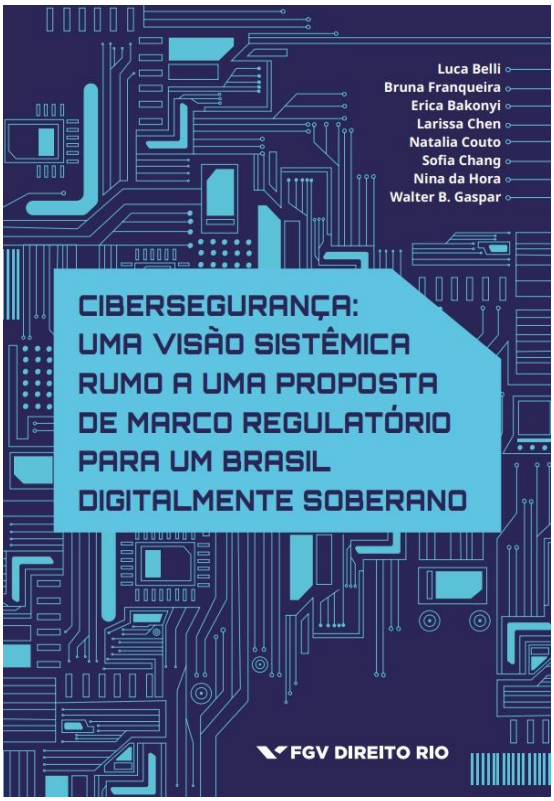
CARTILHA SOBRE CIBERSEGURANÇA E SOBERANIA DIGITAL

CIBERSEGURANÇA: UMA VISÃO SISTÊMICA RUMO A UMA PROPOSTA DE MARCO REGULATÓRIO PARA UM BRASIL DIGITALMENTE SOBERANO

O QUE É CIBERSEGURANÇA?



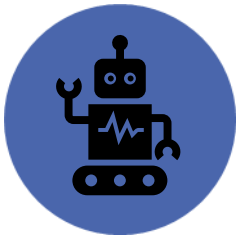
A cibersegurança é o conjunto de normas, práticas e processos que permitem proteger ativos digitais, informações e, sobretudo, pessoas de potenciais riscos e ameaças cibernéticas.

A cibersegurança é um assunto necessariamente multidimensional, multissetorial e, frequentemente, transnacional. Sem possuir um conceito único, definições de cibersegurança muitas vezes se cristalizam em torno de questões, ameaças, atividades e aspectos específicos.

