Direito,
Inovação
& Tecnologia

CIBERSEGURANÇA E CRIMES CIBERNÉTICOS: UMA VISÃO DO BRASIL

2° EDIÇÃO INÉDITA, INCLUINDO ATUALIZAÇÕES:

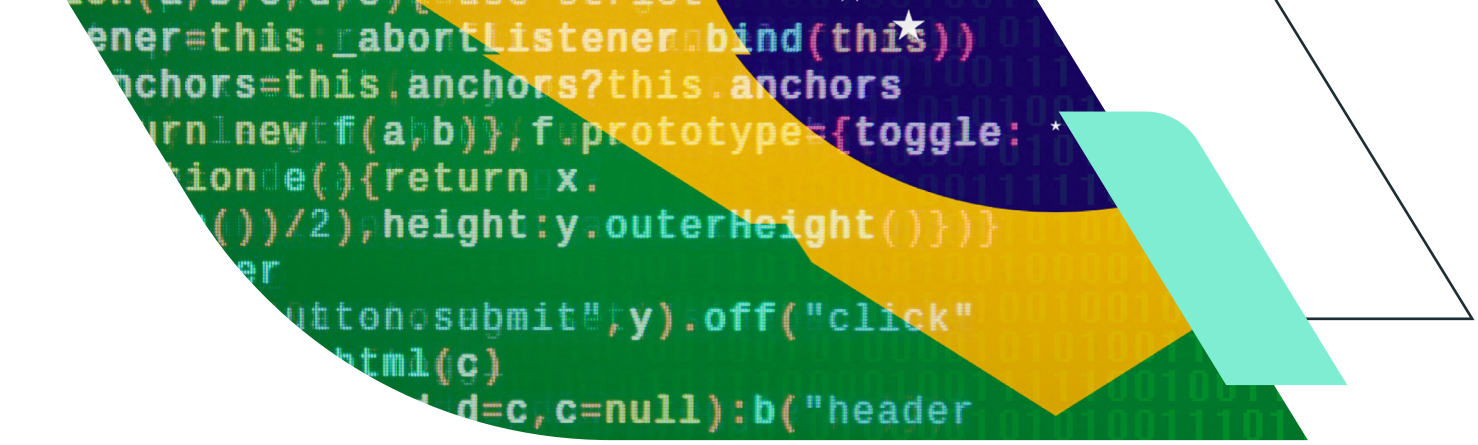
- Global Risks Report 2026 - WEF
- Convenção das Nações Unidas contra o Cibercrime
- Estratégia Nacional de Cibersegurança (Brasil)
- Resolução CMN nº 5.274/2025 (setor financeiro
- Uso de IA em investigações criminais (Portaria 961/2025 do MJSP)

MARÇO 2026

WWW.VLKLAW.COM.BR

INDEX

1. Contextualização do Panorama Brasileiro 3
2. Normas gerais 9
   a) Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/18) 13
   b) Marco Civil da Internet (Lei 12.965/14) e seu Decreto Regulamentador (Decreto 8.771/16)
   c) Código de Defesa do Consumidor
3. Normas setoriais
   a) Setor de Telecomunicações
   b) Setor financeiro
   c) Setor de Energia
   d) Setor de Saúde
   e) Setor de Seguros
4. Serviços essenciais e infraestruturas críticas 22
5. Crimes cibernéticos 24
   a) Tipificação penal das condutas
   Invasão de Dispositivo Informático (Art. 154-A do Código Penal)
   Fraude Eletrônica (Art. 171, §2º-A e §2º-B do Código Penal)
   Furto Digital (Art. 155, §4º-B do Código Penal)
   b) Uso de tecnologia em investigações criminais
6. Rede Federal de Gestão de Incidentes Cibernéticos (Decreto nº 10.748, de 16 de julho de 2021 28
7. Decisões judiciais relevantes 29
8. Política Nacional de Cibersegurança (Decreto nº 11.856/2023) e Comitê Nacional de Cibersegurança 31
9. Nova Estratégia Nacional de Cibersegurança (Decreto 12.573/25) 34
10. Próximos passos no Brasil 36
Conclusão 38
Sobre nós 39



1. Contextualização do Panorama Brasileiro

Incidentes cibernéticos despontam como preocupação crítica de curto e longo prazo, segundo relatórios mais recentes do Fórum Econômico Mundial. A pauta vai muito além de fraudes e vazamentos de dados: ataques cibernéticos têm potencial para paralisar empresas, instituições e até países inteiros.

O Global Risks Report 2026 afirma que o mundo ingressou em uma "Era de Competição", marcada por fragmentação institucional e alta incerteza, na qual os riscos tecnológicos assumem centralidade estratégica. A desinformação é o 2º maior risco no curto prazo (2 anos) e o 4º no longo (10 anos), impulsionada por IA generativa, redes sociais e deepfakes, com impacto direto na polarização social e na erosão da confiança democrática. A inteligência artificial é o risco que mais cresce em gravidade: sai da 30ª posição em dois anos para o 5º lugar em dez, com preocupações ligadas à substituição massiva de empregos administrativos, aumento da desigualdade e uso militar em sistemas autônomos, elevando o risco de escaladas não intencionais. Já a "ciber insegurança" permanece estrutural: 6ª no curto prazo e 8ª no longo, com ataques cada vez mais sofisticados contra infraestruturas críticas e a ameaça emergente do "Q-day", quando a computação quântica poderá romper a criptografia atual. O relatório conclui que alfabetização digital, transição para criptografia pós-quântica e requalificação profissional são medidas urgentes, e que as escolhas regulatórias e de governança tecnológica feitas agora definirão se a tecnologia será vetor de prosperidade ou de

instabilidade sistêmica.

O impacto financeiro é alarmante. O custo direto e indireto dos ciberincidentes representa 14% do PIB global por ano (Fórum Econômico Mundial, 2024). No Brasil, esse valor pode chegar a 18% do PIB — o equivalente a R$ 2,3 trilhões, segundo o INCC. Em média, cada incidente custa US$ 4,48 milhões. No Brasil, o valor é de US$ 1,22 milhão, aparecendo na 16ª posição (IBM, 2025). Quando uma empresa de capital aberto sofre um ataque bem-sucedido, independentemente de sua performance anterior, o valor de suas ações tende a cair, em média, 7,5% (Harvard Business Review, 2023).

O Brasil é um dos principais alvos de ataques cibernéticos e fraudes digitais do mundo, vivendo um paradoxo em cibersegurança: enquanto lidera em inovação e incorpora soluções digitais avançadas, como PIX e Open Banking, também se torna alvo e está cada vez mais exposto a ataques cibernéticos.

