FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

GOVERNANÇA E REGULAÇÃO DA CIBERSEGURANÇA NO BRASIL

Proteção da infraestrutura crítica, segurança da informação e construção da soberania digital

CARTILHA EXPLICATIVA

Esta cartilha apresenta os principais pontos do livro *Governança e regulação da cibersegurança no Brasil: Proteção da infraestrutura crítica, segurança da informação e construção da soberania digital*.

O objetivo é oferecer uma visão sistemática sobre a cibersegurança, entendida como um conjunto de iniciativas voltadas à proteção de pessoas e ativos digitais diante de ameaças que podem gerar impactos em múltiplos níveis, do individual ao nacional.

Ao examinar os elementos constitutivos e as diferentes dimensões da cibersegurança, a cartilha resume o quadro teórico e metodológico desenvolvido na obra, contribuindo para reflexões institucionais e regulatórias mais amplas.

O livro destaca os caminhos para construir a governança da cibersegurança no Brasil, alavancando-a para fortalecer a soberania digital brasileira.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

O que é cibersegurança?

É um conjunto de iniciativas voltadas à segurança de ativos digitais, incluindo pessoas, diante de riscos cibernéticos. A única definição consensual de cibersegurança é oferecida pela União Internacional das Telecomunicações da ONU. A partir dessa definição, podemos extrair três elementos centrais para cibersegurança:

Iniciativas de cibersegurança

- Podem ser políticas públicas, normas, práticas empresariais, medidas técnicas ou compromissos voluntários
- Buscam manter os ativos digitais protegidos de riscos, seja de forma preventiva ou reativa

Ativos digitais

- São softwares, hardwares, redes, bases de dados, infraestruturas, serviços, além das pessoas que usam tais ativos e podem ser afetadas por riscos cibernéticos
- Podem ser públicos, privados ou híbridos

Riscos cibernéticos

- Potenciais explorações de vulnerabilidades com impactos negativos para organizações
- Amplia-se a definição para incluir também as ameaças direcionadas às pessoas

Impacto da não mitigação dos riscos

A ausência de medidas eficazes de mitigação pode provocar incidentes de cibersegurança com consequências de diferentes magnitudes, que vão desde danos individuais até repercussões em nível nacional. Esses impactos podem afetar pessoas, grupos sociais ou organizações inteiras, gerando prejuízos econômicos, sociais e políticos.

Em função da permeabilidade dos ativos digitais em diversas áreas da sociedade, os riscos podem atingir desde a manutenção de um pequeno negócio familiar, passando pelo controle de redes logísticas empresariais, até a continuidade de serviços essenciais ou integridade de infraestruturas críticas.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Abordagem centrada nas pessoas em cibersegurança: o que significa isso?

A abordagem centrada no ser humano em cibersegurança valoriza o fator humano como pilar estratégico, com o objetivo de transformar o indivíduo de elo fraco em elo forte da cibersegurança. Seu objetivo é colocar a proteção e o empoderamento do indivíduo no centro das preocupações, fazendo da cibersegurança uma ferramenta de facilitação, e não de limitação, de liberdades individuais.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Cibersegurança e soberania digital: qual a conexão entre essas áreas?

Soberania digital: é a capacidade de entender o funcionamento das tecnologias digitais, conseguir desenvolvê-las e regulá-las efetivamente, exercendo, portanto, autodeterminação, poder e controle sobre ativos digitais, tais como dados, softwares, hardwares, redes eletrônicas e bancos de dados.

As medidas de soberania digital e de cibersegurança desempenham um papel complementar: o estudo da tecnologia é essencial para identificar e prevenir usos abusivos, enquanto o desenvolvimento tecnológico contribui para criação de soluções mais seguras.

A pesquisa e desenvolvimento são instrumentais para aprimorar a qualidade da regulação que, por sua vez, desempenha um papel fundamental no equilíbrio do setor, definindo os padrões mínimos a serem implementados para facilitar o desenvolvimento e adoção segura das tecnologias digitais. O estudo destaca a necessidade de se considerar pesquisa, desenvolvimento e regulação como dimensões indissociáveis da cibersegurança e soberania digital.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Ações práticas para promover a soberania digital

Fortalecimento da governança nacional da cibersegurança, protegendo dados, sistemas e infraestruturas críticas.

Implementação de políticas regulatórias, com padrões mínimos de segurança.

