

Marco Legal da Cibersegurança no Brasil

Entenda o Projeto de Lei nº 4752/2025 que visa aumentar a resiliência cibernética do país

O problema: por que essa lei é necessária?

O Brasil enfrenta uma onda crescente de ataques cibernéticos que paralisam serviços públicos, expõem dados sensíveis de milhões de cidadãos e ameaçam a estabilidade de instituições governamentais. Sendo uma das maiores economias do mundo, o país ainda não possui uma lei federal robusta para coordenar a defesa digital, deixando uma lacuna crítica em sua segurança nacional.

A Solução Proposta: Projeto de Lei nº 4752/2025

O projeto institui o Marco Legal da Cibersegurança e cria o Programa Nacional de Segurança e Resiliência Digital, estabelecendo uma estratégia unificada e com financiamento garantido para proteger o Brasil no ciberespaço.



O que é o Marco Legal da Cibersegurança?

As mudanças trazidas pelo PL nº 4.752/2025, além de nominais, instituem a governança da cibersegurança no país. Propõe-se a criação da Autoridade Nacional de Cibersegurança (**ANC**), nos moldes de órgãos centrais de coordenação. Isso significa que a ANC ganhará competência para normatização, fiscalização e auditoria, o que permite decisões técnicas e coordenadas.

O que é uma Autoridade de Cibersegurança?

São entidades administrativas com alto grau de especialização técnica, responsáveis por funções de normatização, fiscalização e auditoria. São reguladas pelo próprio Marco Legal. Ainda, passa a contar com competências para instrução de processos administrativos. Diversos países contam com autoridades nacionais para coordenar a segurança digital.

O que muda na prática para a cibersegurança?

- **Para a ANC** - Consolida-se como o regulador da cibersegurança no País, com reforço de competências para regulamentação e fiscalização das políticas de segurança digital.
- **Para o setor privado** - Estabelece novas condições para fornecedores do governo, com conformidade como critério de contratação e avaliação de risco da cadeia de suprimentos. A responsabilidade por incidentes passa a ser compartilhada.
- **Para os cidadãos** - Não há mudanças diretas, pois a ANC atuará na proteção das infraestruturas críticas e dos serviços essenciais. Porém o aumento de uma resiliência cibernética no setor publico e privado, ajudará manter o nível de proteção de dados pessoais mais elevado.
- **Para o cenário internacional** - Pode aumentar a segurança jurídica e a reputação internacional do Brasil, com especial destaque para a cooperação e parcerias em defesa cibernética

Principais Disposições do PL nº 4.752/2025

Obrigações e Riscos ao Setor Privado

Conformidade como Critério de Contratação (Art. 14).

A contratação de soluções pelo governo exigirá a demonstração de conformidade com padrões mínimos de cibersegurança.

Avaliação de Risco da Cadeia de Suprimentos (Art. 13).

Órgãos públicos avaliarão os riscos cibernéticos de seus fornecedores como parte de seus processos de gestão.

Responsabilidade Compartilhada por Incidentes (Art. 13, § 3º).

A responsabilidade por falhas de segurança originadas em fornecedores será compartilhada entre a empresa e o órgão público.

Obrigação de Reporte de Falhas (Art. 15).

Incidentes cibernéticos envolvendo falhas de fornecedores deverão ser reportados à ANC.

Oportunidades ao Setor Privado

Criação de um Índice Público de Fornecedores (Art. 14, § 3º).

Previsão de um índice nacional de maturidade e confiabilidade da cadeia de suprimentos.

Inclusão em Listas de Conformidade Oficiais (Art. 14, § 4º).

A ANC publicará listas de conformidade que podem servir como atestado de adequação.

Acesso a Financiamento para P&D (Art. 16 e 20).

Recursos do Fundo Nacional de Segurança Pública poderão financiar projetos em cooperação público-privada.

Prioridade para Tecnologia Nacional (Art. 14, § 1º)

O texto determina a priorização de fornecedores e tecnologias nacionais que atendam aos requisitos.

Participação em Parcerias Estratégicas (Art. 8).

O setor privado poderá aderir ao Programa Nacional por meio de acordos, convênios ou parcerias.



Próximo passo: o PL possui tramitação no Congresso Nacional. Assim, aguarda-se a sua aprovação em ambas as Casas (Câmara dos Deputados e Senado Federal) e posterior sanção presidencial para plena eficácia.

Para acessar o PL nº 4.752/2025 na íntegra, clique [aqui](#).



Diretrizes Estratégicas para o Setor Privado

- **Diagnóstico interno** para avaliar a maturidade atual dos processos de cibersegurança em relação a padrões de mercado.
- **Adaptação para conformidade** para iniciar a adequação de produtos e serviços para estar apto a demonstrar conformidade quando os padrões mínimos forem publicados.
- **Mapeamento de oportunidades** para identificar como a empresa pode se beneficiar do fomento à P&D, da priorização de soluções nacionais e da demanda por serviços de adequação.
- **Monitoramento ativo** para acompanhar a tramitação do projeto e a futura regulamentação da ANC, pois os detalhes operacionais serão definidos nessas etapas.

Autores



Henrique Fabretti Moraes

Sócio e CEO do Opice Blum
Proteção de Dados e Governança de IA
henrique.fabretti@opiceblum.com.br



Tiago Neves Furtado

Sócio do Opice Blum
Resposta a Incidentes e Proteção de Dados
tiago.furtado@opiceblum.com.br

Guilherme Ochsendorf de Freitas

Advogado do time de Resposta a Incidente

Vinicius Azevedo Coelho

Advogado do time de Resposta a Incidente