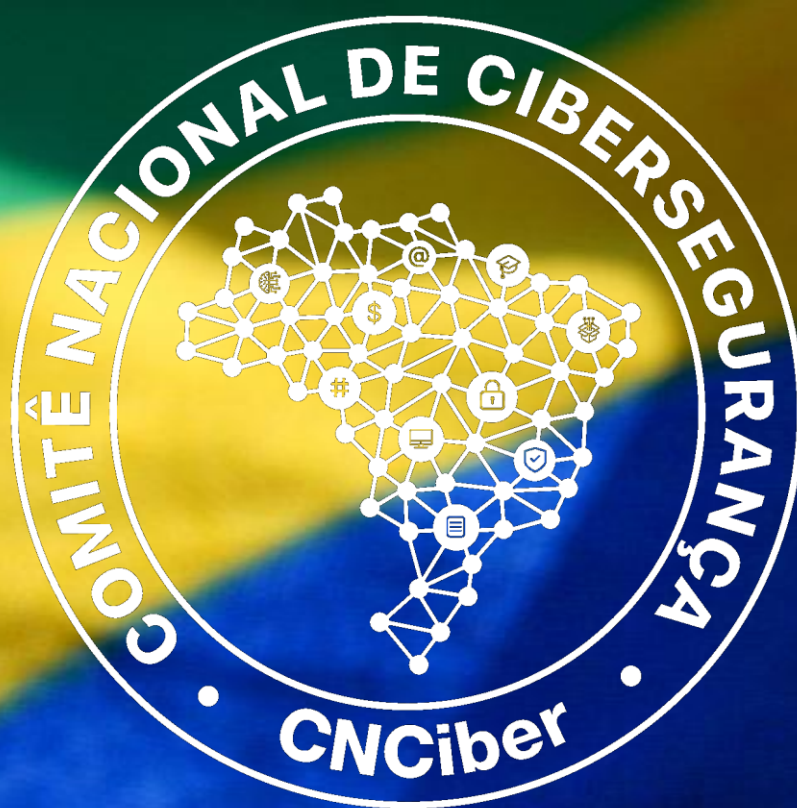




MLCiber (Senado)

+

LGCiber (CNCiber)

**Urgência e Relevância de uma
Política de Estado**

Brasília, 30/06/26





A Escolha pela Soberania Digital

“A soberania digital é composta por três dimensões: autodeterminação, **cibersegurança e capacidade econômica.”**

(TCU, LAR 2024, p. 225, grifos adicionados)

“Ainda em 2026**, será reforçada a **governança da cibersegurança**, com novos mecanismos de regulação, fiscalização, coordenação e controle, essenciais para garantir a confiança digital e o crescimento econômico.”**

(Mensagem Presidencial ao Congresso 2026, p. 762, grifos adicionados)



Sumário Executivo: A Urgência de uma Política de Estado



O Problema

Paradoxo Digital

Melhor Governo Digital

12.750+ Serviços Digitais

4.600 Federais

~8.200 Estaduais)

178 milhões de usuários Gov.Br



Alto Risco TCU (2022 e 2024)

1 dos 3 mais atacados no mundo



A Solução

Melhoria da
**Governança da
Cibersegurança
Nacional** (regulação,
fiscalização,
coordenação e
controle).



O Benefício

**Proteção da
economia digital** pela
prevenção de perdas
significativas,
segurança jurídica
para investimentos,
**proteção do cidadão
e de SEICs** e elevação
da **soberania digital
nacional**.

O Custo da Insegurança



Saúde

INCA (Jan 2024) Radioterapia paralisada, consultas manuais.

IPEN (Mar 2025) Produção de radiofármacos interrompida, 5.000 pacientes/dia com tratamento interrompido.



Finanças

PIX (2025) Ataques a cadeias de suprimentos (PSTIs) com prejuízos da ordem de bilhões.

BNB (2026) Prejuízo de 146 milhões



Outros

Misantropi4 (Jun/26)

Desabilitação do serviço de alertas da Defesa Civil e perda de credibilidade

ANTAQ (Jun/2026)

Paralisação de sistemas e serviços por 40 dias



**WEF: prejuízo médio global de 14% do PIB.
No Brasil corresponderia a ~1,8 trilhão em 2025!**

WEF Global Risks Report

	2 Anos	10 Anos
2023	Cibercrime generalizado e insegurança cibernética (8)	Cibercrime generalizado e insegurança cibernética (8)
2024	Insegurança Cibernética (4)	Insegurança Cibernética (8)
2025	Espionagem cibernética e Guerra Cibernética (5)	Espionagem cibernética e Guerra Cibernética (9)
2026	Insegurança cibernética (6)	Insegurança cibernética (8)