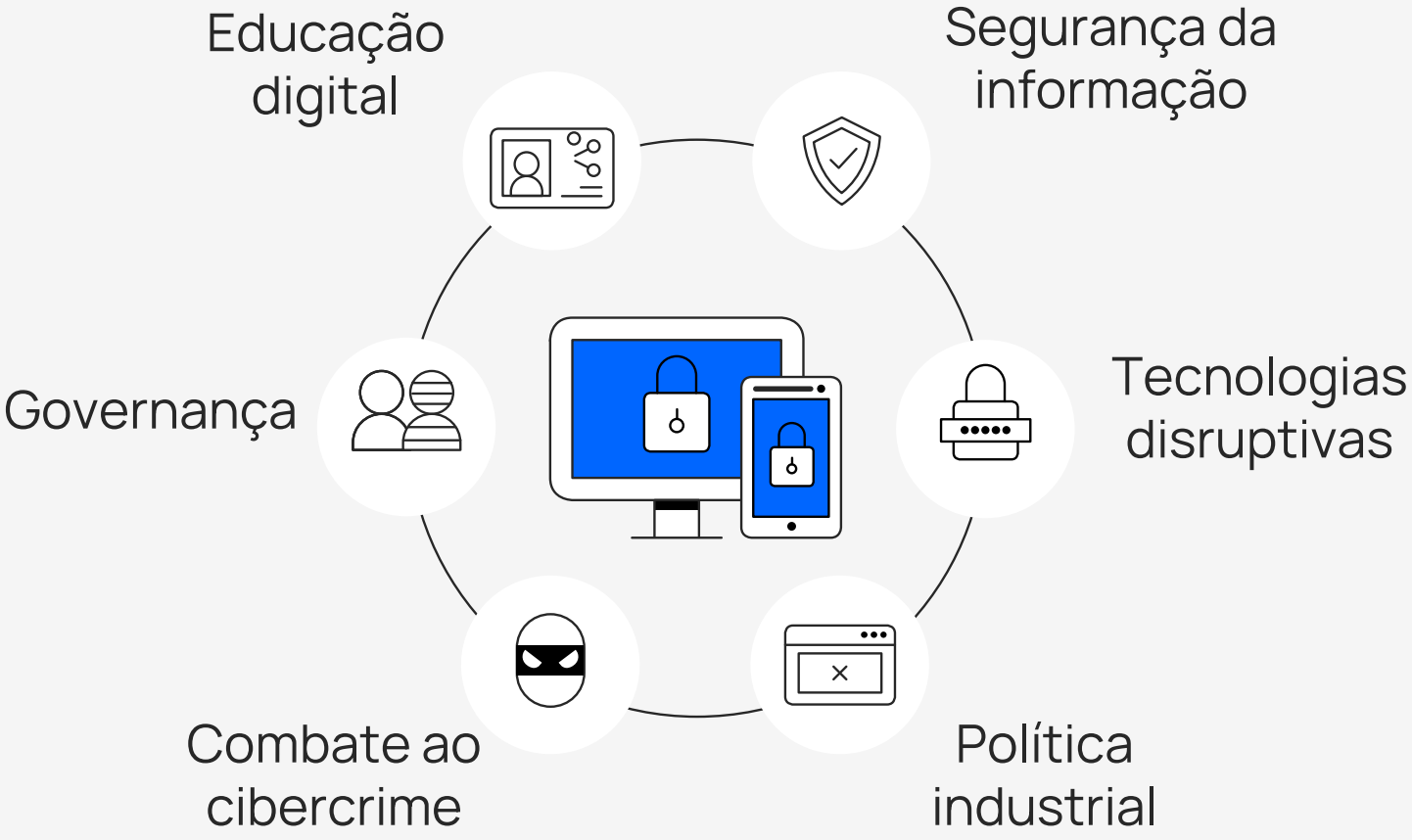
Capacitação contínua da força de trabalho e promoção da educação digital.

Investimento em pesquisa e desenvolvimento tecnológico nacional, incluindo softwares, algoritmos e soluções digitais estratégicas.

Promoção da autonomia tecnológica, incentivando empresas e centros de pesquisa a criar, absorver e desenvolver tecnologias nacionais.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Eixos essenciais para a cibersegurança e consolidação da soberania digital



Esses eixos funcionam como componentes estratégicos mínimos que devem permear a política pública de cibersegurança. Nessa linha, a E-Ciber(2025) foi estruturada em 4 eixos: (i) proteção e conscientização do cidadão e da sociedade; (ii) segurança e resiliência dos serviços essenciais e das infraestruturas críticas; (iii) cooperação e integração entre os órgãos e entidades, públicas e privadas; e (iv) soberania nacional e governança.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Governança

A cibersegurança envolve múltiplos atores e setores, públicos e privados, que desenvolvem, operam e regulam os diversos ativos digitais. Essa multiplicidade gera fragmentação e complexidade na implementação de políticas, tornando essencial a comunicação, coordenação, cooperação entre os diferentes participantes desse ecossistema.