Em termos de fraudes, em março de 2025, 38% da população brasileira foi vítima de golpe bancário (ou tentativa de golpe), segundo a Febraban, comoincluindo clonagem de cartão de crédito (40%) engenharia social no WhatsApp (28%); phishing por ligação (26%); e golpe do Pix, envolvendo link ou QR Code maliciosos (16%).

No primeiro trimestre de 2025, o Brasil registrou, em média, mais de 2,6 mil ciberataques semanais por empresas (Check Point Research), alta de 21% em relação ao mesmo período de 2024. O país sofreu 60 bilhões de tentativas de ataques cibernéticos em 2023 (Fortinet).

Hoje, 40% dos ataques de phishing direcionados a empresas já são gerados por IA (VIPRE Security Group), e até 60% dos destinatários podem cair nesses golpes (Harvard Business Review), revelando uma taxa de sucesso preocupante. É o social engineering de alta conversão: mensagens hiperpersonalizadas, multi-idioma e com clonagem de voz, por exemplo.

Do lado dos criminosos, o uso de IA reduz em até 95% os custos de campanhas fraudulentas (Harvard Business Review), tornando esse vetor ainda mais atrativo.

O impacto também se expande para os deepfakes, que devem elevar as perdas globais em 32% até 2027, cerca de US$ 40 bilhões anuais (Deloitte).

A velocidade dos ataques também atinge patamares inéditos: o tempo médio para que criminosos avancem de uma brecha inicial até a movimentação lateral caiu para 48 minutos, com um caso recorde de apenas 51 segundos (CrowdStrike, 2025).

O fenômeno do Shadow AI, em que funcionários utilizam sistemas de IA sem aprovação corporativa, já foi responsável por 20% das violações e adicionou, em média, US$ 670 mil ao custo dos incidentes. Além disso, 97% dos incidentes envolvendo IA ocorreram em sistemas sem controles adequados (IBM, 2025).



Diante desse cenário, diversas estratégias vêm sendo apontadas como caminhos para a mitigação de riscos. Entre elas, destacam-se:

» A coordenação nacional de cibersegurança, pois a fragmentação entre diferentes stakeholders leva a respostas lentas e ineficazes diante do volume e da complexidade das ameaças;

» A harmonização regulatória, com a criação de um marco legal claro, equilibrado e baseado em risco, alinhado às melhores práticas internacionais e sem impor custos operacionais proibitivos; e

» A implementação de um programa nacional de conscientização em cibersegurança, voltado a empresas e cidadãos, que também integre o tema aos currículos educacionais, desde o ensino básico até o superior.

No cenário internacional, a movimentação já começou há décadas. A Convenção de Budapeste sobre crimes cibernéticos foi adotada em 2001. A partir da segunda década dos anos 2000, a União Europeia aprovou a diretiva NIS, obrigando os 27 países do bloco a criarem legislações e estruturas nacionais de cibersegurança. Mais recentemente, a UE aprovou a NIS2, elevando ainda mais o nível de exigência. Países como China, Rússia, Japão e Coreia do Sul também desenvolveram leis e órgãos específicos.

No âmbito da ONU, a Convenção das Nações Unidas contra o Cibercrime, adotada pela Assembleia Geral no final de 2024 e assinada formalmente em 2025, atravessa o processo de ratificação global para atingir a meta de 40 países e entrar plenamente em vigor. Ela estabelece o primeiro quadro jurídico universal vinculante e visa padronizar a cooperação policial transfronteiriça e a coleta de evidências eletrônicas, buscando equilibrar a soberania estatal e a eficácia no combate a delitos digitais complexos, embora ainda enfrente debates intensos

sobre a proteção da privacidade e dos direitos humanos frente ao poder de vigilância dos Estados.

No Brasil, apenas em 2023 o país promulgou sua adesão à Convenção de Budapeste, além de ter assinado em 2025 o texto final na ONU, o qual precisa passar pelo Congresso Nacional. As exigências existentes são, em geral, setoriais e não harmonizadas. Leis como o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Propriedade Industrial e a LGPD, por exemplo, contêm dispositivos relacionados ao tema, assim como regulações específicas para setores como o financeiro, telecomunicações, seguros e saúde. No entanto, falta um corpo normativo comum, além de outros setores sequer contarem com exigências mínimas em cibersegurança.

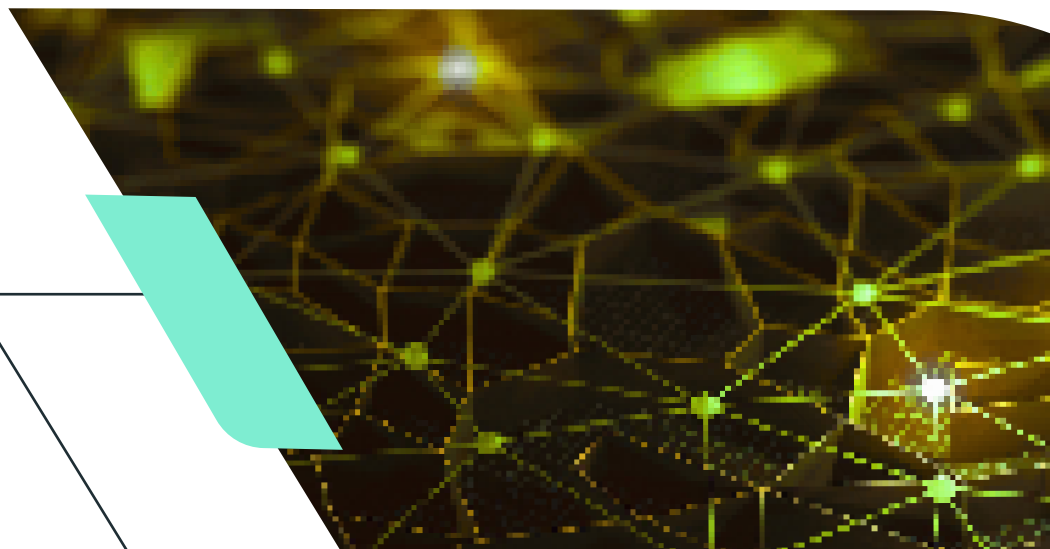
Em 2025, foi publicada a nova Estratégia Nacional de Cibersegurança (E-Ciber - Decreto nº 12.573/2025). Formulada pelo Comitê Nacional de Cibersegurança (CNCiber), a E-Ciber estruturou-se em quatro eixos temáticos: proteção e conscientização da sociedade; segurança e resiliência de serviços essenciais e infraestruturas críticas; cooperação multissetorial; e soberania digital.