“Novas tecnologias mudarão a natureza da ameaça à segurança nacional... Crime cibernético generalizado é o novo elemento na lista dos riscos mais graves.” (WEF, 2023)

Desenvolvimentos Internacionais



Reino Unido

- **2019** – Active Cyber Defense “o ataque é a melhor defesa”
- **Jul/24** – Rei Charles III explicitou a **necessidade de nova lei de ciber-resiliência**
- **Nov/25** – Governo trabalhista enviou nova lei ao Parlamento
- **Dez/25** – *Hot-Line* com a China



Alemanha

- **Jan/26** – MD vai retaliar ciberataques russos
- **Fev/26** – Investimentos bilionários em capacidades forenses e ofensivas



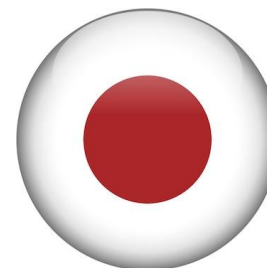
UE

- **2026** – A Diretiva NIS2 (2022) se torna totalmente operacional, incluindo **novos setores e empresas médias**, com **mais alcance**, exigências mais claras e **responsabilização**



França

- **Jan/26** – Pres. Macron lançou nova NSCS
 - “... a cibersegurança tornou-se um pré-requisito para a liberdade. Um requisito vital. Um imperativo estratégico.”
 - *Postura ofensiva*
 - *Aumento significativo de investimentos*



Japão

- **2025** – *National Cybersecurity Office (NCO)*
- **2026** – Entra em vigor o *Active Cyber Defence Act/25*
- **2026** – PM assinou *acordo de cooperação* com o PM do Reino Unido



EUA

- **Jul/23** – US NSCS
 - *Obrigações para a indústria*
 - *Responsabilização de dirigentes*
 - *Consolidação do Defend Forward e do Persistent Engagement*

TCEs & Cibersegurança pelo Mundo (*)

IA



Reino Unido

- AISI + NCSC



França

- INESIA + ANSSI



Itália

- AgID + ACN



EUA

- CISA: IA ↔ CS

TQs



França

- Só *Quantum-Safe* a partir de 2027 (ANSSI)



EUA

- EO 14412: Sensoriamento Quântico até 2027 (DoD) e Quantum-safe até 2031
- EO 14413: Computador Quântico até 2028 (DoE)

(*) Anúncios em Maio-Junho/26!



LGCiber – Agentes Obrigados



Provedores de
**Serviços
Essenciais**



Telecom, Postal
(ANATEL)



Finanças
(BCB, CVM, SUSEP)



Saúde
(ANVISA, MS)



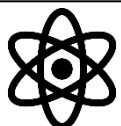
Transportes
(ANAC, ANTT, ANTAQ)



Energia
(ANEEL, ANP)



Operadores de
**Infraestruturas
Críticas**



Nuclear
(ANSN)



Defesa
(MD)



Defesa Civil
(SEDEC/MIDR)



Espaço
(AEB, DCTA/MD)



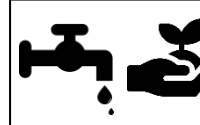
Governo Digital
(SSIC/GSI, SGD/MGI)



**União, Estados e
Municípios** (+100
mil habitantes)



Infras Digitais
(ANATEL, CGI, ITI, ANPD)



Saneamento e M.Amb.
(ANA, IBAMA)



Medicam./Alimentos
(ANVISA, MAPA)



Educação
(MEC)



Segur. Pública e Justiça
(MJSP, MP, CNJ)

Adesão voluntária para os não-obrigados!

Impactos Positivos



Segurança Jurídica

Regras claras e uniformes para o mercado, **harmonização** com a LGPD e com os reguladores setoriais



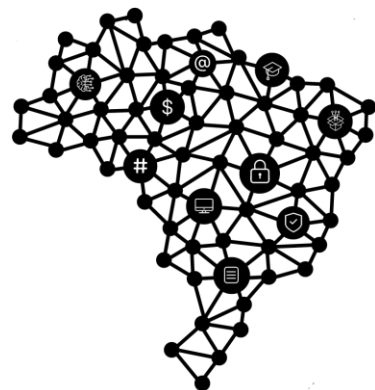
Economia de Dados

Estabilidade regulatória beneficiando a atração de **datacenters**, IA e o **ecossistema de cibersegurança**



Cultura e Educação

Letramento digital e formação de **mão-de-obra qualificada**, pesquisa e **cooperação** internacional

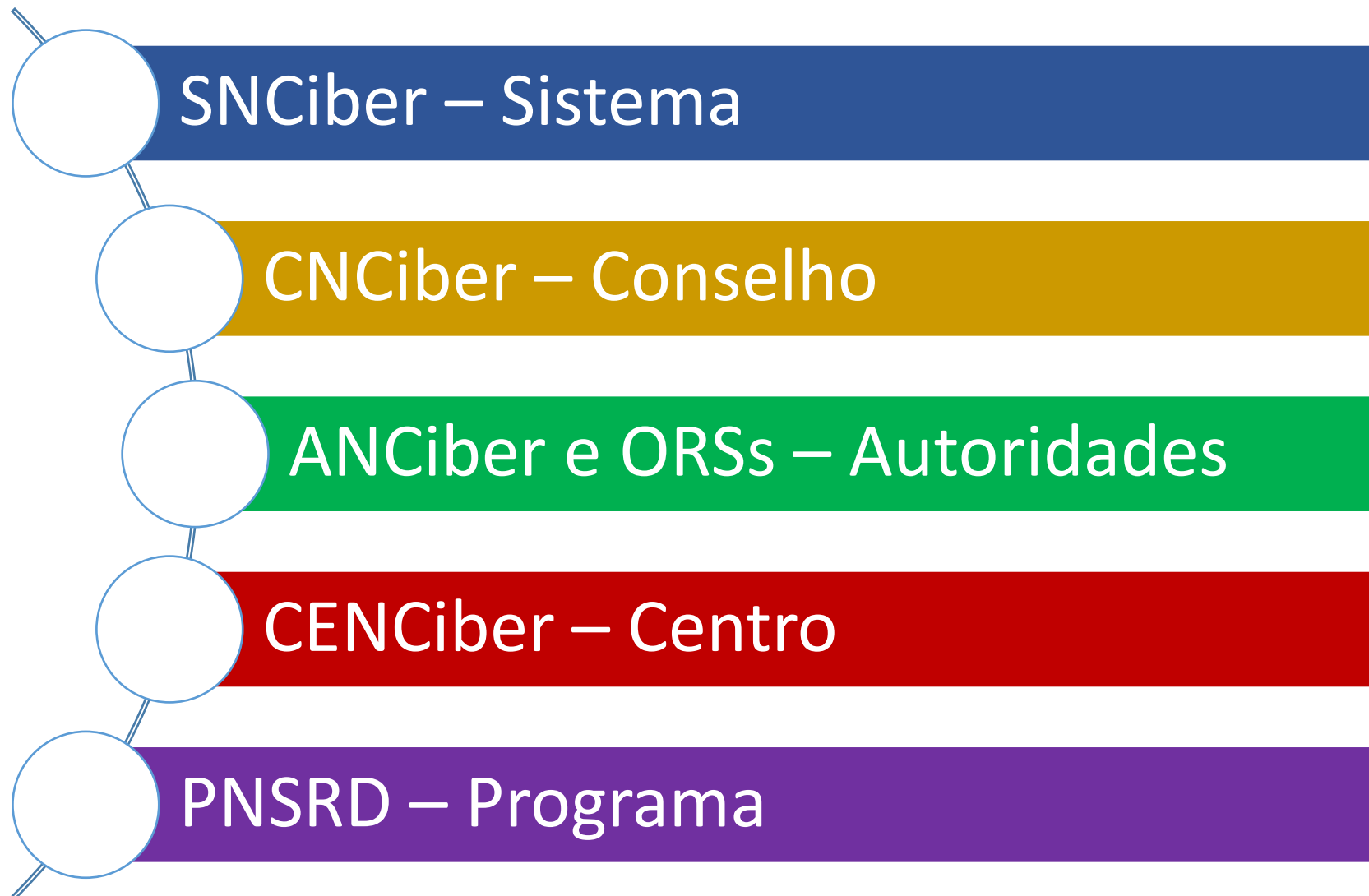


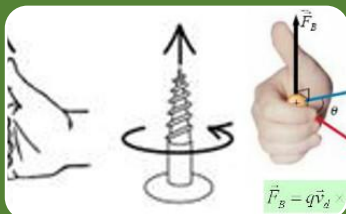
Soberania Nacional

Inclusão do **Brasil na cadeia de valor** global da cibersegurança, **resiliência** operacional e proteção de **segredos de Estado**



Governança





Regulação

- Normas Gerais (“régua mínima”)



Fiscalização

- Cumprimento das normas
- Sancionamento



Coordenação

- Gestão de riscos
- Modelos e padrões
- Cooperação nacional e internacional



Controle

- CENCiber
- Reconhecimento e certificação de produtos e serviços
- Gestão de Crises



Obrigado!

marcelo.malagutti@presidencia.gov.br
cnciber@presidencia.gov.br