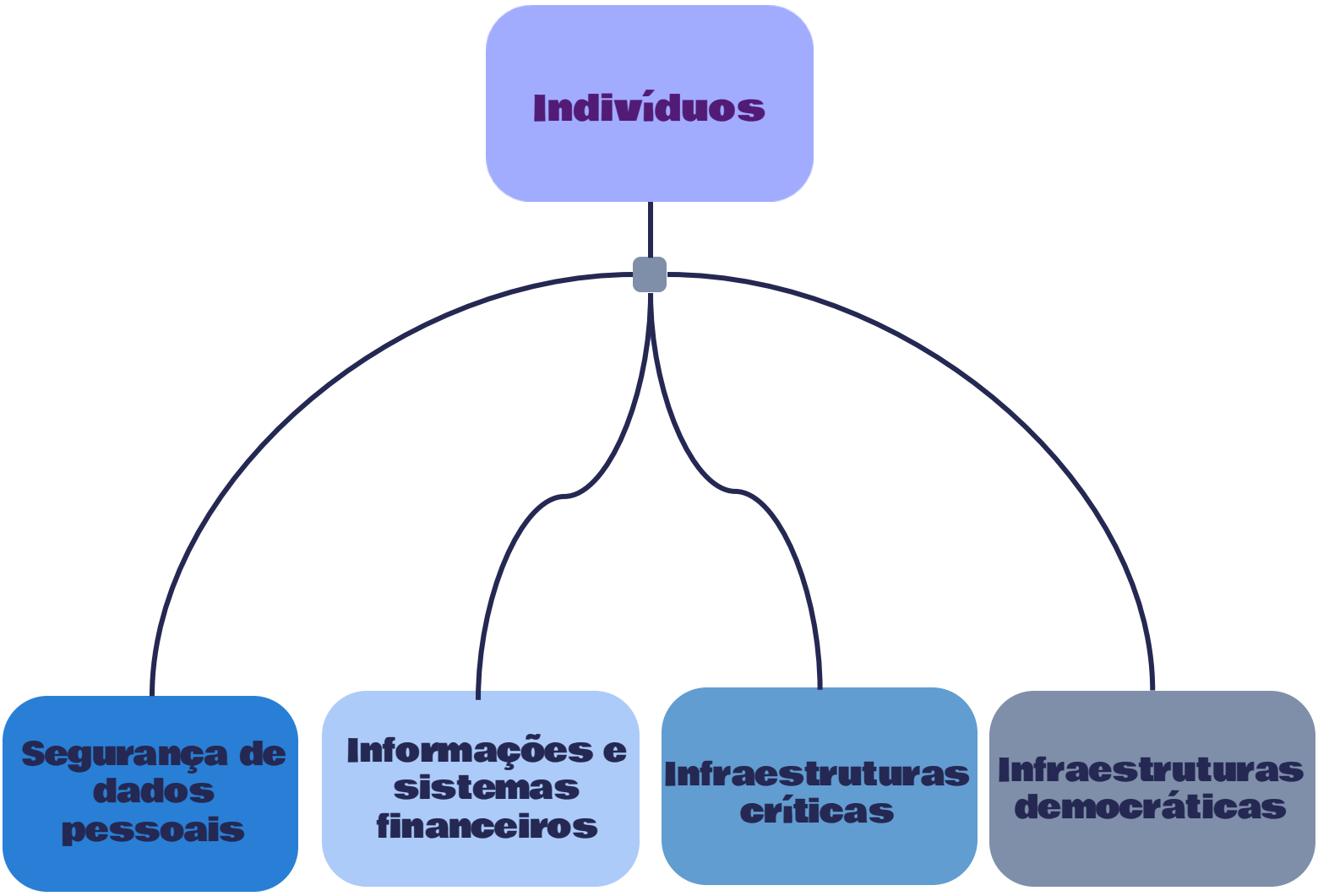
O QUE É CIBERSEGURANÇA?

A única definição consensual existente foi elaborada pelo Setor de Normatização das Telecomunicações da União Internacional de Telecomunicações, órgão da ONU conhecido pelo acrônimo em inglês ITU-T, segundo a qual:

> Cibersegurança é o conjunto de ferramentas, políticas, conceitos de segurança, diretrizes, abordagens de gestão de risco, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser utilizadas para proteger os ativos do ambiente cibernético, da organização e dos usuários. [...] A cibersegurança busca garantir o cumprimento e a manutenção das propriedades de segurança dos ativos da organização e dos usuários contra riscos relevantes à segurança encontrados no ambiente cibernético (ITU-T, 2009).



Quais os valores protegidos pela cibersegurança?



Por que isso é importante?

Diante de uma realidade na qual a conectividade se torna, a cada dia, mais permanente e essencial, nossas infraestruturas críticas estão sendo digitalizadas e automatizadas para incrementar sua performance, mas, com frequência, sem a devida consideração pelos riscos que a falta de cibersegurança acarreta.

As ameaças e riscos cibernéticos podem ocasionar efeitos sociais devastadores e comprometer o acesso às infraestruturas críticas do país. Os impactos são múltiplos e podem refletir efeitos internos, como situações de elevado estresse diante do desconhecimento sobre como lidar com esse tipo de situação, e interrupção de atividades essenciais.