No entanto, a ausência de órgão regulador nacional e intersetorial compromete a implementação de normas transversais, recomendadas pelas boas práticas internacionais. Essa lacuna pode ajudar a explicar por que o Brasil figura entre os países mais atacados do mundo. Sem regras claras, a cibersegurança é frequentemente negligenciada e os prejuízos só se evidenciam quando já é tarde demais.

Lembrando-se que 98% dos ataques cibernéticos poderiam ser evitados com medidas básicas de higiene digital, como uso de antimalware, atualização de sistemas, autenticação multifator, controle de acessos e governança de credenciais (Microsoft Digital Defense Report, 2022). Ou seja, um órgão central pautando a conscientização de empresas e pessoas, já seria suficiente para evitar boa parte dos incidentes.

Embora a criação de uma estrutura nacional de governança em cibersegurança represente investimento relevante, e que deve ser analisado com cautela à luz do cenário fiscal atual, os números indicam que, se bem desenhada e executada com foco em eficiência e coordenação, essa medida pode gerar impactos econômicos positivos. Estima-se que a prevenção de apenas 10% dos prejuízos causados por ataques cibernéticos já resultaria em economia anual entre R$ 150 e R$ 230 bilhões. Mesmo considerando um custo total estimado em R$ 500 milhões anuais a partir do quinto ano, o potencial de retorno seria muito expressivo, com ganhos da ordem de 300 vezes superiores ao investimento. Sob a ótica governamental, a arrecadação tributária derivada dessa economia superaria os R$ 50 bilhões, o que representaria um retorno fiscal superior a 100 vezes o valor investido. Ainda assim, é essencial que qualquer proposta avance com base em diálogo intersetorial, transparência e racionalização de recursos.

Em outras palavras, cibersegurança deixou de ser uma questão meramente técnica. É uma escolha estratégica e essencial, de líderes, conselhos e, acima de tudo, das nações.





2. Normas Gerais

A) LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD – Lei 13.709/18)

Nos termos da LGPD, o tratamento de dados pessoais deve observar a boa-fé e ser pautado por princípios (Art. 6º), como:

- **Segurança:** com a adoção de medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, bem como contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão
- **Prevenção:** mediante a implementação de ações que evitem a ocorrência de danos em decorrência do tratamento;
- **Responsabilização e prestação de contas:** exigindo que o agente demonstre a adoção de medidas eficazes que comprovem o cumprimento das normas de proteção de dados.

O tratamento será considerado **irregular** quando não observar a legislação ou deixar de garantir o nível de segurança que o titular razoavelmente pode esperar, considerando o modo como é realizado, os riscos envolvidos e as técnicas disponíveis à época (Art. 44).

Os agentes de tratamento **devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas** de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (Art. 46).

Os **agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação** em relação aos dados pessoais, mesmo após o seu término (Art. 47).

Além disso, **em caso de incidente de segurança com risco ou dano relevante**, o controlador tem o **dever de comunicar tanto a Agência Nacional de Proteção de Dados (ANPD), quanto o titular afetado** (Art. 48).

Sobre o assunto, a ANPD em 2024 a Resolução 15, a qual aprovou o Regulamento de Incidente de Segurança, trazendo com maior objetividade: i) conceitos relevantes (art. 3º); ii) as situações de alto risco e dano relevante (art. 5º); iii) documentos de accountability que devem ser elaborados, especialmente o Registro do Incidente de Segurança (art. 10), entre outros.

Por fim, importante também mencionar a Resolução da ANPD 4/2023, que aprovou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas da Autoridade Nacional de Proteção de Dados, definindo os critérios, métodos e as circunstâncias para calcular e aplicar sanções administrativas por descumprimento da LGPD, garantindo maior segurança jurídica e proporcionalidade nas punições.

B) MARCO CIVIL DA INTERNET (LEI 12.965/14) E SEU DECRETO REGULAMENTADOR (Decreto 8.771/16)

O **Marco Civil** da Internet estabelece, entre seus princípios, a **preservação da estabilidade, segurança e funcionalidade da rede,** por meio de medidas técnicas alinhadas aos padrões internacionais e do estímulo a boas práticas (art. 3º, V).

Além disso, impõe deveres de guarda de registros:

- O **administrador de sistema autônomo** responsável pela conexão deve manter os **registros de conexão** pelo prazo de **1 ano**, sob sigilo e em **ambiente controlado e seguro** (art. 13).

- Os **provedores de aplicações de internet**, quando organizados profissionalmente e com fins econômicos, devem manter os **registros de acesso às aplicações** por **6 meses**, também sob **sigilo** e em **ambiente seguro** (art. 15).

O **Decreto nº 8.771/2016**, por sua vez, regulamenta os **padrões de segurança e sigilo** na guarda, armazenamento e tratamento dos dados pessoais e comunicações privadas, impondo que os provedores adotem medidas como (Art. 13):

- **Controle estrito de acesso** aos dados, com definição clara das responsabilidades e privilégios dos usuários autorizados;

- **Autenticação robusta**, preferencialmente com múltiplos fatores, para individualizar os responsáveis pelos acessos;

- **Inventário detalhado dos acessos**, incluindo momento, duração, identidade do responsável e arquivo acessado;

- **Soluções de proteção à inviolabilidade dos dados**, como encriptação ou medidas de segurança equivalentes.

C) CÓDIGO DE DEFESA DO CONSUMIDOR

Nos termos do **Código de Defesa do Consumidor,** é considerada prática abusiva a colocação no mercado de **produtos ou serviços em desacordo com normas técnicas estabelecidas por órgãos oficiais competentes** ou, na ausência destas, **pela Associação Brasileira de Normas Técnicas – ABNT** (art. 39, VIII).

Isso implica que **empresas que negligenciam a observância de normas técnicas reconhecidas para cibersegurança**, como a **ABNT NBR ISO/IEC 27001 e a ABNT NBR ISO/IEC 27701, podem ser responsabilizadas por práticas inadequadas ou inseguras**, inclusive no âmbito da defesa do consumidor.



3. Normas Setoriais

A) SETOR DE TELECOMUNICAÇÕES

No setor de telecomunicações, a **Agência Nacional de Telecomunicações (Anatel)** é a entidade responsável por definir diretrizes de **segurança cibernética** aplicáveis às prestadoras de serviços.

