptografia, antivírus, autenticação multifator e VPNs são formas eficazes de defesa. A educação dos usuários também é essencial, pois muitas vulnerabilidades são exploradas devido a erros humanos. A seguir, o exemplo de uma tabela:

Tabela 1 – Estratégias de Defesa em Cibersegurança

ESTRATÉGIA	DESCRIÇÃO
Firewalls	Controlam o tráfego de rede, bloqueando acessos não autorizados.
Criptografia	Protege dados convertendo-os em um formato ilegível sem a chave certa.
Antivírus	Detecta e remove softwares maliciosos do sistema.
Autenticação Multifator	Requer mais de um fator de autenticação para acesso.
VPN (Rede Privada Virtual)	Cria um canal seguro de comunicação pela internet.

Fonte: Stallings (2022)

Legenda: Medidas fundamentais para garantir a segurança da informação e proteção contra ataques cibernéticos.

Notas: A implementação combinada dessas estratégias reduz significativamente os riscos de invasões e vazamento de dados.

1 METODOLOGIA

A pesquisa será baseada em revisão bibliográfica e análise de estudos de caso sobre cibersegurança.

2 RECURSOS

Serão utilizados artigos acadêmicos, relatórios de segurança, softwares de proteção e materiais didáticos.

3 CRONOGRAMA

A pesquisa será realizada ao longo do mês de abril, com revisões periódicas.

ETAPA	ATIVIDADE	PRAZO
1	Revisão bibliográfica	1 mês
2	Análise de ameaças e soluções	1 semana
3	Escrita e revisão do trabalho	2 semanas
4	Apresentação final	1 semana

REFERÊNCIAS

ABNT. *NBR 14724: informação e documentação: trabalhos acadêmicos: apresentação*. 4. ed. Rio de Janeiro: ABNT, 2024.

BARROS, J. *Segurança digital e suas implicações*. São Paulo: Editora Tech, 2022.

BRAVO TECNOLOGIA. *Tipos de ameaças cibernéticas: como se proteger com a segurança cibernética*. São Paulo: Bravo Tecnologia, 2024.

COMMUNITY BANK & TRUST. *How to spot a phishing scam*. Waco: CBT Bank, 2025.

GOCACHE. *Threat Hub – ataques cibernéticos*. São Paulo: GoCache, 2025.

SILVA, M. *Cibersegurança no mundo corporativo*. Rio de Janeiro: Digital Security, 2023.

STALLINGS, W. *Segurança em redes*. São Paulo: Pearson, 2019/2022.

APÊNDICE A – Checklist de Boas Práticas

Para garantir a segurança da informação no ambiente digital, é essencial seguir algumas boas práticas recomendadas. Entre elas, destacam-se o uso de senhas fortes, a atualização regular dos sistemas, a realização de backups periódicos e a implementação de autenticação multifator. Essas medidas simples, mas eficazes, ajudam a reduzir significativamente os riscos cibernéticos e a proteger os dados de usuários e organizações.

ANEXO A – Política de Segurança

A Política de Segurança da Informação (PSI) define as regras que a organização deve seguir para proteger seus dados e sistemas. Isso inclui controlar quem pode acessar informações sensíveis, garantindo que apenas pessoas autorizadas tenham esse acesso, e exigir o uso de senhas fortes e autenticação multifatorial para aumentar a segurança.

A organização também deve realizar auditorias regulares e monitorar continuamente os sistemas para garantir que tudo esteja conforme as políticas. Os colaboradores precisam ser treinados de forma contínua para se manterem atualizados sobre as melhores práticas de segurança. Além disso, é essencial fazer backups frequentes e manter os sistemas sempre atualizados com patches de segurança, evitando assim vulnerabilidades.