O restabelecimento da infraestrutura, por sua vez, poderá levar a custos financeiros e sociais consideráveis, redução de competitividade, danos reputacionais, interrupção das operações e/ou serviços e riscos à privacidade e à proteção de dados.

O perigo do incidente cibernético é o efeito cascata, isto é, quando um incidente ou ataque inicial provoca consequências sucessivas em outros sistemas conectados ou dependentes, ampliando o dano inicial.

Onde mais isso ocorre?

- Infraestruturas críticas
- Sistemas bancários
- Sistemas governamentais integrados.
- Redes corporativas

Alguns exemplos de incidentes cibernéticos no Brasil:

Ataques ao ConecteSUS (G1, 2021) e ao FormSUS (VARGAS; RODRIGUES, 2021), impactando o controle vacinal e vulnerabilizando dados pessoais sensíveis de pacientes

Ataques a sistemas de tribunais, forçando a interrupção de processos e extensão de prazos, como o ataque que afetou a Justiça do Rio Grande do Sul (VASCONCELLOS, 2021) e outro, contra o STJ (VALENTE; VITAL, 2020)

O ataque ao sistema da Prefeitura do Rio de Janeiro, que obrigou a interrupção de serviços públicos ao cidadão (SCHENDES, 2022)

A invasão sofrida em sites do Governo do Ceará (EQUIPE TECMUNDO, 2022)

Precisamos de cibersegurança para alcançar a soberania digital?

A soberania digital refere-se à capacidade de uma dada entidade de exercer agência, autodeterminação e controle sobre dados e infraestruturas digitais.

A soberania digital deve, portanto, ser vista como a capacidade de uma nação, de um grupo ou de uma pessoa, física ou jurídica, de entender o funcionamento da tecnologia digital e exercer controle efetivo sobre as infraestruturas e dados digitais.

É interessante mencionar que soberania digital e cibersegurança se justapõe em diversos pontos. Vejamos:

Soberania digital e a cibersegurança estão presentes na concepção e execução de programas de transformação digital;

Compartilham o objetivo de assegurar a capacidade de controlar os próprios dados, incluindo tanto os dados pessoais, quanto informações importantes que revelam o funcionamento de uma organização ou sistema de infraestruturas críticas;

Precisam de investimento no desenvolvimento digital, o que inclui desenvolvimento de capacidades, investigação, desenvolvimento e manutenção de infraestruturas digitais robustas e atualização contínua da força de trabalho, hardware e software.

Uma visão pautada pela soberania digital passa por quatro elementos:

Autodeterminação

Ser soberano significa exercer livre determinação de seu desenvolvimento econômico, político, social e cultural.

Cibersegurança das Infraestruturas

Ser soberano significa ser capaz de controlar e proteger suas próprias infraestruturas críticas, suas redes eletrônicas, seus bancos de dados e as infraestruturas políticas que permitem a governança do País.

Soberania sobre dados

Ser soberano significa ser capaz de explorar economicamente, estrategicamente e tecnologicamente, ao invés de oferecer esses ativos valiosos para atores estrangeiros sem entender seu verdadeiro valor.

Capacitação Multigeracional

Para ser soberano é preciso forte ação de capacitação e treinamento multigeracional, almejando não somente as novas gerações, mas também aquelas que, apesar de já terem deixado o ensino primário ou secundário, nunca foram preparadas para os desafios da tecnologia digital.

Literacia digital: Por que precisamos fomentar ações nesse campo?

Educação, formação e capacitação são fundamentais e, conforme apontado, fundamentais para o desenvolvimento da soberania digital. Não basta proteger sistemas; é preciso educar as pessoas.

Grande parte dos incidentes cibernéticos ocorre por erro humano, como cliques em links maliciosos ou falhas na configuração de sistemas. Para reduzir esses riscos, é necessário investir em uma estratégia de educação e capacitação em cibersegurança que envolva toda a sociedade. Isso porque a segurança digital não depende apenas da tecnologia, mas também do comportamento dos usuários.

