Relatório de Visão de Futuro

Resumo Executivo – 2026

Comitê Técnico de Cibersegurança

RNP

SUMÁRIO

Resumo

A cibersegurança tornou-se um elemento central para a operação de infraestruturas digitais modernas, especialmente em ambientes acadêmicos e de pesquisa. O avanço acelerado das tecnologias digitais amplia tanto as oportunidades quanto os riscos, exigindo respostas estratégicas coordenadas. Este relatório apresenta uma visão consolidada das principais tendências em cibersegurança, com foco em três horizontes temporais (curto, médio e longo prazo), destacando oportunidades para pesquisa, desenvolvimento e inovação. Também evidencia desafios estruturais, como a escassez de profissionais qualificados e a necessidade de maior coordenação institucional no Brasil.

Panorama Atual

Nos últimos anos diversos desafios têm sido discutidos na área de cibersegurança e demandam a atenção para que ações estruturantes sejam desenvolvidas. Alguns dos principais pontos discutidos no contexto do Comitê Técnico de Cibersegurança são:

- Crescente uso de Inteligência Artificial (IA), especialmente aprendizado de máquina, em soluções de segurança;
- Aumento da importância da proteção de dados, privacidade e governança;
- Emergência de novas ameaças associadas a tecnologias como IA generativa, sistemas autônomos e computação quântica;
- Necessidade urgente de formação de profissionais em cibersegurança;
- Oportunidade de desenvolvimento de serviços avançados de segurança para instituições conectadas à RNP.

Cenário Tecnológico

O ambiente digital atual é caracterizado por alta conectividade, uso intensivo de dados e crescente dependência de sistemas distribuídos. Esse cenário aumenta a superfície de ataque e torna os sistemas mais vulneráveis. A análise de publicações científicas recentes (2020–2024) mostra forte crescimento de temas como:

- Aprendizado de máquina aplicado à segurança;
- Privacidade e proteção de dados;
- Criptografia e técnicas avançadas de proteção;
- Detecção de ataques e análise automatizada.

Observa-se também a transição da pesquisa para aplicações práticas, especialmente na integração entre IA e cibersegurança.

Cenário Nacional

No Brasil, houve avanços relevantes na estruturação da área, incluindo:

- Criação da Política Nacional de Cibersegurança;
- Atuação crescente de órgãos reguladores;
- Expansão de programas de formação, como iniciativas educacionais em larga escala
- Surgimento de centros de competência.

Apesar disso, persistem desafios importantes:

- Déficit significativo de profissionais qualificados;
- Baixa produção de patentes e software;
- Necessidade de maior coordenação institucional;
- Fragmentação dos esforços de pesquisa.

Cenário Internacional

Internacionalmente, observa-se forte investimento em:

- Inteligência Artificial aplicada à segurança;
- Proteção de infraestruturas críticas;
- Tecnologias emergentes (5G/6G, sistemas autônomos);
- Compartilhamento de dados e colaboração entre instituições;
- Regulamentação e governança da cibersegurança.

Esses movimentos indicam um alinhamento global em torno da necessidade de respostas mais automatizadas, integradas e proativas.

Experiências internacionais das *National Research and Education Networks* (NRENs) sugerem que modelos bem-sucedidos de cibersegurança são baseados em colaboração, serviços compartilhados e integração de soluções, reforçando a necessidade de evolução do ecossistema nacional nessa direção. Nesse sentido, recomenda-se:

- Estruturar comunidades nacionais e internacionais de cibersegurança para troca de informações e boas práticas;
- Expandir serviços gerenciados de segurança (como SOC, monitoramento e resposta a incidentes);
- Investir em soluções de identidade federada e controle de acesso;
- Promover integração entre segurança de rede, aplicações e usuários;
- Desenvolver programas nacionais e workshops coordenados de capacitação e resposta a incidentes.

Principais Tendências Tecnológicas

A análise consolidada aponta para cinco grandes direções:

1. **Uso intensivo de IA**: tanto para defesa quanto para ataque.
2. **Automação da segurança**: redução da dependência de intervenção humana.
3. **Privacidade e governança**: impulsionadas por regulações e riscos sociais.

4. **Segurança em sistemas complexos**: IoT, cidades inteligentes e sistemas industriais.
5. **Novas fronteiras tecnológicas**: computação quântica e criptografia avançada.

Visão de Futuro

Curto Prazo (0-2 anos)

Principais tendências:

- Uso de grandes modelos de linguagem (*Large Language Models* - LLMs) para análise de segurança;
- Automação de relatórios e análise de incidentes;
- Ferramentas de apoio à análise de código e detecção de vulnerabilidades;
- Consolidação de soluções como *Security Information and Event Management* (SIEM) e *Endpoint Detection and Response* (EDR);
- Expansão de iniciativas de formação profissional.

Oportunidades:

- Desenvolvimento de serviços gerenciados de segurança;
- Uso de IA para análise de logs e eventos;
- Plataformas educacionais escaláveis.

Médio Prazo (2-5 anos)

Principais tendências:

- Adoção de arquiteturas de confiança zero (*zero trust*);
- Uso de IA generativa para automação de políticas e resposta a incidentes;
- Evolução para soluções integradas: *Digital Forensics and Incident Response* (DFIR), *Extended Detection and Response* (XDR) e *Managed Detection and Response* (MDR);
- Maior uso de inteligência de ameaças;
- Computação confidencial;
- Segurança centrada no usuário.

Oportunidades:

- Sistemas de defesa adaptativos;
- Automação de resposta a incidentes;
- Integração de múltiplas fontes de dados de segurança.

