CIBERSEGURANÇA COMO POLÍTICA DE ESTADO: DESAFIOS E PERSPECTIVAS PARA A PREVENÇÃO NO BRASIL

Major LUIZ PAULO LOPES DOS SANTOS

RESUMO

A crescente frequência de ataques cibernéticos, evidencia a urgente necessidade de uma cultura sólida de prevenção. Este artigo de opinião defende que a responsabilidade pela prevenção não recai apenas sobre o Estado ou as forças de segurança, mas é uma construção coletiva que envolve governos, instituições, empresas, educadores e cidadãos. A partir de uma abordagem ética, educativa e tecnológica, argumenta-se que a antecipação e a vigilância ativa são fundamentais para proteger vidas, informações e estruturas críticas. Prevenir é mais do que reagir: é investir em educação, promover empatia, estabelecer protocolos claros e adotar tecnologias responsáveis.

Palavras-chave: (Prevenção de ataques, Responsabilidades, Legislação, Cibersegurança, Monitoramento de riscos)

1 INTRODUÇÃO

Vivemos em uma era marcada pela intensa digitalização de processos, ampla interconectividade e crescente dependência de sistemas de informação. Nesse contexto, os ataques cibernéticos — entendidos como ações maliciosas que visam comprometer a confidencialidade, integridade ou disponibilidade de informações ou sistemas — configuram-se como uma das mais graves ameaças à segurança de indivíduos, organizações e do Estado. A prevenção desses ataques assume, portanto, papel estratégico para preservar dados pessoais, infraestrutura crítica, continuidade de serviços públicos e confiança digital.

No Brasil, a responsabilidade macro da prevenção de ataques cibernéticos está formalmente distribuída entre diversos órgãos e esferas de governo. A Política Nacional de Cibersegurança (PNCiber), instituída pelo Decreto nº 12.572, de 4 de agosto de 2025, estabelece diretrizes para a ação coordenada entre União, entes federados, setor privado, sociedade civil e academia no enfrentamento de incidentes cibernéticos (BRASIL, 2025). Adicionalmente, a Política Nacional de Segurança da Informação (PNSI), prevista no mesmo decreto, define princípios, objetivos, estrutura de governança e instrumentos para "cyber security, cyber defense, segurança de infraestruturas críticas de informação e proteção contra vazamento de dados".

A União, por meio de órgãos como o Gabinete de Segurança Institucional da Presidência da República (GSI) e do Comitê Nacional de Cibersegurança (CNCiber), criado pelo Decreto nº 11.856, de 26 de dezembro de 2023, assume o papel de coordenação estratégica nacional (BRASIL, 2023). Aos estados e municípios, dentro de suas competências, cabe implementar medidas de proteção, monitoramento e resposta a incidentes, bem como articular com o setor privado e a sociedade civil.

2 PANORAMA DA CIBERSEGURANÇA NO BRASIL

Nos últimos anos, o Brasil tem passado por uma profunda transformação digital: escolas, hospitais, órgãos públicos, empresas e cidadãos estão cada vez mais conectados à internet ou dependentes de sistemas de informação. Isso significa que a exposição a ataques cibernéticos — ou seja, ações maliciosas que visam comprometer a confidencialidade, integridade ou disponibilidade de dados e sistemas — também tem aumentado significativamente.

Estudo da SOCRadar apontou que, em 2024, foram registrados 372.825 ataques do tipo DDoS (Figura 1) no Brasil (SOCRADAR, 2024). Outro levantamento indica que o Brasil foi responsável por cerca de 19% dos ataques na América Latina entre 2023 e 2024, sendo as instituições governamentais e financeiras os principais alvos (GLOBAL.PTSECURITY, 2024). O setor de educação e pesquisa também registrou crescimento expressivo no número de ataques no primeiro semestre de 2024 (TI INSIDE, 2024).

Figura 1 - Fonte: SOCRADAR
Estatísticas de ataques DDoS no Brasil (2024)

Dados da Autoridade Nacional de Proteção de Dados (ANPD) mostram que os ataques por ransomware representaram a maioria dos incidentes registrados no primeiro semestre de 2023, com 97 dos 163 casos reportados. Entre os fatores que explicam essa vulnerabilidade estão o tamanho da economia brasileira (a nona maior do mundo), a quantidade de dispositivos conectados — com 249 milhões de smartphones, segundo a FGV — e a alta penetração da internet: mais de 142 milhões de brasileiros utilizavam a internet diariamente em 2022, com 92% usando serviços de mensagens e 80% acessando redes sociais (CETIC.BR, 2023).