A educação digital deve garantir:

- Conectividade universal e inclusiva: acesso à internet de qualidade, dispositivos adequados e dados suficientes.
- Acesso a softwares e aplicativos: com foco em educação digital, uso de software livre e ensino de programação.
- Conteúdo educacional acessível: uso livre de materiais financiados com recursos públicos e criação de repositórios abertos.
- Segurança e auditoria de tecnologias digitais: para garantir o respeito aos direitos individuais e à soberania nacional.

Capacitação técnica e profissional

Capacitar é mais do que treinar: é um processo contínuo que deve envolver escolas, universidades, empresas e governos (municipal, estadual e federal). É preciso integrar ações que, hoje, ainda estão isoladas. A capacitação em cibersegurança deve ser vista como um investimento estratégico: reduz vulnerabilidades sociais e forma profissionais para uma área com alta demanda e escassez de talentos.

Atenção especial aos grupos mais vulneráveis

É fundamental desenvolver estratégias específicas para proteger e incluir públicos vulneráveis, como crianças, adolescentes, idosos, pessoas com deficiência e minorias sociais. Esses grupos enfrentam desafios particulares no uso seguro da tecnologia e precisam de ações educativas e preventivas adaptadas às suas realidades. Garantir a inclusão digital com segurança é um passo essencial para uma sociedade mais justa e resiliente.

Quais são as principais ameaças cibernéticas?

Desinformação

Vulnerabilidades

Uso da arquitetura de plataformas digitais(em especial, plataformas de redes sociais) para dispersão de desinformação, informações enganosas, ou informações maliciosas

Consequências

1. Efeitos nos processos eleitorais;
2. Disseminação de discursos de ódio, intolerância, racismo, machismo e outros tipos de preconceitos;
3. Desestabilização da política, das instituições e da economia local de um país ou organização social de outra natureza;
4. Impactos de natureza geopolítica;
5. Impactos para a saúde coletiva e para a integridade física das pessoas.

Software ou Código Malicioso (Malware)

Vulnerabilidades

Apresentam-se na forma de links e/ou e-mails em que direcionam à instalação de softwares maliciosos no dispositivo. Os tipos mais comuns, são os diferentes vírus de dispositivos eletrônicos, como softwares *worms* (“vermes”), que se multiplicam para atingir diferentes diapositivos; cavalos de Tróia (arquivos normais em aparência, infectados por vírus).

Consequências

1. Violação da tríade de princípios CIA ou IAA com a finalidade de solicitar resgate para reversão da atividade maliciosa e retomada da disponibilidade dos ativos;
2. Instalação de softwares maliciosos;
3. Obtenção de dados através do *spyware* (softwares de espionagem);
4. Compromete a operabilidade do sistema.

Quais são as principais ameaças cibernéticas?

Estelionato de Dados (Phishing)

Vulnerabilidades

Tipo de engenharia social que se apresenta na forma de links e/ou e-mails de comunicação que simulam uma fonte fidedigna, com objetivo de obtenção indevida de informações por meio do compartilhamento dos seus próprios titulares.

Modalidades de *phishing*:

i. *Smishing*: *phishing* realizado por meio SMS (mensagens de textos enviadas ao celular);
ii. *Vishing*:, *phishing* realizado por meio de ligações telefônica (robô se passando por telefone da instituição bancária da pessoa "alvo" do golpe);
iii. *spear phishing*: bastante comum no Brasil, em que o ator perpetrador do ataque se passa por outra pessoa (próxima ao ciclo da pessoa "alvo" do ataque), para obter informações ou benefícios. Muitas vezes, o ataque é realizado com base em informações públicas ou tornadas públicas pelo seu titular.
iv. *Whaling*: *é* uma modalidade de *spear phishing* realizado com pessoas públicas (famosas, políticas ou pessoas que, por alguma razão, possuem grande influência no debate público);
v. *Qrishing*: é o uso de códigos QR maliciosos (infectados) para roubo de identidade ou dados em geral (seja pela sobreposição do QR legítimo ou pelo redirecionamento do url correspondente para um url não legítimo)