Longo Prazo (5-10 anos)

Principais tendências:

- Criptografia pós-quântica;
- Centros de operação de segurança altamente automatizados (SOCs autônomos);
- Uso de IA avançada na gestão de segurança;
- Novos hardwares para detecção antecipada de ataques;
- Segurança integrada em ambientes multidomínio.

Oportunidades:

- Desenvolvimento de tecnologias disruptivas;
- Parcerias estratégicas em pesquisa;
- Liderança em inovação em cibersegurança.

Desafios Estratégicos

Os principais desafios identificados são:

- Escassez de profissionais qualificados;
- Necessidade de integração entre academia, governo e indústria;
- Baixa maturidade em inovação aplicada;
- Evolução constante das ameaças;
- Necessidade de infraestrutura robusta e resiliente

Recomendações

Com base na análise, recomenda-se:

- Investir fortemente em formação e capacitação;
- Desenvolver serviços avançados de cibersegurança para o ecossistema RNP;
- Incentivar pesquisa aplicada com foco em impacto prático;
- Promover integração entre instituições nacionais e internacionais;
- Acompanhar tecnologias emergentes, especialmente IA e computação quântica.

Considerações Finais

A cibersegurança continuará sendo um fator crítico para o desenvolvimento digital do país. O futuro da área será moldado pela combinação de inovação tecnológica, formação de talentos e cooperação institucional. Organizações que investirem de forma estratégica em cibersegurança estarão mais bem posicionadas para enfrentar riscos e aproveitar oportunidades em um cenário digital cada vez mais complexo.

Referências

[1] ACHARYA, Rajeev et al. Quantum error correction below the surface code threshold. 2024. DOI: https://doi.org/10.1038/s41586-024-08449-y.

[2] CISA. Cybersecurity Strategic Plan FY2024-2026. 2024.

[3] ENISA. 2024 Report on the State of Cybersecurity in the Union. 2024.

[4] ENISA. Reframing Cybersecurity Awareness Raising: Exploring the human factor in cybersecurity communication. 2024. Disponível em: https://www.enisa.europa.eu/news/reframing-cybersecurity-awareness-raising-exploring-the-human-factor-in-cybersecurity-communication

[5] ENISA. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. 2019. Disponível em: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

[6] FALCÃO, E.; Silva, F.; Pamplona, C.; Melo, A.; Asadujjaman, A.S.M.; Brito, A. Confidential Kubernetes Deployment Models: Architecture, Security, and Performance Trade-Offs. Appl. Sci. 2025, 15, 10160. https://doi.org/10.3390/app151810160

[7] FORTINET. 2024 Cybersecurity Skills Gap. 2024.

[8] KUCHARAVY, Andrei et al. Large Language Models in Cybersecurity: Threats, Exposure and Mitigation. Springer Cham, 2024.

[9] LERNER, Alberto et al. Rethinking the Switch Architecture for Stateful In-network Computing. In: PROCEEDINGS of the 23rd ACM Workshop on Hot Topics in Networks. Irvine, CA, USA: Association for Computing Machinery, 2024. (HotNets '24), p. 273–281. ISBN 9798400712722. DOI: 10.1145/3696348.3696897. Disponível em: <https://doi.org/10.1145/3696348.3696897>.

[10] RUSSINOVICH, Mark. 2023. Confidential Computing: Elevating Cloud Security and Privacy. Commun. ACM 67, 1 (January 2024), 52–53. https://doi.org/10.1145/3624577

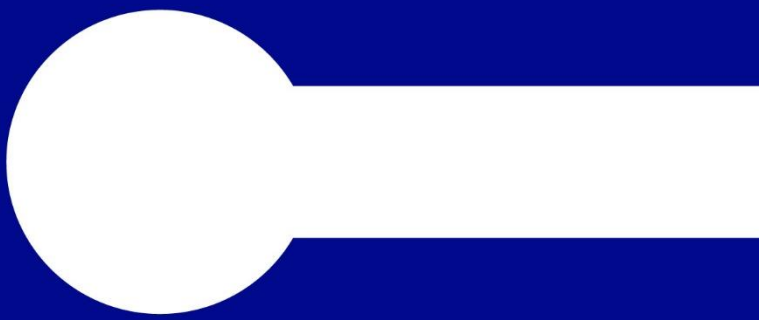
[11] NEVEN, Hartmut. Meet Willow, our state-of-the-art quantum chip. Dez. 2024. https://blog.google/technology/research/google-willow-quantum-chip/.

[12] NIST. NIST Unveils Newly Named Human-Centered Cybersecurity Program. 2023. Disponível em: https://www.nist.gov/blogs/cybersecurity-insights/nist-unveils-newly-named-human-centered-cybersecurity-program

[13] TRIBUNAL DE CONTAS DA UNIÃO. Lista de Alto Risco da Administração Pública Federal. 2024. https://sites.tcu.gov.br/listadealtorisco/index.html.

[14] U.S. BUREAU OF LABOR STATISTICS. Occupational Outlook Handbook - Information Security Analysts. 2025. Disponível em: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[15] ZIMMERMANN, Jamie et al. Approaches to improve preprocessing for Latent Dirichlet Allocation topic modeling. Decision Support Systems, v. 185, p. 114310, 2024. ISSN 0167-9236. DOI: https://doi.org/10.1016/j.dss.2024.114310. Disponível em: https://www.sciencedirect.com/science/article/pii/S016792362400143X.



RNP
MINISTÉRIO DA CULTURA
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DAS COMUNICAÇÕES
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO