# Projeto de Lei 4752

## A visão da Defesa

Marco Legal da Cibersegurança

Programa Nacional de Segurança e Resiliência Digital

- ✓ Uma excelente iniciativa
- ✓ Preenche lacuna relevante no ordenamento jurídico
- ✓ Alinhada com a tendência mundial
- ✓ Criação de Agência reguladora
- ✓ Cria mecanismo de financiamento da atividade

# Ataques Cibernéticos

Começam normalmente com *motivação financeira*, podem migrar para a busca por *Segredos industriais, segredos de Estado, promover caos social, desmoralização de instituições*.

Se tornam um risco à segurança nacional quando afetam *serviços essenciais* e *infraestruturas críticas*

*Atualmente, fazem parte da doutrina de todos os países do mundo como preparação de uma ação militar*

# Principais Considerações da Defesa sobre o PL 4752

*A separação clara entre cibersegurança e ciberdefesa não é burocrática — é estratégica. Confundí-las compromete tanto a prontidão militar quanto a eficácia civil.*

### 🔐 Cibersegurança e Ciberdefesa

*Há necessidade de ressalvar o papel da Autoridade Nacional de Cibersegurança, separando e definindo o conceito de Ciberdefesa/Defesa Cibernética. Desta forma, é importante incluir* ***"as Forças Armadas observarão as disposições da Lei, respeitadas as especificidades da ciberdefesa"***

### ⚠️ Ambiguidade de Competências

*O texto precisa delimitar com precisão as atribuições do GSI, do MD e dos ministérios setoriais para evitar sobreposição de autoridade em momentos críticos.*

***A Proposta do CNCIber apresenta esta separação***

# Contribuições para o PL 4752

## Compartilhamento de Informações

Cibersegurança e tratamento de incidentes se faz com compartilhamento de informações. **A proposta do CNCIber traz um modelo interessante para garantir esse compartilhamento**, mas que precisa ser aperfeiçoado com a ressalva ao tratamento diferenciado das informações classificadas que exponham vulnerabilidades do Estado e de segurança nacional

## Definição de Critérios de Ativação

O PL precisa tambem estabelecer **indicadores objetivos** — técnicos, políticos e estratégicos — que determinem o acionamento das capacidades militares de defesa cibernética.

**Uma proposta está no proximo slide**

# Critérios de Escalada: Do incidente à Defesa Nacional

*Um dos pontos de possivel aperfeiçoamento do PL 4752 é a definição de **limiares claros de escalada** — ou seja, quais condições determinam a transição de uma resposta civil para o acionamento das capacidades de defesa cibernética das Forças Armadas.*

**Nível 1 - Incidente Técnico (Verde):** Foco em sistemas isolados. Resposta local. Risco controlado

**Nível 2 (Azul) - Incidente de Relevância Nacional,** sem comprometer Infraestruturas Críticas (ICID). Risco Moderado.

**Nível 3 (Amarelo) - Crise Cibernética:** Impacto sistêmico, coordenação interministerial. Risco médio contra a resiliência do Estado.

**Nível 4 (Laranja)- Degradação de ICID:** Ações hostis que degradam serviços essenciais. Risco alto, mobilização de ativos de Defesa.

**Nível 5 (Vermelho) - Ameaça à Soberania Nacional:** Cenário de Ataque de Estado ou sabotagem generalizada. Resposta de Defesa Nacional sob coordenação do Ministério da Defesa/ ComDCiber.

**A ausência de critérios objetivos de escalada no texto atual do PL 4752 pode gerar conflito de competências e atrasos críticos em situações de crise real.**

# Projeto de Lei 4752

Marco Legal da Cibersegurança
Programa Nacional de Segurança e Resiliência Digital

- ✓ Sugestão de aspectos interessantes a serem considerados:
  - ✓ Incluir explicitamente Tecnologias Computacionais Emergentes no projeto
  - ✓ Estimular o Fomento a soluções nacionais
  - ✓ Criação de plataforma neutra para compartilhamento de ameaças

*Integrar para proteger as Infraestruturas Críticas*

# O que a Defesa já está fazendo para apoiar a Ciber resiliência?

*Exercício de Simulação Construtiva e virtual*

Discussão de Problemas Cibernéticos Simulados

Acelera a maturidade das instituições

EXERCÍCIO GUARDIÃO CIBERNÉTICO

COOPERAR - INTEGRAR

**Gera conhecimento não apenas técnico, mas também institucional**

Estimula o Compartilhamento de informações

*Discussão de problemas de impacto estratégico que atinjam serviços essenciais*

# GUARDIÃO CIBERNÉTICO - EVOLUÇÃO

**ESTRATÉGIA NACIONAL DE DEFESA**

"3.6.5 (...) aprimorar a Segurança Cibernética, com ênfase na proteção das Estruturas Críticas."

Dec. nº 11.200 (15 SET 2022)

PLANSIC

**Decreto Nº 11.200, de 15 Set 2022**

Aprova o Plano Nacional de Segurança de Infraestruturas Críticas.

"2.2.5. Envolver, nos exercícios de Guardião Cibernético, setores abordados em Segurança de Infraestruturas Críticas."

## ECG 1.0
## 3 DIAS
23 Organizações
106 Participantes

2018

## EGC 2.0
## 3 DIAS
41 Organizações
215 Participantes

2019

## EGC 3.0
## 3 DIAS
75 Organizações
350 Participantes

2021

## EGC 4.0
## 4 DIAS
120 Organizações
450 Participantes
Hub SP

2022

SP

## EGC 5.0
## 5 DIAS
140 Organizações
600 Participantes
Hub SP

2023

SP

## EGC 6.0
## 5 DIAS
143 Organizações
682 Participantes
Hub SP

2024

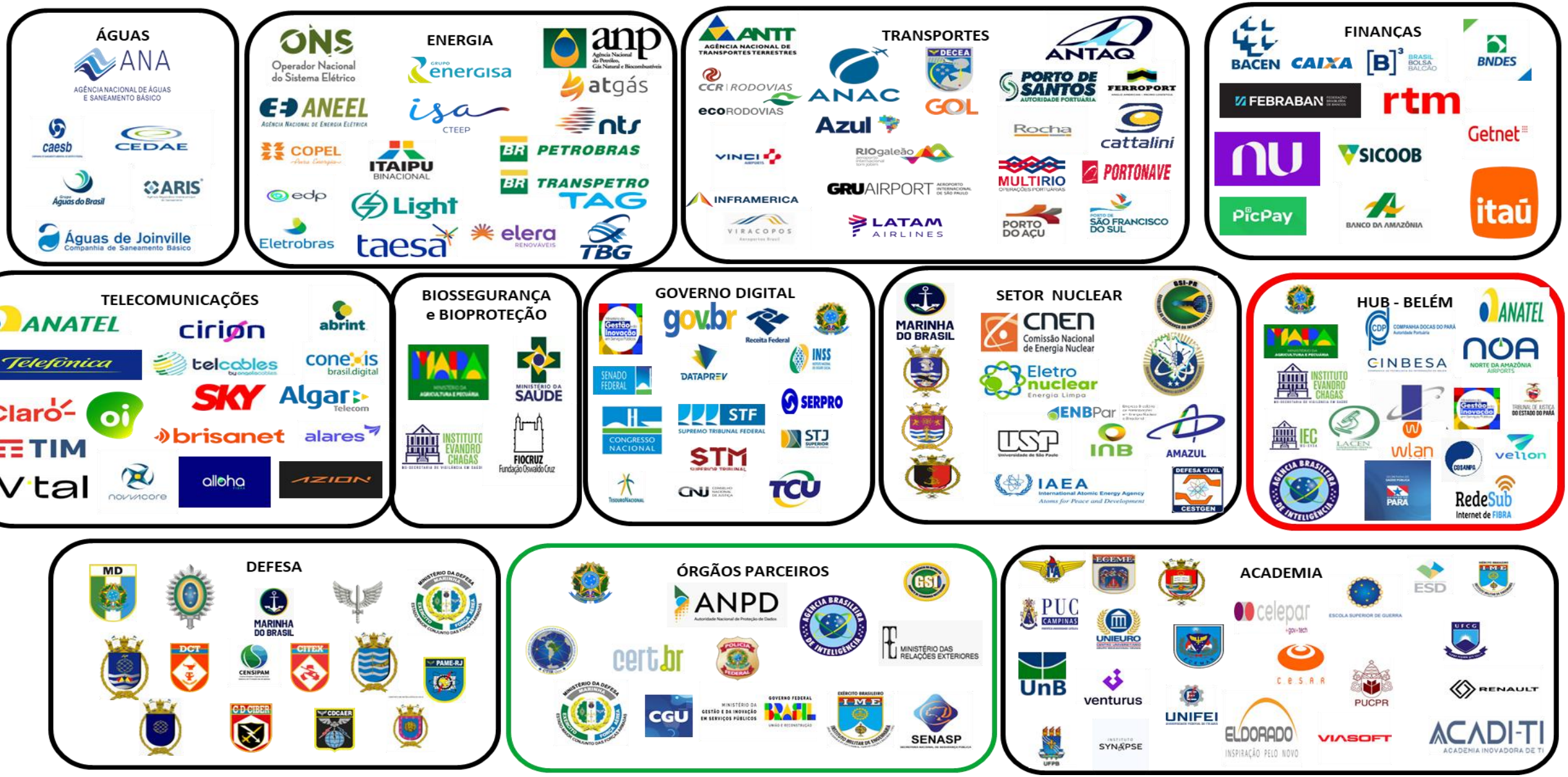
SP

## EGC 7.0
## 5 DIAS
169 Organizações
750+ Participantes
Hub Belém

2025

BELÉM

# 2025 - EGC 7.0 - 169 Organizações / 750 Participantes



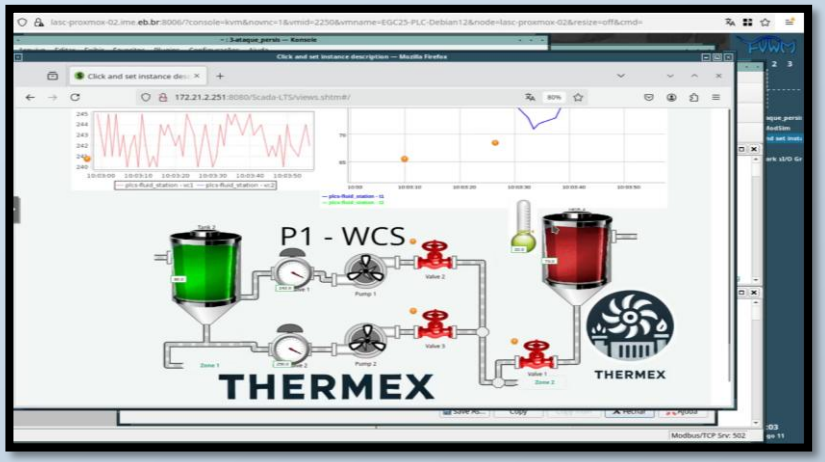