Consequências

1. Obtenção de informações e dados sensíveis, cujo vazamento pode gerar graves consequências aos direitos fundamentais de seus titulares;
2. Realização de chantagem a partir das informações obtidas, para manipulação de comportamentos;
3. Obtenção de benefícios financeiros, por meio de pagamentos ou transferências indevidas.

Quais são as principais ameaças cibernéticas?

Falsidade ideológica/Roubo de identidade

Vulnerabilidades

Uso de aplicativos como plataformas de mídias sociais) para se passar por outra pessoa, valendo-se de informações disponíveis na internet sobre a pessoa que teve a identidade roubada.

Consequências

1. Violação a garantias fundamentais da pessoa que teve a identidade roubada;
2. Danos aos direitos da personalidade da pessoa que teve a identidade roubada.
3. Possíveis perdas financeiras da pessoa que teve a identidade roubada.

Ataque do homem do meio (Man-in the middle attack (MitM)

Vulnerabilidades

São conhecidos como ataques de espionagem em que os invasores podem adentrar ao sistema da vítima através de:

i. locais de acesso à rede Wi-Fi pública não segura;
ii. falsificação de IP;
iii. instalação de *malwares* no dispositivo;
iv. roubo de cookies do navegador.

Consequências

1. Violação a garantias fundamentais da pessoa que teve a identidade roubada;
2. Danos aos direitos da personalidade da pessoa que teve a identidade roubada.
3. Possíveis perdas financeiras da pessoa que teve a identidade roubada.

Quais são as principais ameaças cibernéticas?

Introdução de Linguagem de Questionamento Estruturado (Structured Query Language (SQL) injection)

Vulnerabilidades

Ocorre quando os invasores inserem códigos maliciosos no servidor que usa SQL10 com o objetivo de que este revele informações e dados que normalmente não revelaria. Pode se dar por meio de caixas de pesquisas de websites vulneráveis.

Consequências

Obtenção de informações e/ou dados pessoais que normalmente não seriam revelados

Exploração no dia zero (Zero-day exploit)

Vulnerabilidades

Consiste na descoberta de uma vulnerabilidade de software por invasores não detectada previamente pela própria vítima ou pelo desenvolvedor do sistema. Por meio desta vulnerabilidade os invasores entram no sistema para roubar informações e/ou dados.

Consequências

1. Obtenção de informações e/ou dados;
2. Diante de ataques dessa natureza, há o impacto de aumento nos custos organizacionais de defesa da organização.

Quais são as principais ameaças cibernéticas?

Reencaminhamento do sistema de nomes de domínio (DNS Tunneling)
Vulnerabilidades
Consiste em aproveitar a vulnerabilidade do DNS para realizar o tunelamento não legítimo de informações para o dispositivo do invasor. Pode até ser usado para retornos de chamada de comando e controle da infraestrutura do invasor para um sistema comprometido.
Consequências
O invasor consegue extrair informações e dados do sistema comprometido para o seu próprio dispositivo.
Vazamento de Dados
Vulnerabilidades
Pode se valer das técnicas anteriores para vazar informações disponibilizadas em determinada base de dados, ou de configurações erradas ou erros humanos, que levam à divulgação indevida da base.
Consequências
1. Violação de direitos fundamentais ou coletivos por meio do tratamento indevido ou discriminatório de dados; 2. Desvios nas finalidades;

Quais são as principais ameaças cibernéticas?

Ataques a cadeias de suprimento

Vulnerabilidades

Combina um ou mais dos ataques anteriores para promover ataque à dois alvos, simultaneamente, como entre cliente e fornecedor.