Para exercer essas funções, um arranjo de governança deve:

- Desenvolver competências regulatórias, incluindo normatização, fiscalização e aplicação de sanções;
- Estabelecer padrões mínimos de cibersegurança para aplicação em todos os setores;
- Garantir coordenação e comunicação entre órgãos reguladores setoriais, atores operacionais e entidades privadas;
- Articular mecanismos de resposta a incidentes e prevenção de riscos, em conjunto com CSIRTs e ISACs;
- Fomentar capacitação, educação e cultura de cibersegurança, fortalecendo a educação digital e a preparação de profissionais;
- Facilitar a integração entre setores, promovendo harmonização normativa e colaboração interinstitucional.

A criação de um Sistema Nacional de Cibersegurança, coordenado por uma Agência Nacional de Cibersegurança, é proposta como solução estratégica para estruturar a governança. Nesse sistema, a agência central teria papel multifacetado:

Viabilizar canais de comunicação seguros

Articular a atividade de reguladores com órgãos técnicos essenciais como CSIRTs e ISACs

Promover a harmonização regulatória

Incentivar inovação e capacitação.

Coordenar a atuação de órgãos públicos e privados

O livro destaca que a implementação de tal sistema garante uma governança participativa, inclusiva e efetiva, capaz de reduzir a fragmentação do setor, otimizar a resposta a incidentes cibernéticos e fortalecer a soberania digital do país.

Segurança da informação

A segurança da informação constitui o fio condutor da cibersegurança, sendo central para a proteção dos ativos digitais e para o fortalecimento da soberania digital. A informação, seja pessoal ou não, passou a ser um ativo estratégico essencial, com papel decisivo na gestão de governos, empresas e serviços, refletindo a emergência de um novo paradigma tecno-econômico centrado em dados e conhecimento.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Combate ao Cibercrime

A legislação nacional ainda não consolidou uma lei geral contra crimes cibernéticos. Entretanto, a adesão e internalização da Convenção de Budapeste sobre Cibercrime, representam avanços importantes, ao padronizar a tipificação de crimes digitais e fornecer medidas processuais especiais para investigação e cooperação internacional, essenciais para enfrentar delitos transnacionais.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

O Brasil e a Convenção de Budapeste sobre Cibercrime

O Brasil ratificou a Convenção de Budapeste em fevereiro de 2023 e a internalizou por meio do Decreto nº 11.491/23, assumindo o compromisso de implementar medidas que adequem o ordenamento jurídico nacional às disposições do tratado. A Convenção estabelece uma lista mínima de crimes cibernéticos que todos os Estados-partes devem criminalizar, com o objetivo de harmonizar legislações e facilitar a cooperação internacional.

Esse alinhamento é essencial para eliminar um obstáculo frequente à colaboração entre países: a recusa de cooperação quando determinada conduta não é reconhecida como crime no ordenamento de outro Estado. Porém, nosso estudo destaca que alguns crimes cibernéticos tipificados pelo tratado ainda não tem amparo legal no Brasil.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Literacia digital

A literacia digital é um pilar central da cibersegurança e alicerce da soberania digital. Sua relevância aumenta à medida que novas tecnologias, como inteligência artificial e computação quântica, ampliam não somente as oportunidades, mas também os riscos cibernéticos.

CRIANÇAS

Uso seguro da internet, jogos e aplicativos.

ADOLESCENTES

Redes sociais, privacidade, fake news e cyberbullying.

PAIS

Acompanhamento, diálogo e monitoramento responsável.

IDOSOS

Prevenção contra golpes, fraudes bancárias e desinformação.

EDUCADORES

Inserir boas práticas de cibersegurança na educação, .

PROFISSIONAIS

Atualização constante, protocolos de segurança e práticas no ambiente de trabalho.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Política Industrial

A política industrial pode ser entendida como o conjunto de ações estatais voltadas para o estímulo à produção, à inovação e ao desenvolvimento tecnológico da indústria nacional. Seu objetivo central é:

1. Promover a incorporação de avanços tecnológicos na base produtiva do país
2. Superar falhas de mercado
3. Direcionar recursos e incentivos para setores estratégicos

No Brasil, a política industrial é particularmente relevante para áreas estratégicas como cibersegurança e ciberdefesa, uma vez que a dependência tecnológica externa torna o país vulnerável a riscos relacionados à proteção de dados, sistemas críticos e infraestrutura digital.