*O maior exercício de Ciber-resiliência do Hemisfério Sul*

**240 Organizações e 2000 Participantes**

# Simulação Virtual

## Sistemas de Controle Industrial customizados por Setor Estratégico

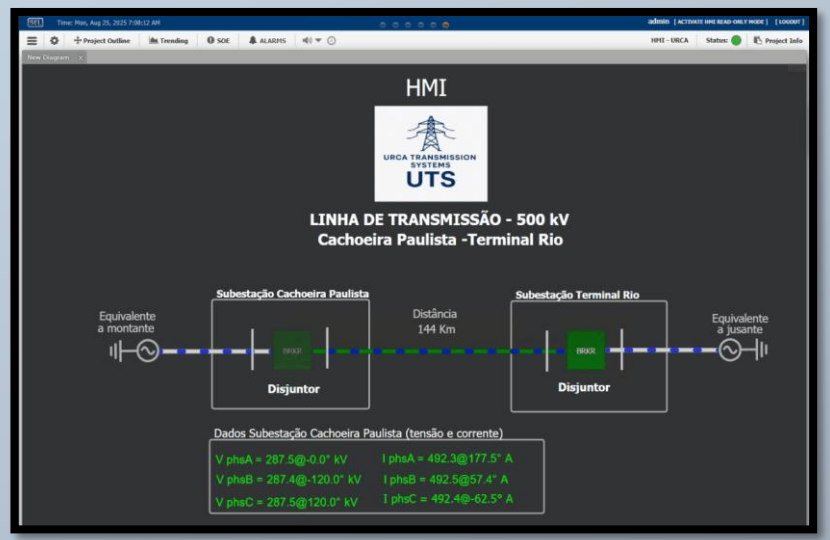
### Setor Defesa – Thermex



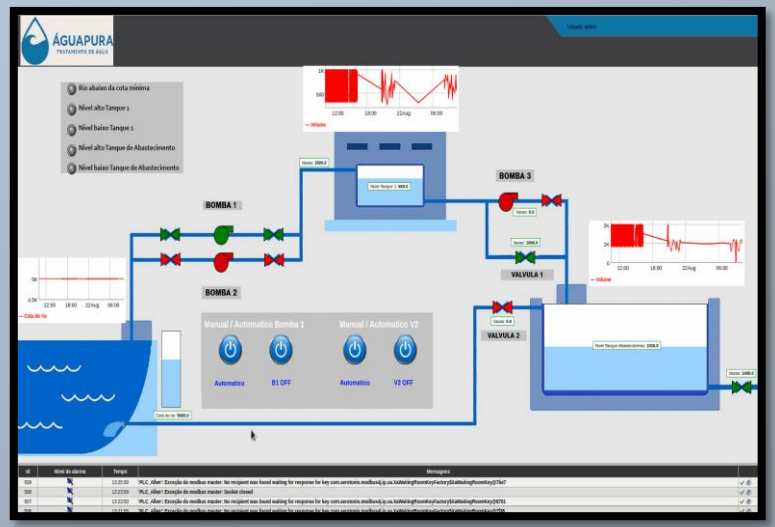

### Setor Defesa – Sistema de Defesa Aérea


### Setor Transportes – C2 Drone

### Setor Energia – Simulador Digital em Tempo Real (RTDS)




### Setor Água, e-Gov, Biossegurança e Bioproteção – Tratamento de Água




### Setor Financeiro e Comunicações – Controle de Temperatura e Baterias de Site e Data Center

# COMANDO DE DEFESA CIBERNÉTICA


- TRABALHO
- COMPETÊNCIA
- PERSISTÊNCIA
- LIDERANÇA