Além disso, provedores de internet e infraestrutura notaram que o Brasil deixou de ser apenas alvo e passou também a ser origem significativa de ataques. Isso levou à necessidade de instalação de centros de mitigação dentro do território nacional, com foco em setores como finanças, telecomunicações e energia (MENEZES, 2024).

Apesar da criação da PNCiber e de avanços institucionais, especialistas apontam que o Brasil ainda é o segundo país mais vulnerável a ataques cibernéticos no mundo, ficando atrás apenas dos Estados Unidos (MARI, 2023; FORBES, 2023). A soma entre digitalização acelerada e vulnerabilidades estruturais resulta em um cenário urgente para a consolidação de uma cultura de cibersegurança.

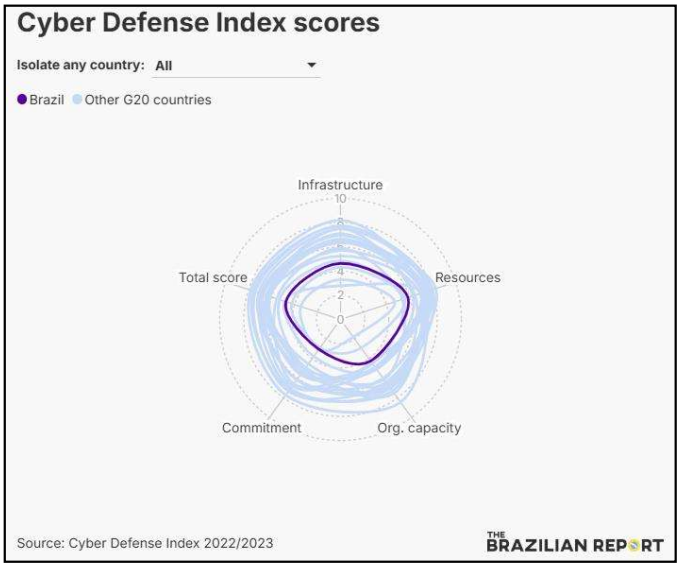

Figura 2 - Fonte: Cyber Defense Index 2022/2023
Índice de Defesa Cibernética: desempenho do Brasil em relação aos demais países do G20.

3. RESPONSABILIDADES E PAPÉIS NO CICLO DE PREVENÇÃO DE ATAQUES CIBERNÉTICOS

Prevenir ataques cibernéticos não significa apenas instalar antivírus ou firewalls. Trata-se de um ciclo abrangente que inclui prever, prevenir, detectar e responder. Cada um desses estágios envolve diferentes atores com responsabilidades distintas.

3.1 UNIÃO (NÍVEL FEDERAL)

A União é responsável por definir a política nacional (como a PNCiber), estabelecer normas e requisitos mínimos, coordenar a cooperação entre os estados, e apoiar com recursos e suporte técnico. Por exemplo, o Gabinete de Segurança Institucional da Presidência da República (GSI-PR) foi apontado como um dos órgãos centrais para esse alinhamento. (BRASIL, 2025)

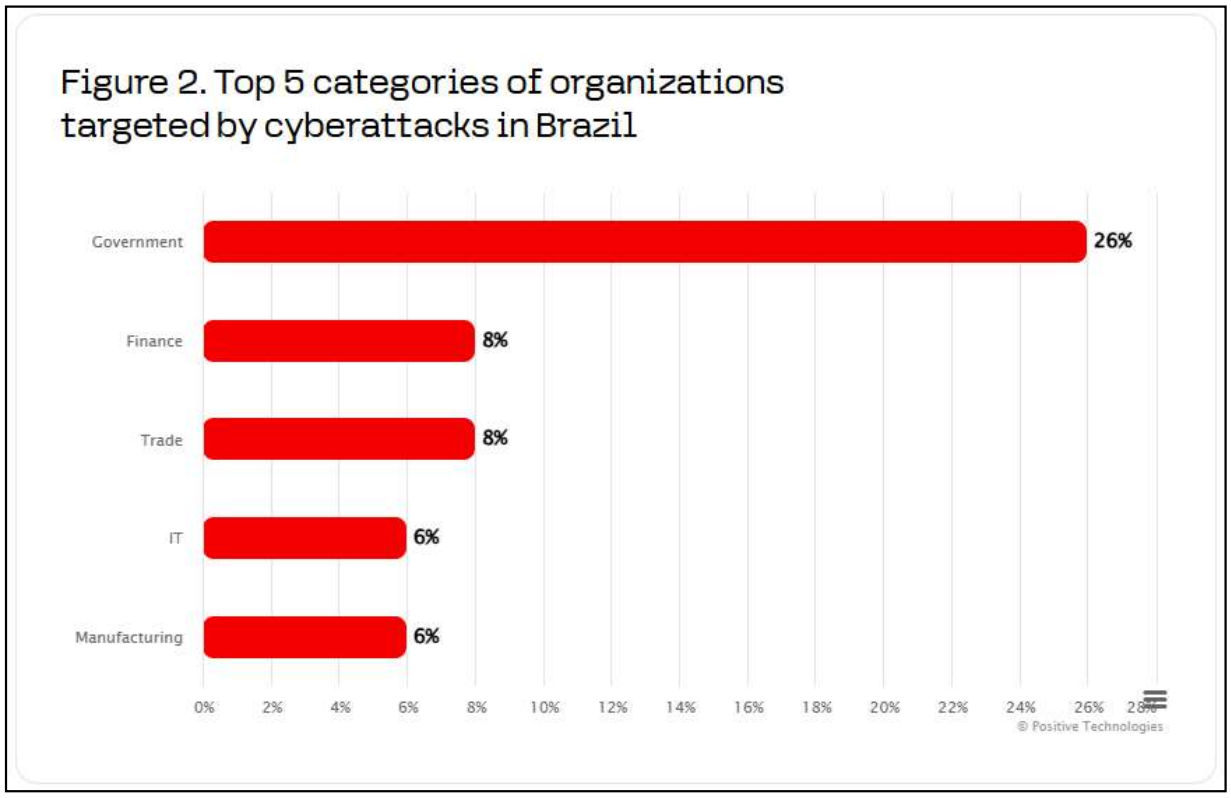

Figura 3 – Fonte: GLOBAL.PTSECURITY
As 5 principais categorias de organizações alvejadas por ataques cibernéticos no Brasil.

O setor público tem ampliado sua digitalização em todas as esferas. A existência de sistemas eletrônicos em saúde, educação e administração, porém, também expõe vulnerabilidades quando não acompanhada de investimentos em segurança da informação. O setor público, por representar 26% (Figura 3) dos ataques registrados, é o mais visado no Brasil (GLOBAL.PTSECURITY, 2024).

3.2 ESTADOS E DISTRITO FEDERAL

Cada estado e o Distrito Federal devem adaptar as diretrizes nacionais à sua realidade, implementar centros de resposta a incidentes (CSIRTs estaduais ou similares), promover a segurança nos sistemas públicos locais (saúde, educação, transporte).

3.3 MUNICÍPIOS

No nível municipal, apesar de menor estrutura em muitos casos, cabe operar parte dos sistemas públicos (escolas, prefeituras, redes municipais), disseminar cultura de segurança digital, articular com empresas locais, sensibilizar a comunidade.

3.4 SETOR PRIVADO E SOCIEDADE CIVIL

Empresas que operam dados sensíveis, provedores de serviços digitais, infraestrutura crítica, têm papel direto: investir em segurança da informação, treinar pessoas, detectar incidentes, cooperar com o setor público. A sociedade civil e os cidadãos individuais também não ficam fora: práticas simples como manter senhas seguras, atualizar softwares, ter cuidado com phishing tudo isso faz parte da prevenção. (CHECK POINT, 2024).

3.5 INTERAÇÃO ENTRE OS NÍVEIS

Não basta que cada ator atue isoladamente: a prevenção eficaz depende da articulação entre União, estados, municípios, setor privado e cidadãos. A PNCiber prevê a articulação entre União, estados, setor privado e sociedade civil (BRASIL, 2023).

Dessa forma, o ciclo de prevenção exige que todos entendam seu papel e colaborem, porque se um dos elos falhar, o conjunto fica vulnerável.

4. CAMINHOS PARA UMA CULTURA NACIONAL DE PREVENÇÃO DE ATAQUES CIBERNÉTICOS

4.1 PRINCIPAIS DESAFIOS

O Brasil enfrenta diversos obstáculos para fortalecer sua postura de cibersegurança:

- Carência de profissionais qualificados em cibersegurança, ainda pouco desenvolvida no país. (BRITO 2024).
- Dependência de tecnologias estrangeiras ou de soluções importadas, o que pode dificultar adaptações à realidade local.
- Baixo nível de maturidade em segurança da informação em muitas organizações, o que amplia a "superfície de ataque".
- Cultura de segurança ainda pouco difundida entre usuários finais, pequenas empresas, administração municipal.
- Integração deficiente entre os diferentes níveis de governo e entre público e privado, o que dificulta resposta coordenada e compartilhamento de informações.

4.2 BOAS PRÁTICAS E INICIATIVAS

Apesar dos desafios, já existem iniciativas que podem ser exemplos:

- Educação contínua: levar a cultura de cibersegurança às escolas, universidades, empresas.
- Simulações de incidentes e exercícios de crise, treinar equipes para "quando acontecer" eles saberem o que fazer.
- Aplicação de frameworks de maturidade (como o NIST Cybersecurity Framework adaptado à realidade brasileira) e adoção de certificações de segurança (ex: ISO/IEC 27001) nas organizações.
- Cooperação público-privado compartilhamento de ameaças, boas práticas, alerta de vulnerabilidades.
- Apoio à inovação e tecnologias nacionais de segurança.

4.3 CAMINHOS FUTUROS

Para consolidar uma cultura eficaz de prevenção de ataques cibernéticos no Brasil, alguns caminhos, muitos que já acontecem, se destacam:

- Fortalecer governança nacional e regional de cibersegurança, tornando mais claros os papéis, responsabilidades, recursos e métricas de desempenho.

- Expandir e profissionalizar a força de trabalho em cibersegurança universidades, cursos técnicos, certificações.
- Promover a cultura de segurança desde as bases desde o cidadão comum, até o gestor público e o diretor de empresa. Quando cada pessoa entender que faz parte do "elenco", a prevenção deixa de ser discurso e vira prática.
- Monitorar e publicar indicadores de maturidade e incidentes transparência e mensuração ajudam a medir o progresso.
- Incentivar alertas colaborativos, resposta a incidentes coordenada, e desenvolvimento de tecnologia nacional de defesa. Ao seguir esses caminhos, o Brasil poderá passar de um país altamente visado a um país mais resiliente e preparado onde prevenir se torna tão natural quanto reagir.

5 CONCLUSÃO

A crescente digitalização da sociedade brasileira, somada à alta exposição a ameaças cibernéticas, impõe a necessidade urgente de adotar uma cultura sólida de prevenção. Conforme defendido ao longo deste artigo, a responsabilidade pela prevenção de ataques cibernéticos não recai exclusivamente sobre o Estado ou sobre especialistas em segurança da informação. Trata-se, antes, de uma construção coletiva e contínua, que exige o engajamento da União, dos entes subnacionais, do setor privado, da academia e, sobretudo, dos cidadãos.

A omissão diante dessa realidade pode acarretar graves consequências, como o comprometimento de serviços públicos essenciais, prejuízos financeiros, perda de confiança digital, violação de direitos fundamentais e até riscos à soberania nacional. A prevenção, portanto, deve ser vista como estratégia de segurança nacional, e não apenas como um requisito técnico.

Assim, propõe-se que, a curto prazo, o país intensifique campanhas de conscientização digital e incentive capacitações em cibersegurança. A médio prazo, é necessário estruturar e equipar centros estaduais e municipais de resposta a incidentes, além de consolidar parcerias público-privadas. A longo prazo, o Brasil precisa investir em pesquisa nacional, desenvolvimento tecnológico autônomo e fortalecer a governança federativa da cibersegurança, com métricas claras, interoperabilidade entre órgãos e políticas sustentáveis de financiamento.

Em um cenário onde a fronteira entre o físico e o digital se dissolve rapidamente, prevenir ataques cibernéticos é mais do que proteger redes — é preservar a integridade da democracia, a continuidade do Estado e a dignidade do cidadão conectado.

6. CONSIDERAÇÕES FINAIS (REFLEXÃO CRÍTICA)

O Brasil encontra-se diante de uma encruzilhada estratégica. De um lado, assume protagonismo no cenário digital latino-americano, com forte base tecnológica, programas de transformação digital e crescente integração ao mercado global. De outro, é o segundo país mais vulnerável do mundo a ataques cibernéticos, segundo a *Forbes* (MARI, 2023).

Esse paradoxo revela um desafio: não basta legislar — é preciso aplicar, fiscalizar e evoluir. Muitas normas brasileiras ainda carecem de aplicação efetiva, articulação entre esferas e tradução em políticas públicas de impacto real. É imprescindível que a inclusão digital venha acompanhada de segurança digital. Deixar isso para depois é correr o risco de transformar avanços em brechas e inovação em fragilidade.

Dessa forma, conclui-se que a construção de um ambiente digital seguro no Brasil exige mais do que tecnologia: exige vontade política, articulação

institucional, investimento em pessoas e um pacto coletivo pela resiliência cibernética.

Abstract

The increasing frequency of cyberattacks highlights the urgent need for a strong culture of prevention. This opinion article argues that the responsibility for prevention does not lie solely with the State or security forces, but is a collective effort involving governments, institutions, companies, educators, and citizens. From an ethical, educational, and technological perspective, it is argued that anticipation and active monitoring are fundamental to protecting lives, information, and critical infrastructure. Prevention is more than reaction: it means investing in education, promoting empathy, establishing clear protocols, and adopting responsible technologies.

***Keywords**: (Attack prevention, Responsibilities, Legislation, Cybersecurity, Risk monitoring)*

7 REFERÊNCIAS

MATTOS FILHO – Sociedade de Advogados. *Brazil's cybersecurity policy*. São Paulo: Mattos Filho, 5 jan. 2024. Disponível em: https://www.mattosfilho.com.br/en/unico/brazils-cybersecurity-policy. Acesso em: 03 set. 2025.

BRASIL. Decreto nº 12.572, de 4 de agosto de 2025. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da Administração Pública Federal. Diário Oficial da União, Brasília, DF, 5 ago. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Decreto/D12572.htm#art12. Acesso em: 03 set. 2025.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: In.gov, 26 dez. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289. Acesso em: 03 set. 2025.

FGV. "Cyber security in Brazil: challenges and urgent need for action" *CGPC – Centro de Governança de Políticas Públicas* 2024. Disponível em: https://periodicos.fgv.br/cgpc/article/view/90972/86755. Acesso em: 17 out. 2025.

SOCRADAR Cyber Intelligence Inc. *Brazil Threat Landscape Report 2024*. São Paulo: SOCRadar, out. 2024. Disponível em: https://socradar.io/wp-content/uploads/2024/10/SOCRadar-Brazil-Threat-Landscape-Report-2024.pdf. Acesso em: 08 out. 2025.

Global PTSecurity. *Cybersecurity Threatscape for Latin America and the Caribbean 2023-2024*. [S.l.]: PTSecurity, 2024. Disponível em: https://global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-for-latin-america-and-the-caribbean-2023-2024. Acesso em: 08 out. 2025.

TI Inside. "Cyber attacks increase by around 70% in Brazil in one year". Redação TC Inside, 17 jul. 2024. Disponível em: https://tiinside.com.br/en/17/07/2024/ataques-ciberneticos-crescem-cerca-de-70-no-brasil-em-um-ano/. Acesso em: 28 ago. 2025.

MENEZES, Fabiane Ziolla. "Why is Brazil a top target for cyberattacks?". *The Brazilian Report*, 6 mar. 2024. Disponível em: https://newsletters.brazilian.report/p/brazil-top-target-cyberattacks. Acesso em: 16 out. 2025.

MARI, Angelica. "Brazil Is The World's Second Most Vulnerable Country To Cyberattacks". *Forbes*, 27 set. 2023. Disponível em:

https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-is-the-worlds-second-most-vulnerable-country-to-cyberattacks/. Acesso em: 01 ago. 2025.

CHECK POINT SOFTWARE TECHNOLOGIES. *Cyber Security Report 2024*. [s.l.], out. 2024. Disponível em: https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024-3a0a. Acesso em: 02 out. 2025.

BRITO, Flavia. "Cybersecurity in Brazil: Challenges and Urgent Need for Action", Associação Brasileira das Empresas de Software (ABES), s.d. Disponível em: https://abes.org.br/en/seguranca-cibernetica-no-brasil-desafios-e-necessidades-urgentes-de-acao. Acesso em: 02 out. 2025.