O volume explica que, para alcançar esses objetivos, a política industrial precisa considerar instrumentos como:

Tais mecanismos permitem que a cibersegurança seja vista não apenas como um custo, mas como uma oportunidade para fortalecer a indústria nacional e reduzir dependências externas.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Tecnologias Disruptivas e os desafios da inteligência artificial (IA)

A inteligência artificial (IA) é um exemplo de tecnologia disruptiva, isto é, que é capaz de transformar operações técnicas, econômicas e políticas por meio de inovação potencialmente desestabilizadora. O impacto da IA na cibersegurança depende diretamente de como ela é utilizada. Quando aplicada defensivamente, aumenta a capacidade de proteção e a resiliência digital; quando utilizada ofensivamente, amplia os riscos e a complexidade do ciberespaço.

ASPECTOS POSITIVOS IA DEFENSIVA	• fortalecer a proteção de sistemas, redes e dados, aumentando a resiliência; • automatizar a detecção de malware, monitorando ameaças em tempo real; • apoiar processos de tomada de decisão; • aprimorar a análise de vulnerabilidades.
ASPECTOS NEGATIVOS IA OFENSIVA	• Servir de ferramenta para automatizar ataques cibernéticos e explorar vulnerabilidades; • manipular sistemas de IA para causar previsões incorretas.

Conclusão: Caminhos da Soberania Digital e da Cibersegurança

O objetivo desta cartilha é facilitar o entendimento para profissionais de diversas áreas interessados em compreender as múltiplas dimensões da cibersegurança e sua relação com a soberania digital. Esse entendimento é essencial não apenas para proteger os ativos críticos e a população do país, mas também para que nossa nação se posicione como protagonista da governança digital regional e global, transformando desafios tecnológicos em oportunidades de fortalecimento econômico, social e democrático.

Para ter acesso ao livro em sua íntegra, acesse o QR Code abaixo:

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Autores do livro:

Luca Belli PhD, é Professor da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (FGV Direito Rio), onde coordena o Centro de Tecnologia e Sociedade (CTS) e o projeto CyberBRICS. Em julho de 2025 foi nomeado membro do Conselho Nacional sobre Transformação Digital, estabelecido pela Presidência da República e, em fevereiro 2024, foi nomeado membro do Comitê Nacional de Cibersegurança da Presidência da República.

Breno Pauli Medeiros é pesquisador e coordenador do projeto CyberBRICS – cibersegurança, no Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (FGV Direito Rio). Pesquisador de Pós-Doutorado na Escola de Comando e Estado-Maior do Exército (ECEME), no projeto PRO-DEFESA V: Inteligência Artificial e Tecnologias Quânticas.

Natália Couto é pesquisadora e coordenadora de projetos no Centro de Tecnologia e Sociedade (CTS) da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (FGV Direito Rio) no projeto CyberBRICS – cibersegurança. É professora convidada do LL.M em Direito: Regulação da Inteligência Artificial e Tecnologias Digitais na FGV Direito Rio.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

Autores do livro:

Erica Bakonyi é pesquisadora na FGV Direito Rio/CTS, no projeto CyberBRICS. Membro do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade (CMPDPP) da cidade do Rio de Janeiro. Advogada e Consultora na área de Proteção de Dados. Atuação como DPO-as-a-service. Ministra cursos nas áreas de proteção de dados pessoais, segurança da informação e inteligência artificial.

Walter Britto Gaspar é pesquisador e coordenador de projetos no Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (FGV Direito Rio), nos projetos Data Regulations e CyberBRICS. É Advogado e designer gráfico. É professor de Ética na Manipulação de Dados na Escola de Matemática Aplicada da Fundação Getúlio Vargas. Membro do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade (CMPDPP), Rio de Janeiro.

Daniel Dore Lage é pesquisador do Centro de Tecnologia e Sociedade (FGV Direito Rio/CTS). Consultor em proteção de dados pessoais e privacidade. Fellow of Information Privacy, CIPP/E e CIPT (IAPP).

Acompanhe-nos nas redes sociais!

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

@CTS_FGV

Material produzido pelo Centro de Tecnologia e Sociedade da FGV Direito Rio