Consequências

1. Promover ataque a toda a base de clientes de uma organização;
2. Interromper os serviços ou oferta de produtos por determinada organização;
3. Interromper as atividades de determinada organização pela interrupção da prestação de serviço ou oferta de produto de determinado fornecedor.

Fraudes

Vulnerabilidades

Ato de enganar com a intenção de obter alguma vantagem indevida. Também pode ocorrer a ocultação de informações, mimetização de relevantes. Podem ser utilizadas informações públicas ou obtidas indevidamente para prática da fraude.

Consequências

1. Prejuízos financeiros a determinada pessoa;
2. Uso indevido de dados;
3. Danos reputacionais a organizações.

Muitos desses ataques combinam diferentes técnicas para explorar as vulnerabilidades das redes e seus usuários.

Cibersegurança Setorial no Brasil: quais os setores já regulam a cibersegurança?

A cibersegurança no Brasil é um ecossistema complexo e multidimensional, que envolve diversos setores, órgãos públicos e entidades reguladoras. Por isso, é fundamental que exista uma governança integrada e um marco regulatório harmonizado, capaz de coordenar essas iniciativas de forma eficiente e efetiva.

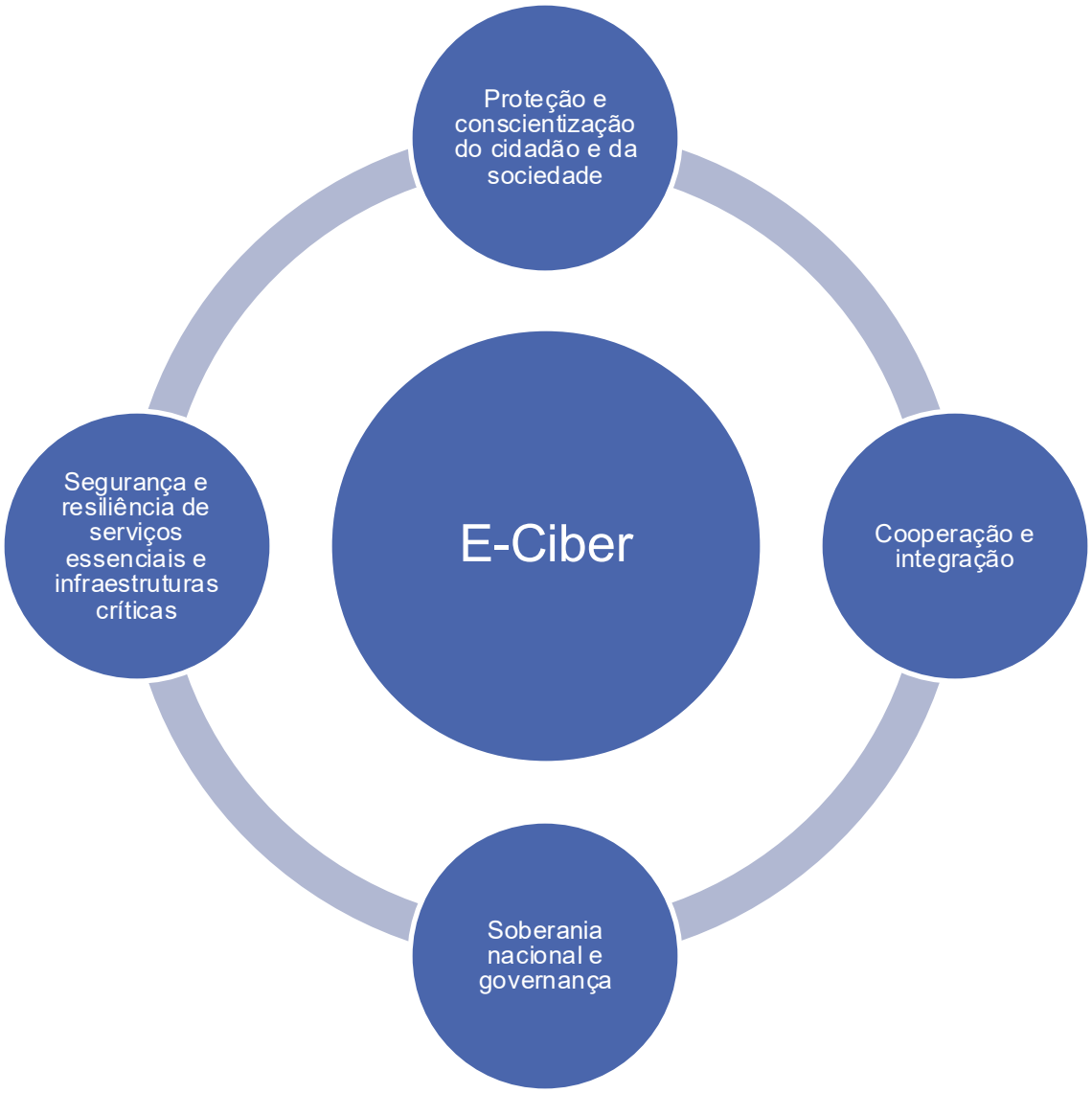
Atualmente, a regulação da cibersegurança no Brasil é feita de forma setorial, ou seja, cada órgão ou setor define suas próprias regras e políticas, dentro de suas competências legais. Não há uma norma federal unificada que integre todas essas ações em uma estratégia nacional consistente.

