67- DATA-CENTER

Claro. Segue um resumo estruturado da proposta apresentada:

A proposta consiste na criação de um **arcabouço legal e institucional robusto** para garantir a soberania e segurança dos dados brasileiros, dividido em dois pilares principais:

1. Criação da Empresa Brasileira de Dados Soberanos (EBDS)

- **Natureza:** Empresa pública federal vinculada à **Presidência da República**, com personalidade de direito privado para agilidade e flexibilidade.
- **Finalidade Principal:** Implementar, gerir e operar a infraestrutura nacional de data centers estatais, assegurando a soberania, segurança e privacidade dos dados.
- **Atribuições-Chave:**
    - Construir e operar data centers de alta segurança.
    - Prestar serviços de nuvem (IaaS, PaaS, SaaS) para toda a administração pública.
    - Desenvolver pesquisas em segurança cibernética e criptografia.
    - Coordenar respostas a incidentes cibernéticos.
- **Governança Forte (CONAD):** Conselho de Administração com representantes de vários ministérios (Casa Civil, GSI, Defesa, Justiça, etc.) e especialistas, garantindo equilíbrio entre segurança, legalidade e desenvolvimento.
- **Controle Interno Rigoroso:** Criação do COSEA, um comitê com poder de veto para auditoria contínua e investigação de desvios.
- **Regime de Pessoal Híbrido:** Combina a estabilidade do regime estatutário com a flexibilidade da CLT, com processos rigorosos de seleção e monitoramento para todos os funcionários.
- **Sistema Nacional (SINAD):** Cria o SINAD, consolidando a infraestrutura da EBDS como o ambiente preferencial para os dados públicos, com prazo de 5 anos para migração.

2. Lei de Proteção de Dados Soberanos e Segurança Cibernética Nacional

Esta lei complementar estabelece **regras duras e punições exemplares** para proteger os dados.

- **Princípios Fundamentais:** Soberania dos dados, finalidade específica, minimização e transparência controlada.
- **Regras Operacionais "Duras":**
    - **Segurança Física:** Localização secreta, acesso biométrico multifatorial, zonas de exclusão e blindagem contra ataques.
    - **Segurança Lógica:** Sistemas "air-gapped" (isolados) para dados sensíveis, criptografia quântica, múltiplas camadas de defesa e auditoria contínua com IA.
    - **Governança de Pessoal:** Investigação de antecedentes, termo de sigilo perpétuo e monitoramento contínuo.

- **Crimes e Punições Exemplares:**
    - **Divulgação Não Autorizada:** 8 a 20 anos de reclusão. Se para governo estrangeiro, equiparado a **traição nacional** (20 a 30 anos).
    - **Invasão Cibernética:** 10 a 25 anos de reclusão.
    - **Negligência Grosseira:** 3 a 10 anos de reclusão e proibição de exercer cargo.
- **Fiscalização e Aplicação:**
    - Criação de um **Tribunal de Contas de Dados (TCD)** para auditorias, aplicar sanções e julgar os crimes.
    - Criação de uma **Agência Nacional de Segurança de Dados (ANSD)** como órgão regulador.

Conclusão do Resumo:

A proposta visa criar um sistema **"blindado"** onde:

1. A **prevenção é máxima**, com infraestrutura física e lógica de segurança extrema e governança diversificada.
2. A **dissuasão é total**, com penas de prisão longas e agravantes severas (como equiparação à traição) para quem violar a segurança dos dados.

O objetivo final é transformar a visão de soberania de dados em uma realidade operacional, protegendo as informações da população e do Estado como um **pilar da segurança nacional no século XXI**.