O tema é disciplinado principalmente pela **Resolução nº 740/2020**, alterada pela **Resolução nº 767/2024**, que institui o **Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações**. Dentre suas principais exigências, destaca-se a obrigatoriedade de:

- **Estabelecimento de Política de Segurança Cibernética**, com procedimentos de **resposta a incidentes** (art. 14);
- **Comunicação obrigatória à Anatel** de incidentes de segurança considerados relevantes, tais como:

- Aqueles também reportáveis à ANPD (art. 2º-C);
- Incidentes que afetem substancialmente a segurança das redes ou dos dados dos usuários (art. 9º e 17), com necessidade de notificação aos usuários e inclusão de análise da causa, impacto e ações de mitigação.

A forma de comunicação deve seguir diretrizes do **GT-Ciber da Anatel**, conforme estabelecido no **Despacho Decisório 49/2021/COQL/SCO**: o incidente deve ser reportado pelo SEI **em até 2 dias úteis**, ainda que de forma preliminar, com complementação em até 60 dias. São exemplos de incidentes relevantes:

- Vazamentos de dados corporativos ou de clientes;
- Ataques de *ransomwares* bem-sucedidos e ameaças persistentes avançadas (APT);
- Ataques de negação de serviço (DDoS) com tráfego igual ou superior a 50Gbps ou 20Mpps;
- Problemas de roteamento com impacto na entrega de serviços;
- Indisponibilidade de serviço causada por incidente cibernético.

O regulamento também impõe **obrigações de avaliação prévia de fornecedores**, inclusive de serviços em nuvem, quanto à conformidade com as regras, exigindo **auditorias independentes periódicas** e documentação do processo, a ser apresentada à Anatel mediante solicitação.

Há ainda a exigência de **compartilhamento de informações sobre incidentes relevantes** entre prestadoras, de forma sigilosa e não discriminatória, inclusive com opção de anonimato, para fins de coordenação com outras entidades (art. 18).



Complementarmente, a Anatel publicou, em outubro de 2023, um **Guia Orientativo de Segurança Cibernética**, com recomendações práticas, como a criação de planos de resposta a incidentes, designação de responsáveis pela gestão desses eventos e manutenção de canais de contato específicos para comunicação de incidentes.

B) SETOR FINANCEIRO

No setor financeiro, as diretrizes sobre segurança cibernética e resposta a incidentes são estabelecidas por **entes reguladores como o Banco Central do Brasil (BCB), o Conselho Monetário Nacional (CMN) e a Comissão de Valores Mobiliários (CVM).**

A Resolução CMN nº 5.274/2025 elevou o padrão de governança ao detalhar o conteúdo mínimo obrigatório das políticas de segurança cibernética, exigindo mecanismos específicos de autenticação, criptografia, prevenção de vazamento de informações e gestão de cópias de segurança, atualizando em parte a Resolução CMN nº 4.893/2021, atualizada em 2024, estabelece diretrizes para a política de segurança cibernética e requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem por instituições financeiras, prevendo as seguintes obrigações:

Política de Segurança Cibernética

- Deve ser elaborada, implementada e compatível com o porte, perfil de risco e complexidade da instituição.
- Precisa conter objetivos, controles e procedimentos específicos, como de autenticação, criptografia, detecção de intrusão, gestão de cópias, entre outros; e
- Revisada anualmente e aprovada pela alta administração.

Plano de Ação e Resposta a Incidentes

- Estabelecer ações preventivas e reativas, com área responsável por registrar efeitos dos incidentes.
- Elaborar relatório anual, incluindo incidentes, testes e efetividade

Comunicação de Incidentes ao BCB

- Incidentes relevantes e interrupções de serviços essenciais devem ser comunicados **tempestivamente**.
- Devem ser informadas também as providências adotadas para a retomada das atividades.

Contratação de Serviços de Nuvem e Processamento de Dados

- Avaliação prévia da empresa contratada e aderência à regulação.
- Responsabilidade integral da instituição pelos serviços contratados.
- Comunicação ao BCB após contratação/alteração de serviços relevantes.
- Exigências adicionais para serviços prestados no exterior.

Designação de Diretor Responsável

- A instituição deve nomear **diretor responsável** pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

No âmbito do **Pix**, a **Resolução BCB nº 1/2020,** a **Resolução BCB nº 402/2024** e a **Instrução Normativa BCB nº 412/2024**, determinam que os participantes que oferecem contas aos titulares **devem comunicá-los diretamente sobre incidentes com seus dados pessoais**, mesmo quando não forem os responsáveis diretos pelo incidente, e ainda que não haja risco ou dano relevante.

A comunicação deve seguir os seguintes critérios operacionais:

- Ser realizada conforme prazo definido pelo BCB, via sistema oficial de correio eletrônico;
- Incluir linguagem clara, individualizada, e conter informações sobre o incidente, os dados afetados e os riscos envolvidos;
- Ser arquivada, estando disponível ao BCB a qualquer tempo.

Já no mercado de capitais, a **Instrução CVM nº 505/2011**, com as alterações da **Instrução CVM nº 612/2019**, impõe obrigações aos intermediários de valores mobiliários quanto à **segurança da informação e continuidade de negócios**. A norma exige a adoção de **Política de Segurança da Informação**, abrangendo:

- Tratamento e controle de dados de clientes;
- Avaliação da **relevância de incidentes de segurança**;
- Comunicação aos clientes afetados, quando o incidente envolver **processos críticos de negócio** ou **dados sensíveis**, com **impacto significativo**.

C) SETOR DE ENERGIA

No setor de energia elétrica, a **Agência Nacional de Energia Elétrica (ANEEL)** estabelece, por meio das **Resoluções nº 24/2021** e **nº 964/2021**, obrigações específicas relacionadas à **segurança cibernética**.

De acordo com o **art. 4º da Resolução nº 964/2021**, os agentes regulados devem adotar mecanismos de prevenção, detecção, resposta e recuperação de incidentes como parte integrante de sua **Política de Cibersegurança.** Essa política também deve prever critérios para avaliar a relevância dos incidentes e orientar a comunicação à equipe de coordenação setorial designada.

É obrigatória a **comunicação à ANEEL dos incidentes considerados de maior impacto** (art. 6º), os quais devem ser registrados, analisados em termos de causa e impacto, e acompanhados de medidas de controle de efeitos, incluindo dados fornecidos por **prestadores de serviços terceirizados**.



A norma define **incidente cibernético** como qualquer evento que comprometa, real ou potencialmente, a **disponibilidade, integridade, confidencialidade ou autenticidade de sistemas** de informação ou dos dados neles tratados, inclusive **tentativas de exploração de vulnerabilidades** que configurem violação de normas ou políticas internas (art. 2º, I).