Alguns setores e agências já avançaram na criação de regras próprias para a proteção digital. Veja alguns exemplos:

- Banco Central do Brasil: Resoluções nº 4893/2021 e nº 454/2025
- ANATEL (Agência Nacional de Telecomunicações): Resoluções nº 740/2020 e nº 767/2024
- ANEEL (Agência Nacional de Energia Elétrica): Resolução nº 964/2021
- SUSEP (Superintendência de Seguros Privados): Circular nº 638/2021

Além disso, outros documentos estratégicos, como a E-Ciber, estabelecida pelo Decreto 12.573/25, orientam as ações da Administração Pública Federal.

A Estratégia Nacional de Cibersegurança (E-ciber) tem como objetivo fortalecer a segurança cibernética nacional e soberania digital. Está estruturada em 4 eixos:



Paralelamente, a partir de uma perspectiva ampla e, portanto, sem adentrar às ações e aos controles específicos, algumas boas práticas relacionadas à garantia da segurança da informação podem ser extraídas de documentos de soft law. São elas:

- Implementação de estruturas e padrões técnicos criadas por entidades especializadas
- Adoção de certificações em cibersegurança
- Uso de códigos de conduta internos ou setoriais
- Inclusão de cláusulas padrão de segurança em contratos
- Aplicação de regras corporativas vinculantes
- Contratação de seguros cibernéticos

Embora os avanços setoriais representem um passo importante, falta uma coordenação nacional que una todos os esforços em um programa de segurança da informação amplo e coerente. A ausência de um marco normativo federal impede a construção de políticas públicas integradas e prejudica o avanço da soberania digital do Brasil.

Um marco regulatório nacional deve garantir que a cibersegurança seja tratada como uma política de Estado, com diretrizes claras, transversais e eficazes.

Por que é difícil regular a cibersegurança?

A cibersegurança é um assunto multidimensional que exige a adoção de uma visão sistêmica, reconhecendo a complexa rede de atores e instituições envolvidos no tema, bem como o importante papel da participação multissetorial na definição de normas, padrões e políticas. Neste sentido, é essencial compreender como os diferentes elementos dos ecossistemas digitais se inter-relacionam e como desenvolver, usar e regular a tecnologia, em vez de ser regulado por ela.