Já os incidentes de maior impacto são aqueles classificados como de **alta severidade**, conforme a matriz de risco de cada agente (art. 2º, II).

Adicionalmente, os agentes devem manter registros detalhados e fornecer à ANEEL, mediante solicitação, informações como:

- Resultados dos modelos de maturidade aplicados, incluindo extensão e impacto dos eventos, grau de ameaça, relevância, vulnerabilidade, esforço de normalização e frequência;
- Riscos cibernéticos identificados e respectivas formas de tratamento;
- Dados das equipes responsáveis pela prevenção, tratamento e resposta a incidentes cibernéticos.

D) SETOR DE SAÚDE

No setor da saúde, a **Agência Nacional de Vigilância Sanitária (Anvisa)** é o principal ente regulador com disposições voltadas à segurança da informação, especialmente no que se refere a **dispositivos médicos e proteção de dados pessoais**. A **Agência Nacional de Saúde Suplementar (ANS)**, por sua vez, **ainda não possui regulação específica sobre o tema**.

A **Portaria Anvisa nº 1.184/2023** determina, entre os **arts. 29 a 31**, que fornecedores de serviços de tecnologia da informação e comunicação adotem **procedimentos e plano de resposta a incidentes de segurança**, devendo comprovar a existência de **garantias de segurança** e **comunicar imediatamente** qualquer risco ou incidente que possa afetar dados pessoais. A norma também prevê que a Anvisa deverá editar r**egulamentação própria para o gerenciamento de incidentes envolvendo dados pessoais**, ainda pendente de publicação.

O **Guia nº 33/2020** da Anvisa, voltado à **validação de sistemas computadorizados** aplicados nas Boas Práticas de Fabricação, trata da **gestão**

de incidentes (Seção 11.5), ressaltando a importância de respostas rápidas, notificações claras às autoridades competentes e comunicação escalonada em caso de impacto relevante. Na **Seção 11.6**, são abordadas as **ações corretivas e preventivas (CAPA)**, com foco na **documentação rigorosa** das medidas adotadas e na **avaliação da eficácia**, assegurando melhoria contínua e robustez dos sistemas.

Já o **Guia nº 38/2020**, que trata dos **princípios e práticas de cibersegurança em dispositivos médicos**, estabelece diretrizes para que os f**abricantes desenvolvam processos sólidos para avaliação, resposta e comunicação de incidentes cibernéticos**, em colaboração com a Anvisa e os prestadores de serviços de saúde, ao longo de todo o ciclo de vida dos dispositivos (Seção 6.5).

E) SETOR DE SEGUROS

No setor de seguros, a **Superintendência de Seguros Privados (Susep)** regulamenta as exigências de **segurança cibernética** por meio da **Circular SUSEP nº 638/2021**, aplicável a seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores locais.

A norma determina que as supervisionadas mantenham **processos, procedimentos e controles atualizados** para **identificar e reduzir vulnerabilidades**, bem como **detectar, responder e se recuperar de incidentes cibernéticos**, o que deve estar formalizado no **Plano de Continuidade de Negócios (PCN)** da companhia (art. 5º)

É obrigatória a implementação de **Plano de Ação e de Resposta a Incidentes**, contendo:

- Ações de adaptação da estrutura organizacional às diretrizes da política de segurança cibernética;
- Procedimentos, controles e tecnologias para prevenção e resposta a incidentes;
- Designação da área responsável pelo registro e acompanhamento dos efeitos de incidentes relevantes (arts. 6º e seguintes).

Incidentes relevantes são definidos como eventos adversos (maliciosos ou não) que comprometam substancialmente a **confidencialidade, integridade ou disponibilidade de dados ou serviços relevantes** (art. 2º, IV). Já **dados relevantes** abrangem dados pessoais (conforme a LGPD), informações de clientes, processos críticos e quaisquer outros definidos como sensíveis pelas próprias supervisionadas (art. 2º, VI).

A comunicação desses incidentes à **Susep deve ocorrer em até 5 dias úteis** (art. 8º) e deve conter:

- A extensão do dano;
- As ações em curso para correção;
- Os responsáveis e prazos, quando aplicável.





4. Serviços Essenciais e Infraestruturas Críticas

As infraestruturas críticas e os serviços essenciais representam áreas estratégicas para a segurança nacional, o funcionamento da sociedade e a continuidade de atividades econômicas vitais. A regulação sobre o tema encontra-se nos seguintes marcos normativos no Brasil:

A Política Nacional de Segurança de Infraestruturas Críticas, instituída pelo Decreto nº 9.573/2018, atribui ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) a competência para acompanhar os temas relacionados às infraestruturas críticas no âmbito da administração pública federal (art. 2º).

Complementarmente, a Estratégia Nacional de Segurança de Infraestruturas Críticas, prevista no Decreto nº 10.569/2020, reforça o papel estratégico de setores como comunicações, energia, transportes, finanças e águas, cuja interrupção ou destruição pode gerar impactos sociais, econômicos, políticos ou à própria segurança e soberania nacionais. A estratégia destaca a atuação do GSI na identificação e análise de riscos, em cooperação com entes públicos e privados.

Já a Lei nº 7.783/1989 define os serviços e as atividades essenciais, que devem ser mantidos mesmo em contextos de greve, dada sua importância para o atendimento das necessidades inadiáveis da comunidade. O rol inclui, entre outros:

- Abastecimento de água, energia elétrica, combustíveis e gás;
- Assistência médica e hospitalar;
- Distribuição de medicamentos e alimentos;
- Telecomunicações e transporte coletivo;
- Processamento de dados ligados a serviços essenciais;
- Controle de tráfego aéreo, atividades bancárias e portuárias;
- Atividades médico-periciais e funerárias.

A legislação determina que sindicatos e empregadores mantenham equipes mínimas em operação durante paralisações, de forma a evitar prejuízos irreversíveis e garantir a continuidade dos serviços essenciais (arts. 9º e 11).



5. Crimes Cibernéticos

A) TIPIFICAÇÃO PENAL DAS CONDUTAS

A legislação penal brasileira prevê sanções específicas para crimes cometidos no ambiente digital, com foco na **proteção de dispositivos informáticos, dados e sistemas** contra invasões e fraudes.

INVASÃO DE DISPOSITIVO INFORMÁTICO (ART. 154-A DO CÓDIGO PENAL)

É crime **invadir dispositivo informático de uso alheio**, com ou sem conexão à rede, com a finalidade de **obter, adulterar, destruir dados ou instalar vulnerabilidades**, sem autorização do usuário.

- **Pena:** reclusão de **1 a 4 anos**, e multa.
- Incorre na mesma pena quem **produz, vende ou distribui programas ou dispositivos** com o intuito de permitir essa prática.
- A pena é aumentada de **1/3 a 2/3** se a invasão causar **prejuízo econômico.**
- Se a invasão resultar na obtenção de **comunicações privadas, segredos comerciais ou industriais, informações sigilosas ou controle remoto do dispositivo**, a pena é de **2 a 5 anos**, e multa.
- Haverá **agravamento de 1/3 a 2/3** se os dados obtidos forem **divulgados,**

comercializados ou transmitidos a terceiros.

FRAUDE ELETRÔNICA (ART. 171, §2º-A E §2º-B DO CÓDIGO PENAL)

Trata-se da prática de **fraude para obtenção de vantagem ilícita**, com uso de **redes sociais, ligações, e-mails ou outros meios digitais** que induzam a vítima ou terceiros a erro.

- **Pena:** reclusão de **4 a 8 anos**, e multa.
- A pena é aumentada de 1/3 a 2/3 se o crime for praticado com **uso de servidores no exterior.**

FURTO DIGITAL (ART. 155, §4º-B DO CÓDIGO PENAL)

Caracteriza-se pelo **furto mediante fraude**, cometido por meio de **dispositivos eletrônicos ou informáticos**, ainda que sem violação de mecanismos de segurança ou com uso de **software malicioso.**

- **Pena:** reclusão de **4 a 8 anos**, e multa.



B) USO DE TECNOLOGIA EM INVESTIGAÇÕES CRIMINAIS

Portaria 961/2025, do Ministério da Justiça e Segurança Pública (MJSP), estabelece normas inéditas para o uso de soluções tecnológicas em investigações criminais e atividades de inteligência de segurança pública, com três pilares fundamentais:

- O fortalecimento dos mecanismos de investigação e inteligência por meio de soluções tecnológicas avançadas;
- A proteção rigorosa de dados pessoais para prevenir uso ilícito em fraudes, golpes financeiros e perseguições; e
- A criação de parâmetros claros para aplicação de inteligência artificial (IA) em operações de segurança pública.

A portaria se aplica a todas as forças de segurança federais, como Polícia Federal, Polícia Rodoviária Federal, Polícia Penal Federal, Força Nacional de Segurança Pública e Força Penal Nacional.

Entre as principais inovações, a portaria autoriza o uso de tecnologias nas investigações criminais, desde que respeitados os princípios de legalidade, necessidade e finalidade.

Pela primeira vez no país, uma normativa específica estabelece parâmetros claros para uso de inteligência artificial em segurança pública, definindo limites éticos e operacionais que garantem eficiência sem comprometer direitos fundamentais dos cidadãos.

Na área prisional, a medida autoriza o uso de tecnologia para localizar e bloquear celulares e, mediante autorização judicial, acessar dados armazenados nos dispositivos. Essas ações visam coibir o crime organizado e ampliar o controle sobre comunicações ilícitas feitas de dentro de presídios.
A regulamentação estabelece rigorosas regras de governança, incluindo controle de acesso aos sistemas, revisões periódicas de perfis de usuários, planos de resposta a desastres, auditorias regulares, investigação de acessos indevidos e registro detalhado de todas as ações realizadas.

A contratação de tecnologias deverá seguir regras específicas de licitação, com transparência e controle social sobre os investimentos em tecnologia de segurança.



6. Rede Federal de Gestão de Incidentes Cibernéticos

(DECRETO Nº 10.748, DE 16 DE JULHO DE 2021)

O **Decreto nº 10.748/2021** institui a **Rede Federal de Gestão de Incidentes Cibernéticos**, com base no Decreto nº 9.637/2018, com o objetivo de **fortalecer a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional** no enfrentamento de riscos cibernéticos (art. 1º e 2º).

A finalidade da Rede é **elevar o nível de resiliência em segurança cibernética** dos ativos de informação da administração pública federal, por meio de ações integradas de **prevenção, tratamento e resposta a incidentes cibernéticos.**

Dentre seus **principais objetivos**, destacam-se (art. 3º):

- **Divulgação de medidas preventivas e reativas** relacionadas à segurança cibernética;
- **Compartilhamento de alertas** sobre ameaças e vulnerabilidades;
- **Disseminação de informações** sobre ataques cibernéticos;
- **Promoção da cooperação institucional** entre os participantes da Rede;
- **Agilidade na resposta a incidentes**, garantindo eficiência no enfrentamento de eventos cibernéticos relevantes.

7. Decisões Judiciais Relevantes

O Superior Tribunal de Justiça (STJ) tem analisado casos relevantes sobre vazamento de dados e responsabilidade das empresas, interpretando a LGPD:

- Em 2023, a Segunda Turma entendeu que, **embora o vazamento de dados seja uma falha indesejável, ele não gera, por si só, o direito à indenização por danos morais**. Para tanto, o titular deve comprovar o efetivo prejuízo causado pela exposição, pois os dados vazados eram comuns e frequentemente fornecidos em cadastros e sites de consulta. Porém, poderia ser diferente o entendimento se o caso envolvesse dados sensíveis, como os de saúde, origem racial ou étnica, convicção religiosa ou biométrico, por exemplo.
- Seguindo a premissa acima, em 2025, a Terceira Turma do STJ reconheceu que, em contrato de seguro de vida, **o vazamento de dados pessoais sensíveis do segurado gera responsabilidade objetiva da seguradora e caracteriza dano moral presumido**, sendo destacado que dados sensíveis exigem maior proteção e que seu vazamento pode comprometer aspectos da vida do segurado, como honra, imagem e segurança pessoal.



- Em 2024, a mesma Terceira Turma do STJ entendeu que instituição financeira responde pelo defeito na prestação do serviço consistente **no tratamento indevido de dados bancários, quando essas informações são utilizadas por estelionatários para aplicar golpes contra consumidores.**
- Em outro caso decorrente de ataque hacker, a Terceira Turma do STJ, em 2024, reforçou que o fato de **a invasão ter sido causada por terceiros não afasta a responsabilidade da empresa, pois a organização precisa demonstrar que adotou boas práticas de segurança**, incluindo governança de dados, ferramentas de supervisão e políticas de mitigação de riscos. Se não conseguir provar sua diligência (responsabilidade proativa), poderá ser responsabilizada, não sendo suficiente a alegação de "fortuito externo".