A abordagem compartimentada produz estratégias, regulações, instituições e ações fortemente limitadas e fragmentadas. Isso configura uma vulnerabilidade sistêmica adicional, que pode ser frequentemente explorada. O valor da proposta de construir uma compreensão sistêmica da cibersegurança está em oferecer uma abordagem capaz de lidar com essa complexidade.

Conclusão

A cibersegurança é um tema complexo que exige uma abordagem sistêmica, democrática e eficaz. Sua discussão está diretamente ligada à soberania digital, essencial para o desenvolvimento sustentável do Brasil. No entanto, o país ainda carece de políticas estruturadas, como um Marco de Cibersegurança, uma Agência Nacional de Cibersegurança e um sistema eficiente de governança digital.

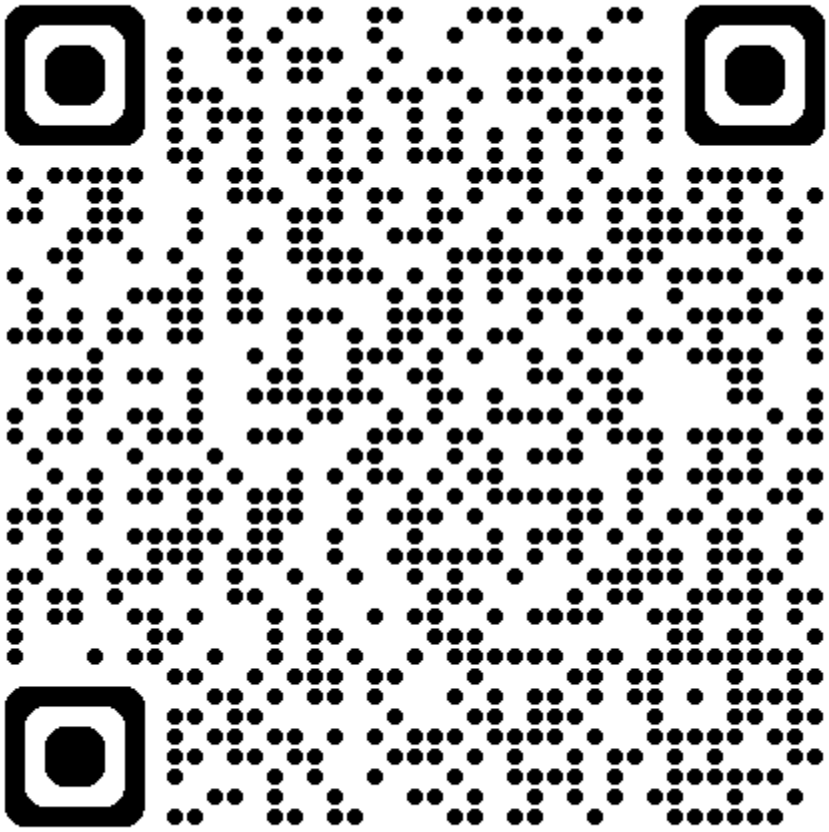
Este trabalho tem como objetivo oferecer ao leitor uma base para compreender o tema de forma crítica e informada, considerando os aspectos jurídicos, culturais e nacionais envolvidos. Para isso, defende-se a construção de um debate público amplo, multissetorial e inclusivo, capaz de guiar o país rumo a um ambiente digital mais seguro e soberano.

Como contribuição prática, ao final do livro apresenta-se uma proposta inicial de Marco de Cibersegurança e Soberania Digital, com foco na transformação do conhecimento técnico em políticas públicas e ações concretas.

Além disso, destaca-se a importância de discutir incentivos fiscais para medidas preventivas de cibersegurança, promovendo uma cultura de segurança digital nas organizações.

Por reconhecer a complexidade do tema, a proposta adota uma abordagem principiológica e minimalista, que valoriza o diálogo democrático e a construção coletiva de soluções.

Livro completo:



Acesse o trabalho completo pelo Qr code