8. Política Nacional de Cibersegurança e Comitê Nacional De Cibersegurança

(DECRETO Nº 11.856/2023)

O Decreto nº 11.856/2023 instituiu a Política Nacional de Cibersegurança (PNCiber), com a finalidade de orientar a atuação do Estado brasileiro no tema. A política se estrutura a partir de princípios fundamentais, como:

- Soberania nacional e priorização dos interesses do País;
- Prevenção de incidentes e ataques cibernéticos, sobretudo contra infraestruturas críticas e serviços essenciais;
- Reforço à resiliência de organizações públicas e privadas;
- Promoção da educação e do desenvolvimento tecnológico em cibersegurança;
- Cooperação entre entes públicos e privados; e
- Fomento à cooperação técnica internacional.

A PNCiber estabelece também objetivos estratégicos, entre os quais se destacam:

- Desenvolvimento de produtos, serviços e tecnologias nacionais voltados à cibersegurança;
- Garantia da confidencialidade, integridade, autenticidade e disponibilidade das informações digitais;
- Proteção reforçada a grupos vulneráveis no ciberespaço, como crianças, adolescentes e idosos;
- Combate aos crimes cibernéticos e ações maliciosas;
- Estímulo à adoção de medidas de proteção, gestão de riscos e resiliência organizacional;
- Fortalecimento da educação e capacitação técnico-profissional em segurança cibernética;
- Incentivo à pesquisa científica, à inovação e à articulação entre diferentes níveis de governo, poderes, setor privado e sociedade;
- Criação de mecanismos regulatórios e de controle para aprimorar a segurança nacional no ambiente digital; e
- Estruturação de ações coordenadas para a cooperação internacional

Como **instrumentos de implementação**, a política será operacionalizada por meio de:

- Estratégia Nacional de Cibersegurança;
- Plano Nacional de Cibersegurança.

Para acompanhar e promover sua execução, o decreto cria o **Comitê Nacional de Cibersegurança (CNCiber)**. Suas atribuições incluem:

- Propor atualizações à PNCiber e seus instrumentos;
- Avaliar e sugerir medidas para ampliar a segurança cibernética nacional;

- Formular propostas para aprimorar a prevenção, detecção e resposta a incidentes;
- Propor ações de formação em cibersegurança e estratégias de colaboração internacional;
- Atuar como instância de interlocução com a sociedade e entes federativos.

O CNCiber é um colegiado presidido pelo representante do Gabinete de Segurança Institucional da Presidência da República, e composto por 14 representantes de órgãos da administração pública federal, por 1 representante do Comitê Gestor da Internet no Brasil e por 9 representantes de entidades da sociedade civil, sendo entre elas 3 entidades com atuação relacionada à segurança cibernética ou à garantia de direitos fundamentais no ambiente digital, 3 instituições científicas, tecnológicas e de inovação relacionadas à área de segurança cibernética e 3 entidades representativas do setor empresarial relacionado à área de segurança cibernética.



9. Nova Estratégia Nacional de Cibersegurança (Decreto 12.573/25)

A E-Ciber tem características de 3ª geração, em comparação com suas equivalentes de outros países, embora seja o segundo documento do gênero no Brasil. A estratégia prevê que as cerca de 40 ações estratégicas serão desdobradas em iniciativas descritas em Planos Nacionais de Cibersegurança, atualizados periodicamente pelo CNCiber.

São 4 eixos temáticos que se articulam e avançam em paralelo:

- **1º EIXO:** ações para maior proteção e conscientização dos cidadãos e da sociedade, contemplando ações de educação formal e informal em todos os níveis e para públicos de diferentes idades.
- **2º EIXO:** segurança e resiliência de serviços essenciais e infraestruturas críticas, propondo ações que permitem continuar a acelerada transformação digital por que passa o Brasil enquanto se reduz o risco de incidentes que desestabilizem a sociedade.
- **3º EIXO:** ações concentradas na cooperação e integração entre órgãos e instituições nacionais e internacionais.
- **4º EIXO:** concentra-se em iniciativas para assegurar a soberania nacional e a governança da cibersegurança.



Destaques:

- propõe governança centralizada, promovendo o desenvolvimento de mecanismos de regulação, fiscalização, coordenação e controle;
- fortalece a soberania e independência do Brasil ao promover o desenvolvimento tecnológico nacional e a redução de dependência de tecnologias estrangeiras;
- promove a inclusão e a diversidade, ao incentivar a proteção e conscientização de grupos vulneráveis;
- promove a estruturação de maturidade cibernética, evoluindo estruturalmente a cibersegurança no Brasil;
- melhora a proteção de serviços essenciais e infraestruturas críticas, ao promover preparação e resiliência dos serviços essenciais e infraestruturas críticas, incluindo padrões mínimos e seguros e a certificação de produtos e serviços;
- fomenta a inovação em Pequenas, Microempresas e Startups, incluindo ações específicas para criar um ambiente de inovação para empresas de menor porte;
- propõe o incremento de atividades de cooperação internacional para o fortalecimento conjunto de cibercapacidades;
- promove educação e conscientização, ao perseguir uma cultura de cibersegurança sustentável e enraizada na sociedade;
- favorece a comunicação e resposta a incidentes, ao promover a gestão de riscos e da proteção e resposta a ciberincidentes;
- enfatiza a adoção de tecnologias emergentes, promovendo a redução do débito tecnológico do País em tecnologias emergenciais e disruptivas; e
- desbloqueia período de vigência (agora indeterminada), passando a considerar objetivos e ações de curto, médio e longo prazos, ajustável por meio de planos anuais.



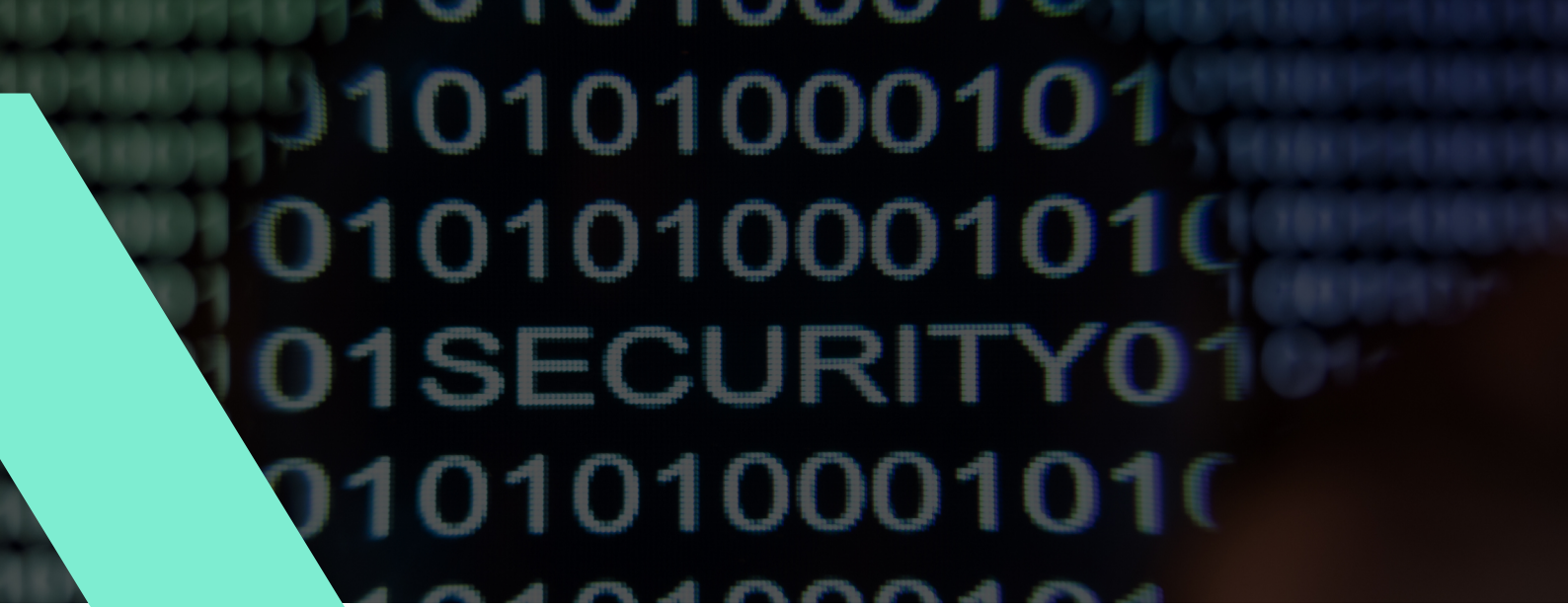
10. Próximos passos no Brasil

O Brasil está caminhando com a consolidação de sua governança em cibersegurança, incluindo as seguintes avaliações e medidas:

- **Proposta de criação de Órgão de Governança da Atividade de Cibersegurança no Brasil:** a tendência é que o Brasil avance na institucionalização de marco legal robusto de cibersegurança, acompanhado da definição formal de órgão central de coordenação e autoridade nacional nessa matéria. Discussões recentes no CNCiber indicaram a ANATEL como possível autoridade central de cibersegurança, refletindo a necessidade de estrutura capaz de articular respostas a incidentes, supervisionar setores críticos e coordenar políticas públicas.
- **O papel da ANPD e da LGPD na Cibersegurança:** a LGPD, coordenada pela atuação da ANPD, tende a ser cada vez mais integrada às políticas de cibersegurança, reforçando a noção de que a proteção de dados e a segurança da informação são dimensões indissociáveis da governança digital. A ANPD deverá intensificar orientações técnicas, padrões mínimos de segurança e expectativas de compliance, especialmente em contextos de incidentes que

envolvam dados pessoais, na linha de iniciativas internacionais que vinculam proteção de dados a requisitos operacionais de segurança cibernética. Inclusive, medidas de segurança, técnicas e administrativas (incluindo padrões técnicos mínimos de segurança), está como item prioritário da Agenda Regulatória da ANPD.

- **Cibereducação e Ciberhigiene:** conscientização e boas práticas para pessoas físicas e empresas, com foco em prevenção de riscos.
- **Referenciais mínimos de segurança cibernética:** desenvolvimento de recomendações práticas para operadores de Serviços Essenciais e Infraestruturas Críticas, estabelecendo parâmetros mínimos de proteção.
- **Diretrizes para ISACs (Information Sharing and Analysis Centers):** elaboração de guia para a criação e funcionamento de centros de compartilhamento e análise de incidentes, com base na Portaria nº 148 do GSI, visando integração à Rede Governamental de Gestão de Incidentes Cibernéticos (REGIC).
- **Plano Nacional de Cibersegurança:** construção do plano operacional que dará suporte à futura Estratégia Nacional, consolidando diretrizes, metas e ações coordenadas.



Conclusão

A **cibersegurança é pilar fundamental para a transformação digital**, a competitividade das empresas brasileiras e, por consequência, a estabilidade econômica e social do país, motivo pelo qual é importante que o Brasil:

- Estabeleça Marco Legal equilibrado, flexível e eficiente, alinhado com as melhores práticas internacionais, restringindo maior carga normativa às infraestruturas críticas e serviços essenciais para a economia brasileira;
- Crie entidade central de coordenação nacional de cibersegurança, com função de organizar e coordenar as ações regulatórias e políticas públicas relacionadas ao tema, bem como evitar sobreposição de competências;
- Fomente à conscientização, educação e capacitação em cibersegurança;
- Inserirá as PMES na esteira de governança da cibersegurança;
- Incentive à pesquisa, desenvolvimento e inovação em cibersegurança;
- Estimule e crie segurança jurídica para o compartilhamento de dados, inteligência e estabelecimento de uma rede nacional de resposta a incidentes cibernéticos;
- Fortaleça suas relações internacionais para colaborar em iniciativas globais de cibersegurança.

Direito,
Inovação
& Tecnologia

SOBRE NÓS

No VLK, **o Direito não é barreira**. É impulso para **inovar, viabilizar negócios** e construir uma sociedade mais próspera e justa.

Somos uma **boutique de Direito Digital** movida por **entregas que fazem a diferença**.

Conciliamos:

» Riscos e oportunidade;

» Complexidade e clareza; e

» Proteção e progresso.
Não importa o quão ousado seja o projeto: **faremos acontecer**, com segurança e **quebrando formalismos desnecessários**, nas seguintes áreas:

» Proteção de Dados Pessoais

» Governança Ética e Responsável de IA

» Cibersegurança e Resposta a Incidentes

» Legal Marketing e Propriedade Intelectual

» Regulação de Tecnologia

» Contencioso Estratégico

AUTORES



Rony Vainzof
rony@vlklaw.com.br



Caio Lima
caio@vlklaw.com.br

Direito,
Inovação
& Tecnologia

O e-book: "Cibersegurança e crimes cibernéticos: uma visão do Brasil" de Março de 2026.

CC BY-ND - Esta licença permite cópia e distribuição do material em qualquer meio ou formato apenas de forma não adaptada e apenas desde que a atribuição seja dada ao criador. A licença permite o uso comercial.